In the Name of God, the Most Compassionate, the Most Merciful

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 Second Session of the Committee

The present submission does not prejudice contributions of the Islamic Republic of Iran on the provisions and subjects referred to in the guiding questions as well as other provisions and subject of the convention 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 and questions as well as other provisions in the course of elaboration of the convention including during the substantive sessions of the Ad hoc Committee.

We underline that views of Member States whether in the form of general comments, proposals, statement or submission, concrete drafting proposals or in any other forms, should be taken into account throughout the process of elaboration of the Convention.

A. Agenda Item 4: Provisions on criminalization

Response to the First Group of Guiding Questions on Criminalization

- The one-size-fit-all approach in establishing offences may not always reflect legal exactitude. As in legal parlance depending on the crime and other factors, the objective element may require that the offender have a general or specific intent, know or should have known the circumstance, be reckless and so forth. Nevertheless, in the case of illegal access, the general intent suffices for incriminating the offender; a higher threshold may actually create a loophole for criminals to escape justice. Concerning protection for professionals, we believe that the national legal framework that criminalizes certain acts, could also decide the circumstances under which such acts may be authorized, hence, it is not necessary to include this topic in the convention and it should be left for States

to, in accordance with their domestic laws, adopt measures on ways and means of addressing this issue.

- When dealing with the offences in terms of injury and damage they cause or when considering the nature of offences as being illegal, unauthorized, etc. It may be needed to adopt a case-by-case approach since various crimes may require differentiated elements and results. For example, regarding illegal access, the very access *per se* could lead to bringing charges and prosecution of the perpetrator; yet in case of fraud, infliction of harm is the threshold that is required for prosecuting the offender. This approach would actually ensure that, as necessary, the specificities of crimes are taken into account and that responses commensurate with that.
- As for the question on the infringement of security as a requisite for establishing offences, we would like to note that not all conducts necessitate infringement of security measures since at times it is the case that the offender uses security loopholes to commit a crime. However, in some cases, such infringements could be considered as aggravating circumstance. Regarding the question on the forms of illegal interference, the said conducts such as disruption of information and communications technologies networks and systems could constitute as such interference.
- It is self-evident that criminals use information and communications technologies to carry out traditional and emerging crimes. The harms inflicted upon societies due to such misuse are no less detrimental than crimes dependent on ICT and in numerous cases they exact heavy tolls on victims even leading to grievous bodily harm. The international community requires a comprehensive framework that ensures effective fight against these crimes; hence, the convention should also stipulate provisions on criminalization of crimes enabled by ICT taking into account the specific factors and elements needed for ensuring legal accuracy and on a case-by-case basis.

Response to the Second Group of Guiding Questions on Criminalization

- On question number one regarding fraud and whether it would include theft, scam, financial offences, etc. we are of the view that, in general, such fraud encompasses the said conducts. In accordance with the domestic laws of the Islamic Republic of Iran, a person commits fraud related to computer offences if the said person, without authorization and through information and communications systems, obtain property, services or benefit of another person, by, *inter alia*, altering, obliterating, blocking or disrupting systems.

- Regarding the second question on ICT-related forgery, the specific intent to cause harm and through deception is necessary; yet, the very specific *mens rea* suffices. Whether the wrongful act has ultimately inflicted damage or not, would be immaterial; though depending on the circumstances the penalties for commission of such offences might differ.
- As to the question regarding professionals, it is understood that national legislations, in particular, laws and regulations related to procedural measures have stipulated provisions that addresses lawful activities in enforcement of law; therefore this should be left for States to adopt necessary measures for addressing this issue, nevertheless, national measures in this area should not entitle professionals such as penetration testers to commit an act to the injury and detriment of third parties.
- On question number three, if it is proved that the offender has actually intended to cause harm to the plaintiff, the said conduct could be considered as a form of forgery since through this illegal act, data is altered or created in a fraudulent manner to deceive another. Such alteration or creation should be reasonably capable of misleading and damaging another person.
- Fighting identity-theft is important since the propensity of criminals has increasingly inclined to utilize various forms of such theft to pursue illegal objectives. At times, identity-theft is one of the first steps that some criminals take in furtherance of their unlawful activities and when they acquire the identity of another person, potentially they will be able to commit many other forms of crimes. That being said, criminalization of identity-theft could be considered as a means to support law enforcement authorities in efficiently countering these criminals before they move forward and victimize more people. Identity-theft, could be considered, among others, as illegal and without right possession of another person's identity with the intent to cause material or non-material harm to that person or another one for economic gains.
- There is no need to include provisions on copy right in this convention as it has sufficiently been discussed in various other international settings.

