Statements by
Delegation of the Republic of Kazakhstan
to the Fifth Substantive Session of the Open-ended Working Group on Security of and in the Use of information and telecommunications technologies

New York, 24 – 28 July 2023

B. Existing and Potential Threats.

Kazakhstan fully supports the work of the Open-ended Working Group aimed at finding consensus on the key international agenda in the field of ICT.

In March 2023, we adopted the Concept of Digital Transformation, the development of the ICT industry and cybersecurity, which noted the documents in the field of cybersecurity.

On the presented report, our delegation expresses the following opinion:

On paragraph 10 (bis), we believe that there is no need to list all sectors of critical infrastructure, since the list can be endless. We propose to remove all spheres of activity and replace them with the following words "that provide a threat to the state and the provision of public life ".

[10 bis] States further expressed particular concern regarding the increase in malicious ICT activities impacting critical infrastructure (CI) and critical information infrastructure (CII), including CI and CII that provide ***a threat to the State and the provision of public life*** ~~*essential services across borders and jurisdictions, which can have cascading domestic, regional and global effects, as well as malicious ICT activities that target humanitarian organizations. The vulnerability of the healthcare, maritime and aviation sectors was particularly noted.*~~

On paragraphs 14 and 21. Given the rapid development of technology, we consider it right to mention AI. This technology could potentially have implications for the safe use of ICT.

In this regard, Kazakhstan has begun work on implementing a strategy for the development of AI.

On paragraphs 15 and 20. Our delegation supports the creation of a threat directory that will allow all countries to use threat information at the same level.

Mr.Chair, Statements will be send to Secretariat.