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, 25 July 2023

Thank you for giving the floor.

Regarding section C Kazakhstan generally supports the rules, norms and principles of responsible State behavior.

On paragraph 22C we confirm that the private sector plays an important role in ensuring the safe use of ICT. In this regard, Kazakhstan cooperates with the private sector on an ongoing basis. Kazakhstan with the private sector, as well as with the involvement of international organizations such as the ITU UN, the OSCE annually holds practical training events, conferences dedicated to solving modern problems in the field of cybersecurity. Such events make it possible to use the experience of the private sector to ensure the protection of the country's cybersecurity.

Considering that this paragraph is aimed to the work of the private sector, and also taking into account the importance of interaction between private companies and the state, we propose to include in this paragraph the importance of using public private partnership in the field of cybersecurity.

In addition, according to paragraph 22d, Kazakhstan fully supports the compilation of a glossary of technical terms and terminology in the field of ICT to develop a common understanding.

We believe that the creation of a single glossary will improve the effectiveness of normative work in international documents in the field of cybersecurity.

Regarding paragraph 27, we propose to delete sub-paragraphs A and B and suggest the following revision to the paragraph 27:

The OEWG Chair is requested to convene an informal intersessional meeting to discuss <u>the development of a common</u>

understanding of rules, norms and principles, including responsible State behavior in the use of ICT.

This would reduce discussions during the next official session.

As for section E and F, by the end of research the reference information document on the global directory of contact points in general, we have no objections.

For our part, we have identified the technical contact of the national computer incident response service KZ-CERT, which can already be contacted by e-mail today team@cert.gov.kz

KZ-CERT received more than 1,000 incident reports from 48 states in 2023.

In addition, Kazakhstan is actively working on capacity-building within the framework of the national cybersecurity concept updated this year.

In conclusion, we would like to note that our delegation generally supports the section "Capacity building", as well as the list of confidence-building measures.