Contribution of the Government of Mexico for consideration by the *Ad Hoc* Committee at its second substantive session

The Government of Mexico reiterates its commitment to substantially participate in the process to elaborate a comprehensive international convention on countering the use of information and communication technologies for criminal purposes.

Mexico considers that the mandate given by the General Assembly also establishes a clear opportunity to strengthen international cooperation and reaffirms the multilateral dialogue to better address the challenges posed by cybercrime.

As the international community expresses its many expectations on this process, it is time to advance by discussing concrete proposals to consolidate a comprehensive legally binding instrument, which includes substantive and procedural aspects, aimed at establishing basis for international cooperation and the exchange of information, experiences, capacities and best practices, but avoiding excessively detailed considerations which could fall into non-exhaustive provisions and far beyond the mandate given.

While it is expected to contribute to promote certainty and confidence at international level when countering cybercrime the Convention should include general calls and commitments to improve prevention, investigation, response, mitigation and prosecution efforts as far as allowed by national legal frameworks.

Aware of the complex process to elaborate any new international convention, Mexico emphasizes two challenges faced by this Ad Hoc Committee against cybercrime: 1) The existence of a much more robust and elaborated bodies of international legislation, in contrast with processes carried out in the past, especially with regard to traditional crimes that can be enhanced by the use of ICTs and significantly increase their scope, speed and scale but also the anonymity of the perpetrator; 2) The rapid evolution of cybercrimes as a consequence of exponential technological change.

The first challenge implies, then, that the new convention cannot and should not ignore, duplicate, reverse or nullify already existing international legal obligations and binding instruments. The second challenge implies that the value and relevance of the new convention could be questioned in a considerably shorter period of time. This means that, unlike previous cases, it might be useful to elaborate the new convention with flexibility to the future by using general and preferably timeless precepts, such as:

"*Recognizing that technological change is accelerating and that new developments in this field will persistently challenge the responses aimed at preventing and combating crimes committed with the use of new technological advances.*"

"Commending the work carried out by other international and regional organizations in this field, and aware of existing international and regional instruments to strengthen cooperation to prevent, respond, investigate, mitigate and prosecute cybercrimes."

Preamble and General Provisions

In order to prevent possible omissions and lack of compliance to the implementation of other future legally binding instruments, and according to precedent international and regional treaties, Mexico supports the inclusion of general references as initial provisions instead of very exhausted and detailed ones.

Regarding sovereignty, and following the example of the United Nations Framework Convention on Climate Change, Mexico recommends to include from the Preamble a general reference to reaffirm sovereignty, as follows: ***"Reaffirming the principle of sovereignty of States in international cooperation to countering the use of information and communication technologies for criminal purposes."***

Mexico also recommends including a preambular paragraph reaffirming the UN Charter, the applicability of international law and the Universal Declaration of Human Rights and other Human Rights obligations, as follows: ***"Reaffirming the purposes and principles of the Charter of the United Nations, the international law and the Universal Declaration of Human Rights and other relevant instruments on Human Rights."***

It is also recommended to include a general provision on the importance of States taking appropriate measures to protect people and in particular vulnerable groups: ***"Decided to take actions of prevention, response, mitigation, investigation and prosecution to effectively protect people and in particular vulnerable groups from the use of information and communication technologies for criminal purposes."***

As stated in this previous proposal, for the Government of Mexico it will be key to take into account along the Convention measures of prevention, response, mitigation, investigation and prosecution.

During the process of negotiation of the Convention it will be important to recognize the relevance of previous international legally binding instruments, and in particular the UNTOC, by bringing to the table concrete experiences which could be used to make international cooperation against cybercrimes more efficient. A related call to promote UN system-wide coherence must be included as a general provision.

Also in the preamble, Mexico recommends to include an explicit recognition of the opportunities and benefits bring by ICTs to make clear that they are not *per se* used by criminal and illicit purposes: ***"Recognizing that information, telecommunications and digital technologies bring opportunities to enhance development, close inequality gaps, to promote inclusion, well-being, justice and the exercise of human rights, and acknowledging the importance of promoting universal access to these technologies and to protecting their benefits."***

In addition, Mexico shares its interest in avoiding falling into the excessive use of safeguards that might act as a constraint, contrary to the spirit of international cooperation which should lead this process.

"*The purpose of this Convention is to promote bilateral and multilateral cooperation and legal assistance, including multi-sectorial cooperation, to prevent, respond, investigate, mitigate and prosecute the use of ICTs for criminal purposes."*

Mexico considers that other general provisions must be added on the following issues: defining conflict resolution procedures; establishing an implementation review mechanism; ensuring participation and collaboration of other relevant stakeholders in supporting the efforts carried by States Parties to prevent and counter the use of ICTs with criminal purposes; the recognition of the public core of the Internet and the relevance of net neutrality approach for the purposes of the Convention.

Criminalization

National jurisdiction will be a fundamental element to define criminalization obligations. In this regard, Mexico considers that UNTOC and UNCAC offer examples of provisions applicable by extension to countering crimes related to the use of ICTs, except for those cases linked to information in the cloud which will require further analysis and discussion from recent experiences of concrete investigations.

A departing point for criminalization should be to consider in the Convention those behaviors recognized by international law as crimes, particularly in the terms provided by other treaties adopted within the framework of the United Nations, which are carried out by ICTs, electronic and digital means. Then, it is recommended to include the following Article:

"States Parties recognize as crimes for the purposes of this Convention, all criminal acts recognized by the existing International Law that are perpetrated by information technologies and electronic means."

Among other criminal offenses, for the Government of Mexico it will be crucial to include those crimes related to child sexual exploitation as well as those related to gender violence by the means of ICTs.

It is recommended to include operative elements to strengthen investigation and prosecution, then it will be relevant to consider including annexes with those templates specifying needed data to proceed with information sharing requests.

As it is not expected to listing all kind of criminal offenses but primarily cyber-dependent crimes, and in order to prevent incompatibility or duplications to national laws, it is recommended to include a general commitment to States Parties to harmonize their legislations, if needed.

"Nothing in this Convention shall affect the rights, obligations and responsibilities of States and individuals under existing international law aimed to prevent and countering the use of ICTs for criminal purposes."

"In all actions aimed at the implementation of the present Convention, the best interests of the victims -individuals and institutions and organizations- of the crimes recognized in the present Convention shall be a primary consideration."

Procedural Measures and Law Enforcement

Given the importance of digital evidence for investigation, prosecution and law enforcement purposes, it is so expected States Parties to the Convention to agree general and minimally homologated procedural measures for obtaining, handling and preservation of digital evidences. It could be added: ***"States can consider and make use of all provisions contained on existing international instruments, such as the United Nations Convention Against Transnational Organized Crime for investigative purposes or/and evidence gathering and preservation of electronic evidence."***

With respect to private entities that provide ICTs services, Mexico recommends to include the following Articles:

"States Parties commit to make private entities that provide ICTs services, constituted in their respective territory or operating under their national jurisdiction to adopt and implement due diligence policies and procedures to avoid damages to third parties."

"States Parties also commit to take appropriate measures to promote that private entities constituted in their respective territory or operating under their national jurisdiction do not violate the laws of other States Parties."

It would be also relevant to include a general call to the responsibility of private entities which provide ICTs services to effectively collaborate with national law enforcement and judicial authorities with regards to investigations and prosecution of cybercrimes while respecting applicable privacy regulations.