Response to the Third Group of Guiding Questions on Criminalization

- The vital significance of responding to child sexual exploitation enabled by ICT cannot be overstated. Responding to this appalling crime which inflicts unbearable and often life-changing traumas upon children and societies requires a zero-tolerance approach. In this regard, in our domestic legislations, a robust and comprehensive act has recently been adopted for enhancing protection of minors, in particular, from sexual exploitation through criminalizing related

conducts and setting aggravating circumstances as well as stipulating other measures for protection of the child.

- The convention should establish related offences in a manner that ensures criminals cannot circumvent regulations or exploit possible loopholes to perpetrate this heinous crime. In this respect, to ensure provision of effective protection for minors, conducts such as, among others, dissemination of child sexual exploitation via ICT, exploiting children for the purpose of producing materials depicting child sexual abuse and willful and intentional provision of content depicting pornographic materials to children through ICT should be criminalized. Also, it should be established as an offence if a person encourages or coerce a child via ICT with the intent to provide the latter access to pornographic materials or otherwise with the same intent to instruct or deceive the child to gain such access. In addition, to provide children with the greatest protection from harm, the responsibility of service providers in this area should be taken into account.
- On question number three, within our domestic laws especially legislations pertaining to protection of minors and juvenile, the age limit has been defined as under 18.
- With respect to question number four, the specific features of the virtual space such as its potentials for criminals to anonymize identity as well as its very decentralized and borderless nature requires that the convention prevent offenders from exploiting such features to commit acts of extortion and dissemination of pornographic content.
- Regarding question number five, it is noted that misuse of ICT has led to emergence of crimes such as encouragement or coercion to suicide which cases are unfortunately increasing as ICT-based services develop. Commission of such offences may even occur on gaming platforms that encourages the person to perform certain life-threatening acts. Children, by far, are one of the most vulnerable against such offences as well as criminal acts endangering life including severe violence and drug abuse.
- On the last question, it should be noted that threat and blackmail, in particular, through threatening to disclose personal content as well as violation of privacy has appeared to be prevalent. To counter this crime, we could consider establishing as offence, the dissemination and distribution of personal and intimate images, videos, etc. of persons for blackmailing or sexual exploitation purposes. Aggravating factors could also be established when the said crimes are committed against children and women.

Response to the Fourth and Fifth Group of Guiding Questions on Criminalization

- The convention, in addition to crimes dependent on ICT, should also have within its purview crimes that are enabled by ICT; the inclusion of the former does not and should not mean the exclusion the latter. The very rationale and mandate of the Ad hoc Committee pursuant to resolution 74/247 is, "to elaborate a *comprehensive* international convention". Without addressing crimes enabled by ICT, the convention would lack such comprehensiveness. To fulfil the mandate of the Committee, inclusion of both variations of crimes are essential. To this end, an approach that considers legal elements surrounding various forms of crimes and their definitions as well as the extent and magnitude of harm intensified in the commission of such crimes as a result of the use of ICT could be taken.
- Misuse of ICT has multiplied and transformed the extent of harm inflicted by crime and criminal phenomena, such as, among others, racism, racial discrimination, xenophobia, insult to religious values and Divine prophets, distribution of drugs and psychotropic substances, trafficking in persons, trafficking in cultural property, child sexual exploitation and distribution of pornographic content.
- Criminal networks, often in the deep layers of web, engage in various activities related to the distribution of drugs and psychotropic substances; they remotely congregate with other criminal networks and disseminate know-hows for cultivation, production and manufacturing drugs. Misuse of technology on a drastically wider scope has also increased the magnitude of insult to religious values and Divine prophets and in many cases has led to offensive acts disrespecting religious values of hundred millions of people, in particular, Muslims who are increasingly being victimized to racism and xenophobic attitudes fueled by ICT means. Human traffickers have scaled up their harmful activities using ICT as a conduit for recruitment, coercing and deceiving victims, in particular, women and children. Other crimes mentioned above have also become prevalent in the virtual space and enabled by ICT often on a much larger scale incomparable to that of traditional means of crimes. These are the realities on the ground which emanate from criminal behavior enabled by ICT, these realities should not and could not be ignored, and the convention is the exact place that such challenges could be responded to.
- As to the question regarding obstruction of justice, we highlight the importance of criminalization of intentional acts that interfere, in particular, with the production of evidence and exercise of official duties of justices and law enforcement authorities. Such acts could include physical force, threats or

