PHILIPPINES

STATEMENT
by
Ms. Mary Rose E. Magsaysay
Director IV, Cybercrime Investigation and Coordination Center

Ad Hoc Committee for Countering the Use of ICTs for Criminal Purposes
Agenda Item 6: Scope and objective of the convention
02 March 2022

Madam Chair,

At the onset, the Philippines welcomes the proposal of the Chair on the objective and scope of the Convention (17 February 2022) as it captures in a succinct manner the general ideas of Member States on what the future Convention should be about.

For its part, the Philippines believes it is crucial to categorize the current initiative of the AHC as pertaining to cybercrime and not that of cybersecurity. Cybercrime enforcement is uniquely a government responsibility, whereas cybersecurity is the responsibility of a range of public and private actors. In the Philippines, cybersecurity and cybercrime are interrelated but may be distinguished in the context of law. Cybersecurity refers to the collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets[1]. On the other hand, cybercrime is a species of penal law that punishes crimes committed with the use of computer systems or wherein the systems itself are the target.

This delegation would like to put it on record that many of the conclusions and recommendations arrived at by the Open-ended Intergovernmental Expert Group (IEG) to Conduct a Comprehensive Study on the Problem of Cybercrime encourage the use of existing instruments, such as the UN Convention on Transnational Organized Crime (UNTOC) and the Budapest Convention on Cybercrime (BCC) in coming up with a UN Convention that deals with cybercrime.

Given that the legislation and practices of most States worldwide have been shaped or influenced by existing agreements, future standards, such as the AHC on Cybercrime, need to be harmonized therewith. Hence, the objective of the AHC on Cybercrime should be to enhance international cooperation for a timely and effective

[1] Section 3 (k), Republic Act (R.A.) No. 10175 or the Cybercrime Prevention Act of 2012.

global response to cybercrime, and reduce duplication of efforts to optimize the use of existing mechanisms, channels, and platforms in addressing the same.

Additionally, we wish to see the Convention address the following matters:

- That adequate security of data and/or content not limited to Personal Identifiable Information should be taken into account, including on information and data creation and sharing, data reconstruction for legal purposes, and the standardization of risk mitigation structures;
- That there should be balance in defining the responsibilities of technology providers, creators of programs, platforms, websites, and the creators, administrators, technology providers, content delivery providers and/or any such complementary or ancillary services such as fintech companies, with standards allowing ease of businesses to proliferate in the digital world;
- That critical infrastructure should also be given due consideration by ensuring their security against unauthorized interference and recognizing the important role of power and energy generation in cyber-secure critical infrastructure.

Due to time constraints, this delegation will not go into the details and minutiae of the aforementioned points raised. Nonetheless, we shall be providing a more comprehensive text of our intervention to the Secretariat in due course.

Thank you, Madam Chair. END