STATEMENT BY

MR. MOHD ISHRIN BIN MOHD ISHAK
DELEGATE OF MALAYSIA

ON

AGENDA ITEM 5: PROVISIONS ON TECHNICAL ASSISTANCE

AT THE THIRD SESSION OF THE AD HOC COMMITTEE TO ELABORATE A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES

NEW YORK, 1 SEPTEMBER 2022

Distinguished Madam Chair, Delegates, Ladies and Gentlemen,

On questions 24 and 25, technical assistance should include, *inter alia*, exchange of information and experience, technology transfer and training programmes for personnel responsible for preventing and combating cybercrimes. The convention should lay down provisions on technical assistance which must be rendered only upon request by a State Party. The exchange of information, knowledge and best practices are key components
in the prevention and investigation of cybercrime. It is equally important to gather data and conduct analyses of cybercrime trends and the latest modus operandi used by cyber criminals and appropriate countermeasures. These should be made easily accessible by the public.

On questions 26, 28 and 30, specific needs of developing countries in countering cybercrime would include, among others, better ICT infrastructure and equipment, enhanced legislation related to cybercrime, in depth understanding of mutual legal assistance procedures in other States Parties and assisting States Parties with both financial and technical resources for a 24/7 point of contact. These specific needs can be addressed in the technical assistance chapter of the convention as follows:

1) Capacity building in relation to the latest technology development in ICT that may aid cybercrime investigations comprises investigative techniques, evidence collection, forensic analysis, etc.;

2) Modern law enforcement equipment and techniques and the use thereof;

3) Specific training for legislators concerning developments of cybercrime laws and suitability of adoption and application of such laws in States Parties domestic laws;

4) Specific training for law enforcement officers in terms of investigations related to the cyber crimes; and
5) Training competent authorities in the preparation of requests for mutual legal assistance and other means of cooperation that meet the requirements of this convention especially for the collection, preservation and sharing of electronic evidence.

On question 27, Malaysia would like to support paragraph 2.3 in Japan’s written submission which proposes that the Ad Hoc Committee can consider inserting provisions on the specific roles of the UNODC, INTERPOL, and other organizations in providing technical assistance. And that the Committee should consider the details of the provisions so that these provisions will be useful in the fight against cybercrime without undermining existing efforts, listening to the opinions of each organization.

On question 31, Article 39 of UNCAC provides a good starting point for the development of a provision that sets out a clear role for the private sector, in particular communication service providers, in the early detection of cybercrime trends and potential criminal activity, as well as in facilitating public reporting of cybercrime-related incidents to law enforcement authorities. Private and non-governmental organizations can share their experience and best practices on creating awareness to the public.

I thank you, Madam Chair.