intimidation as well as concealment or obliteration of evidence; in addition, the commission of such acts by legal persons, in particular, service providers, could also be tantamount to obstruction of justice and giving rise to their liability. We would like to also underline the importance of recovery and return of assets and proceeds of crime as an important element in denying criminals of illicit profits.

- On the second question, we believe that accessory of crimes committed via ICT often includes facilitating the commission of an offence, encouragement, coercion, alluring, persuasion and enticement of another to commit a crime, notwithstanding, we are of the view that given the differences in the legal systems, the legal approach in criminalization of ancillary offences should be left to domestic laws.
- As regard the question on aggravating circumstances, the convention should stipulate the following aggravating factors:

    - Crime committed against minors and women; especially in crimes related to pornography, extortion and threat to disclose intimate and personal images
    - Crime committed as an organized crime and on a large scale
    - Severity of the offence
    - Repetition of crime
    - Involvement of multiple victims and injured persons

- 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 measures should hold legal persons liable for deliberate or otherwise knowingly involvement in the commission of offences to be established in accordance with the convention. In this respect, given the fact that responsibility of service providers constitutes an essential factor in fighting these crimes, provisions on the liability of legal persons should take into account the specialized context of crimes committed via ICT.

B. Agenda Item 5: General Provisions

Response to the Guiding Questions on General Provisions

- Given the rapid transformations in the field of ICT, the convention needs to keep pace with developments in this area as well as the evolving *modi operandi* of criminals. For this purpose, where necessary adoption of a technologically

neutral language may be the solution, however, neutrality of language should not be construed as neglecting the importance of adopting concrete languages on pressing challenges we encounter today as a result of crimes enabled by ICT, rather, quite contrary, where we could address crimes as we find them, regard should be given to specific languages that responds to the current and also future needs.

- To ensure that the convention withstand the test time and to improve measures for realizing the purposes of the convention concurrent with the technological advancement, establishing a conference of states parties is necessary. Within the framework of the conference, various future forms of the use of ICT for criminal purposes falling within the scope and provisions of the convention could be well discussed and states parties would have the opportunity to address new and emerging forms and manifestations of such crimes so as to ensure resilience of the convention in the face of new challenges.
- Regarding the fourth question, we believe 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 and also to strengthen national responses to such crimes and to assist state parties, in particular, developing countries, in fighting these crimes, *inter alia*, through provision of technical assistance, capacity building and transfer of technology taking into account the needs and priorities of requesting states. 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.
- For realizing these objectives, adopting an approach that cherishes a shared future in cyberspace for all Member States with equal opportunities and without discrimination is vital. In the same vein, 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.
- The Islamic Republic of Iran reaffirms that specific sections on protection of sovereignty should be included in the general provisions and the purpose of the convention 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 within the Charter of the United Nations, in particular, sovereignty equality, territorial integrity of states and that of non-intervention. Nothing in the Convention should entitle a State to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the

authorities of that other State. This is an established practice in elaboration of conventions in the field of preventing and combating crimes.

