PHILIPPINE STATEMENT

Item 4. Provisions on International Cooperation

29 August – 31 August 2022

Second group of questions

In Ilocano, a Philippine local dialect, “Agyaman ak Madam Chair, naimbag nga agsapa.” Let me now translate in English: thank you Madam Chair, good morning.”

Regarding the second group of questions on the transmission of requests and materials, we submit the following:

Transmission of requests for extradition may be made through a 24/7 point of contact (POC) network. We will elaborate on this when we get to this specific question, but would like to present now that this mechanism may be applicable for the issues in this group of questions.

Due to the nature of crimes to be covered by this Convention, in urgent circumstances, Parties may make requests for mutual assistance or related communications by expedited electronic means of communications, to the extent that such means provide appropriate levels of security and authentication. The requested Party may respond using the same. Encryption or other means of secure communications should always be used or higher levels of cybersecurity protocols that may evolve in time to ensure cybersecure transmission.

As for the means of addressing requests, electronic evidence may be stored and transmitted electronically, provided there are appropriate conditions and safeguards set in place. In this regard, capacity-building and technical assistance will be crucial to ensure that all state parties are able to implement the proper safeguards.

As for key information needed in a request for cooperation, the convention should set out provisions on the minimum information required. This will facilitate smoother cooperation. The requesting Party should submit a specific order, supporting information and any special procedural instructions to the requested Party. We will have a written submission on what the order and supporting information should specify. In general, the information should be adequate to assist the requested Party to give effect to the order. This information should not be disclosed to the service provider without the consent of the requesting Party. It would be a welcomed feature if a template for requests will be
provided that could guide those who intend to utilize international cooperation under this convention.

On the last question of this cluster, establishing a 24/7 POC network under the convention is a welcome innovation. This mechanism is key for urgent circumstances and will ensure the provision of immediate action. Additionally, channels through INTERPOL could be utilized. An “urgent” circumstance should be defined as a circumstance where critical information or evidence may be lost or before a request for assistance could otherwise be prepared, transmitted, and responded to, or where there is a significant and imminent risk to the life or safety of a natural person.

Thank you, Madame Chair.
Annex to the second group of questions (for the written submission)

In its request, the requesting Party shall submit the order, the supporting information and any special procedural instructions to the requested Party.

a) The order shall specify:

i. the issuing authority and the date the order was issued;
ii. a statement that the order is submitted pursuant to this Protocol;
iii. the name and address of the service provider(s) to be served;
iv. the offence(s) that is/are the subject of the criminal investigation or proceeding;
v. the authority seeking the information or data, if not the issuing authority; and
vi. a detailed description of the specific information or data sought.

b) The supporting information, provided for the purpose of assisting the requested Party to give effect to the order and which shall not be disclosed to the service provider without the consent of the requesting Party, shall specify:

i. the domestic legal grounds that empower the authority to issue the order;
ii. the legal provisions and applicable penalties for the offence(s) being investigated or prosecuted;
iii. the reason why the requesting Party believes that the service provider is in possession or control of the data;
iv. a summary of the facts related to the investigation or proceeding;
v. the relevance of the information or data to the investigation or proceeding;
vi. contact information of an authority or authorities that may provide further information;

vii. whether preservation of the information or data has already been sought, including the date of preservation and any applicable reference number; and

viii. whether the information has or data have already been sought by other means, and, if so, in what manner.

c) The requesting Party may request that the requested Party carry out special procedural instructions.
Third group of questions

Thank you, Madame Chair,

Regarding the third group of questions on grounds for refusal, we submit the following:

First, if a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this convention as the legal basis for extradition with respect to any criminal offense established by this convention.

In addition, the UNTOC and UNCAC, among others, provide grounds for refusal. The same could serve as a model for the drafting of provisions of the convention on the matter.

Second, the convention may deny assistance to a mutual legal assistance request if:

   a. the request concerns an offense which the requested Party considers a political offense or an offense connected with a political offense, or

   b. it considers that execution of the request is likely to prejudice its sovereignty, security, public order or other essential interests.

Third, taking into consideration the differences in legal systems, it would be beneficial to leave the determination of the grounds for refusal to domestic parties.

Fourth, there must be no outright provision in the convention as regards to cybercrime being a political offense, and thus, international cooperation shall not be rejected solely on this ground. This considering the fact that cybercrimes may be committed in furtherance of some political goal or agenda.

Thank you, Madame Chair.
Fourth group of questions

Thank you, Madame Chair.

In response to the group of other questions under this agenda item, we submit the following:

First, the convention should include provisions on mutual legal assistance regarding expedited preservation of stored computer data and electronic information, and the expedited disclosure of preserved traffic data. The requested Party shall expeditiously disclose a sufficient amount of traffic data to identify the service provider and the path through which the communication was transmitted.

Second, on investigative powers, the convention should include provisions on mutual assistance regarding the disclosure of stored computer data, real-time collection of traffic data, and interception of content data. At the operational level, the establishment of Joint Investigation Teams can assist in expeditious cross-border preservation and sharing of evidence and resources.

International cooperation provisions may include procedural measures for as long as the latter focus on enhancing cooperation and easing the disclosure of electronic evidence between and among memberStates. The Second Protocol of the Budapest Convention could serve as a model for provisions on these matters.

The convention may include a provision for transborder access to personal data of this nature. However, the consent of the person who has lawful authority to disclose said personal data through that computer system shall not only be the sole basis to grant access. There must be measures that allow the data subject, or the State party, to limit such access only to personal data strictly necessary or proportional to stated purposes, taking into consideration the general principles of data processing as may be provided by the member states' domestic laws over the personal data of its citizens, which may include extraterritorial applications.

Fifth, we support including a provision for a 24/7 point of contact network. In our national experience, this has been an effective practice in addressing cybercrime. Such a network established under this convention should be complementary to existing instruments and frameworks. The point of contact would ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data. If permitted by domestic law, the point of contact may also provide technical advice, preserve data pursuant to the articles of this Convention, and communicate with its counterparts in an expedited manner. The point of contact may also carry out or coordinate mutual assistance and extradition, consistent with its authority.

Provisions on the process in carrying out electronic surveillance and other types of covert investigative techniques must be carefully and specifically laid out in the convention premised on the inclusion of strong safeguards for the protection of basic human rights and freedoms, and local legislation of the requested party thereon.
Lastly, the convention should include a provision permitting video conference hearings. The procedures relating to the conduct of the video conference specified by the requesting Party shall be followed, except where incompatible with the domestic law of the requested Party. Hearings may be conducted through the use of the requesting State’s diplomatic missions and consular posts with respect to their own nationals on a voluntary basis, as part of consular functions.

Thank you, Madame Chair.