Mr. Chair,

I will deliver our position on the agenda item 6 and 7.

Firstly, on the preventive measures.

32. The chapter on preventive measures may cover the law enforcement cooperation both in evidentiary and intelligence level. Additionally, this chapter may include a general provision to encourage states to draft domestic policies and legislation to improve punishment strategy for the people who commit the crime and report it unless that deed does not create severe outcomes. Convention may also prioritize the prevent measures in relation to the vulnerable group of people, such as children and disabled persons.

33. If the convention is to criminalize the cyber-criminal attacks targeting critical infrastructures, there can be specific provisions to prevent these attacks. In our opinion, the other chapters of the convention should be in the boundaries of the criminalization chapter, except international cooperation.

As an answer to the Questions 34 and 36, the convention may put specific burden on the member states to take specific measures to cooperate with civil society, the private sector and academia, with a view to preventing the use of information and communications technologies for criminal purposes. For example, logging policy for traffic data has a crucial importance in combatting crimes committed through ICTs, which demands higher resources and technological means to provide such kind of cooperation with law enforcement agencies. Thus, States should define requirements in their domestic legislation towards ISPs to install systems that can log the internet traffic that is essential to prevent, detect and investigate such criminal activities committed through ICTs. In addition, the convention should put requirement for the Member States to define SOPs for private sector for fruitful cooperation, since the criminal networks operates over networks managed by private sector, the owner of those networks should be ready for sharing required data for prevention and investigation of committed criminal acts.

35. According to our point of view, designation of a national authority responsible for preventing the use of information and communications technologies for criminal purposes may not be a requirement, since many member states have different domestic governmental structure. However, we are open to discussions on this question with other member states.

37. The convention should encourage the State parties and private sector to collect, analyze, exchange, and share the information on trends and best practices on the field of crimes committed through ICTs.

Furthermore, on the implementation mechanism.

Answer to the questions 38 and 39: A chosen implementation mechanism should ensure the universal adoption and ratification of this convention and to maintain
flexibility by taking the nature of the crimes to be defined into consideration. Like many other member states, we are of the view that the establishment of a specific body for the review of the implementation of the convention under a Conference of Parties can be a suitable option. We are ready for discussions with other member states.

40. The convention may foster the participation of non-governmental organizations, civil society organizations, academic institutions and the private sector in the activity of a specific body to be established for the review of the implementation of the convention.

Thanks,

Mr. Chair