Madam Chair,

Distinguished colleagues,

Thank you once again for giving me the floor and possibility to address some of the challenges listed in questions 17 to 23 of agenda item 4.

 Expedited preservation and disclosure of stored computer data and electronic information are one of the most important aspects of any legal document, in this case international treaty, regarding cybercrime. Digital evidence is volatile in every possible mean, and its’ existence is not guaranteed for longer periods of time. Securing its’ availability and disclosure is actually marking the start of the criminal investigation which itself is very much depending on the success of such procedural actions.

 Real-time collection of traffic data, interception of content data, and similar measures are belonging to the group of so-called special investigation measures, and they are welcomed for criminal acts provided by the law, further providing that safeguards are in place for its’ implementation, acquisition and sharing.

 Cross-border access to data, although much debated by some, is reality of the contemporary world and communication through international computer networks, like Internet is. For example, in the very moment when we are accessing our web-based email services in most cases we are leaving territory of our country and entering international digital communication waters. Depriving such possibility would be a significant impediment to the cybercrime investigations what would lead not only to the loss of data but to the loss of the suspect, most likely. Of course, conditions should be put in place which would allow such action only if lawfulness of it exists, together with a legal consent of a person in question.

 Regarding 24/7 networks of contact points, we are of the belief that existing 24/7 networks for direct and almost instant cooperation in cybercrime cases, like the one based on Budapest Convention, can be used as a good example of how successful mechanisms for exchange and acquisition of information, evidence, and mutual legal assistance request, being them formal or informal, should be organized. It is important to underline that 24/7 cybercrime network should not only cover the communication and cooperation amongst law enforcement, but also
executing MLA authorities, having on mind a need for expeditious reaction of criminal justice authorities regarding electronic evidence and cyber criminals.

Allow me to reiterate that 24/7 system of communication should be a system with truly existing and conducting 24 hours a day, seven days a week available authority with trained personnel and equipment, and what is most important - sufficient authorization to execute MLA request in every part of the requested country in expedited manner.

As an evidentiary measure or action, remote hearings of persons in different procedural qualities who are participating in the cybercrime case, especially the witnesses, should be allowed not only through the diplomatic posts, what can significantly slow down proceedings, but also, under certain conditions, through the direct cooperation between competent authorities of countries included in case with such need or possibility.

Thank you, Madam Chair.