Thank you, Madame Chair.

To address the first question, regarding the areas of focus under preventive measures, we submit the following:

a. Strengthening cooperation between law enforcement authorities, prosecutors, and other relevant stakeholders such as but not limited to the private sector, civil society organizations, non-governmental organizations, and educational institutions;

b. Implementation of mechanisms to facilitate cooperation between state parties and relevant international and regional organizations, and other stakeholders in promoting and developing the measures referred to in this article;

c. Providing education efforts for the public, developing campaigns and conducting capacity-building activities on the safe use of the internet, considering programs tailor-fitted for the vulnerable groups such as women, children, and the elderly; and

d. Developing appropriate measures, policies, and strategies that encourage the participation of individuals and groups from both the public and private sectors, civil society, non-governmental organizations, and community-based organizations in preventing and combating the use of information and communications technology for criminal purposes; and

e. Encouraging the State parties to raise awareness of the threat of cybercrime, and for companies, organizations, and individuals to take action that will make them more resilient to cybercrime and other criminal uses of information and communication technologies.

As to the second question, on measures to prevent cybercrime attacks targeting critical infrastructures, we view the importance of the periodical evaluation of the existing relevant legal instruments on the matter and administrative practices in the detection of the said infrastructures’ vulnerability to misuse by organized criminal groups. Further, we recommend the inclusion of provisions in developing and sharing analytical expertise on the prevention of cybercrime attacks.

Concerning the third question, each State Party should take appropriate measures, within its means and in accordance with its domestic law, to promote the active participation of individuals and groups outside the public sector, such as civil society, non-governmental organizations, and community-based organizations in the prevention of and the fight against cybercrime.

Further, each state party shall take appropriate measures, in accordance with its domestic law, to prevent offenses covered by this Convention and other acts of
cybercrime/using ICTs for criminal purposes in the private sector. One concrete way is to update current local legislations or to draft one, if none exist yet, that is in harmony with the provisions of this convention with respect to the offenses covered.

Regarding the fourth question, we concur that there should be a designated national authority that will be responsible for the prevention of the use of information and communications technologies for criminal purposes.

With respect to question number five, we agree that there should be a provision for states parties to create responsibilities for the private sector to establish and implement cybersecurity and data protection standards that are aimed at enhancing measures to prevent criminal uses of personal information, data in whatever form, and communications technologies.

Cybersecurity and data privacy resilience is founded on a deep understanding and awareness of its risks. It is vital for the governments, private institutions, and citizens of the State parties to adopt best practices of data protection and cybersecurity from a multilevel and multisectoral approach so that individuals, organizations, and governments become accountable for the security of the information that they control. Prevention is a key measure in minimizing possible cybercrime incidents. Moreover, we also welcome a provision aimed at harmonizing domestic legislation to provide clear guidance for the private sector on cybercrime prevention.

Finally, the Convention should encourage states to promote best practices and policies aimed at the prevention of cybercrime. This could include measures that are targeted to the needs of the vulnerable population and consistently monitored such as:

a. Up-to-date research on cybercrime issues, trends, and responses;
b. Tailor-fitted educational programs and resources, including information for victims on how to report cybercrime incidents;
c. Raising public awareness by providing information based on qualitative and quantitative evidence;
d. Encouraging state parties to cooperate and share best practices and expertise, wherever appropriate and practicable; and
e. Encouraging state parties to create and keep updated and targeted national plans to address and prevent cybercrime domestically.

Thank you, Madame Chair.

***