- To ensure a common understanding of the text of the convention, important terminologies in a specific section in the general provisions should be defined. As to whether the Committee should first define terminologies before other substantive parts or vice versa, it is plausible that important terms be defined after the substantive portions of the convention are discussed; it does not prejudice however the possibility of defining specific terms during the process of elaboration when the need arises to have a clearer picture of is being drafted and where consensus could be reached. In any way, discussions on definitions should take place within specific and limited time frame to ensure that the draft convention is provided to the General Assembly at its seventy-eighth session, as envisaged in resolution 75/282.
- On the question regarding human rights, deliberations made by Member States yesterday and also the nature of the convention signifies the existence of a consensus on the fact that this is not a human rights treaty; along the same line, we would like to recall that the practice of the international community in elaboration of the UNTOC and UNCAC, which were highlighted by many Member States, was to address crimes in a technical context. The remarkably wide adoption or signing of the conventions by 190 Member States is axiomatically in favor of this technical approach and cannot in any ways be understood as any form of prejudice to the importance of human rights. Consistent with the practice of the international community, such issues should be addressed in their right context and within their own specific instruments.
- On question number six, we believe that the convention could be considered by states as a basis for cooperation on electronic evidence in relation to other crimes provided that the crime in question fall within the purpose and purview of the convention and that such measures are in good faith.
- On the question related to asset recovery, the inclusion of provisions of seizure, recovery and return of assets and proceeds of crimes is essential for ensuring the comprehensiveness of the convention and denying criminals of illicit profits.
- Pertaining to the question on the terms computer systems, we are of the view that consistent with the mandate of the Committee we could utilize the term ICT systems.
- On the last question, we would like to note the importance of adopting a gender perspective in the specific contexts that requires so, for example in case of trafficking in persons, in which as per the TIP protocol to the UNTOC, the position that sometimes makes women vulnerable to TIP is abused, however, in the context of ICT that covers a broad range of crimes, which developments and

specificities might alter and not be even known today, its inclusion throughout the provisions of the convention from should be first justified especially from a legal standpoint.

C. Agenda Item 5: Provisions on procedural measures and law enforcement

Response to the First Group of Guiding Questions on procedural measures

- On question one, we believe that jurisdiction should be addressed in the section of the convention on procedural measures. Article 42 of the UNCAC could be the basis for this purpose nevertheless the specific features of the ICT realm may require to modify the provisions. This is contingent upon the development of topics in the process of elaboration of the convention and legal aspects of the issue including whether a crime was committed against ICT infrastructures.
- Noting the principle of *aut dedere aut judicare*, the answer to question number three is yes, extradition-related matters could be addressed in the convention.
- On the question as to whether procedural measures and law enforcement should be limited to the offences established in the convention, subject to future development in the negotiation and drafting of the text we might consider such procedures to be applicable to other offences that fall within the scope of the convention. Regarding the scope of procedural measures, we would like to also emphasize that such measures should enable law enforcement as well as entities such as service providers to effectively engage in international cooperation in fighting the use of ICT for criminal purposes.
- As regard the question on conditions and safeguards, it is underlined that criminal justice systems as a requisite usually address such elements in general and also context-specific legislations concerning procedural laws which provisions and conditions are applicable to all forms of crimes. It should be left for states to address these topics in accordance with their domestic laws. Just as this is not a human right treaty, it is not a convention on criminal procedures; rather procedures that are being discussed are meant to realize the purpose of the convention and to ensure effective responses and cooperation in fighting the use of ICT for criminal purposes. To this end, the convention should have within its provisions on procedural measures and law enforcement, areas including collection of electronic evidence, criteria for determining factor such as admissibility and validity of such evidence, special investigative techniques, expeditious preservation of data and cooperation of service providers.

- On the last question, just like the approach taken in elaboration of the UNCAC which led to its successful adoption and ratification at the global level, it is essential that we also take a technical approach in elaboration of the convention and refrain from addressing issues that fall outside the context of the convention.

