Chile's views on the scope, objectives, and structure (elements) of the new convention, regarding the implementation of UN General Assembly resolutions 74/247 and 75/282

The Government of Chile is pleased to respond to the invitation to Member States to submit their views on the scope, objectives, and structure (elements) of the new convention, regarding the implementation of UN General Assembly resolutions 74/247 and 75/282.

Chile considers that the new convention should not conflict with other pre-existing treaties or agreements on cybercrime. It should be based on international cooperation and technical assistance as the foundation of the multilateral approach to the fight against cybercrime. The views of all countries must be considered of equal importance, as also to maintain an open, inclusive, transparent, and multi-stakeholder process.

1.- General aspects:

a. *Jurisdiction.* The new convention is an excellent opportunity to discuss this issue, which is the basis for many of the procedural tools that can be addressed.
b. Ensure that the definitions are drafted in a comprehensive way, so as to ensure their relevance and applicability in the context of the rapid technological transformation. To include definitions, such as the different types of data.

2.- Substantive Criminal Law:

a. Including the crime of receiving computer data. Although some countries have a restricted conception of this criminal type, it seems appropriate to include an illegal act that pursues this type of conduct when the "goods" stolen correspond to computer data and whoever stores them knows or not can less than know of the spurious origin of the same.

b. From the point of view of authorship and participation, it seems appropriate to specifically address the collaboration provided by the recipient of the money or securities illegally stolen through computer fraud, since, taking into account the particularities and investigative challenges that present this class of crimes in the vast majority of cases, it is pertinent to give special treatment to the persecution of those people who, as a general rule, constitute the first link to be followed in the criminal chain, so it is appropriate to increase their participation in the status of authors of the fraud, without prejudice to the possibility of offering a reduction of penalties in case they provide efficient cooperation in the capture of the rest of the computer criminals.

3.- Rules of Procedural Law:

a. It is appropriate to discuss possible new ideas and working tools that authorities could use for detecting potential crimes that are being developed or intended to be carried out on the Internet and the most effective way to face this type of crime.

b. It seems appropriate to discuss the balance that must be struck between the necessary and due protection of citizens, personal data, and the criminal investigation since overprotection of this type of information could generate consequences in the development of investigative procedures that allow a correct and timely criminal prosecution of this type of crime that benefits from the anonymity, transnationality, and lack of traceability that this type of behavior brings with it.

4.- International Cooperation Chapter:

a. It is important to establish principles on mutual legal assistance in criminal matters.
b. Countries should explore ways to help to ensure that information is exchanged among investigators and prosecutors handling cybercrime in a timely and secure manner.
c. Countries should cooperate closely with one another, consistent with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement action to combat cybercrime. Each country should adopt effective measures to establish channels of communication between their competent authorities, agencies, and services to facilitate the secure and rapid exchange of information concerning all aspects of cybercrime.
d. To consider the electronic transmission of MLA as a valid and permanent form and not only in emergencies.
e. Preservation and delivery of data.
f. To analyze the positive contribution of 24/7 networks, as an innovative contribution to international cooperation.
g. To regulate emergencies.
h. Countries should jointly identify the existence of the "digital gap" among countries as some countries lack the capacity and capability to prevent, detect and combat cybercrime and are more vulnerable in the face of cybercrime challenges.

5.- Special tools for international cooperation:

a. Delivery of data by Internet service providers and their relationship with the States.
b. Cross-border data access.
c. Special investigation techniques: online undercover agent, joint investigation teams and joint investigations, among others.

6. - Prevention:

a. Prevention of cybercrime requires participation by various stakeholders, including governments, law enforcement authorities, the private sector, international organizations, non-governmental organizations, academia, etc.
b. Promote victim-centered prevention strategies deal with interpersonal cybercrimes.
c. Countries should consider implementing mechanisms for cooperating with industry, including referrals to competent national authorities and takedowns of harmful criminal material such as child sexual exploitation and other abhorrent violent material.

7. - Gender perspective in the Context of a Cybercrime Convention

a. To include a gender perspective in the implementation and evaluation of the impact of the provisions of this convention, as well as account for a gender-sensitive analysis when it comes to the use of information and communication technology (ICT), in particular when referring to gender-specific issues related to cybercrime to promote gender equality and the empowerment of women online and offline.

b. Address cybercrime and prevent and combat violence against women and children.