Response to the Second Group of Guiding Questions on procedural measures

- On question number one, we are of the view that given the fact that crimes committed via ICT often transcend geographical boundaries which requires expedited cooperation at various levels, procedural measures should support law enforcement and judicial authorities in collection of electronic evidence in due time. In this context, procedural powers should also include provisions on the responsibility of service providers for expedited preservation of digital evidence; such provisions should define procedures for preservation and disclosure of trafficked data, cooperation with law enforcement including on the part of entities specialized in the field of registration of domain names and IP addresses as well as transparent measures to be taken by service providers in preventing dissemination of, *inter alia*, criminal content, malwares and identity-theft.
- Regarding question two, we are of the view that in procedural measures on collection of digital evidence, required information should be relevant and appropriate and be gathered in a manner that does not prejudice factors such as the validity, integrity and admissibility of the evidence.
- On question three, we believe that procedural measures may vary based on the form of data. In some cases, online tracing and real-time collection of data is required and in some cases there is a need for search and seizure of stored data. At times, it is also essential to seize ICT systems to conduct digital forensics examinations. In respect, we believe that the convention should aim to set standard and harmonized procedures that enables expedited and efficient measures in collection and preservation of digital evidence.
- Also, in relation to question one and two, where search and seizure is required, factors such as existence of strong suspicion, limitation in the scope of search and seizure orders, presence of the owner of data, ensuring functioning of systems in particular, systems providing public services, could also be taken into account.
- Regarding question number four, if the question aims to refer to the period of time that data are preserved, one year could be considered as the minimum period for preservation of data, however, the convention should allow for longer periods of time when the need arises. Where preservation orders are issued, time

limits will be determined by the issuing judicial authority to ensure proper investigation of the case.

- On question five, the term "data" which is a more general term is preferred. We see merits in defining the term at the earliest possible, which helps us all have a clearer picture of the relevant provisions of the convention.
- On question number six, if the Committee finally agrees on how to phrase this term, it may be more appropriate to define it in the general provisions where we define terminologies.
- As to question seven, in our domestic laws, not all such suspicions could be considered as grounds for instituting judicial investigation, rather, it is essential that the prima facie evidence demonstrate commission of an offence. Therefore, in the domestic relevant legislations, initiating an investigation and issuing search and seizure orders are subject to the existence of strong suspicions and should be conducted in accordance with the circumstances set out in the Code of Criminal Procedures.
- Regarding question eight, we are of the view that the convention should allow for declaration and reservations; though the approach to be taken for this purpose might need to be discussed at later stages and subject to the draft text of the convention. Finally, on procedural measures and law enforcement, due regard should be had to the fundamental principles of domestic legal systems.

Response to the Third and Fourth Group of Guiding Questions on procedural measures

- On question one, we believe that the provisions on freezing, seizure and confiscation and recovery, should enable competent authorities to return the proceeds of crimes and property in response to request of another State Party, where applicable. The approach in this respect should take into account and effectively address the current challenges that Member States, in particular, developing countries face in this area and should also aim to remove obstacles on applying measures for recovery.
- On question two, due to the specific features of crimes committed via ICT which contrast them from so-called traditional crimes, we believe that more discussions is needed on the very notion of "witness" in such diversified offences.
- Regarding question three, it is may not be necessary to address this topic through the whole convention especially given the fact that the convention would almost encompass an ambit of crimes in which the status and extent of harm inflicted upon victims might differ, however, in some offences there may

be a particular need for addressing this issue based on the dimensions of the crime in question and the injury caused to victims.

- The answer to question one of the Fourth Group of Questions is yes, we are of the view that the convention for the purpose of international cooperation, should generally set technical and where necessary time-sensitive standards in collection and admissibility of digital evidence such as standard formats for log reports and files, standard technical measures for preservation that ensures integrity and validity of evidence and essential items to be included in the digital evidence reports. Technical standards in this area could ensure and expedite effective cooperation including police-to-police cooperation in sharing admissible evidence and responding to crimes in due time. These standards however, should be without prejudice to domestic laws and measures that States may deem appropriate to take in this regard.
- Regarding question number four, we deem the enhancement of cooperation with law enforcement authorities an important element in fighting the use of ICT for criminal purposes, its formulation however needs more discussion that take into account the nature of the ICT realm.

***