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

New York, 6 – 10 March 2023

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. We believe that discussions within the framework of the current session will fully contribute to the achievement of the final goals of the OEWG aimed at ensuring the security of ICT in accordance with UN General Assembly Resolution 76/19.

Continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security, inter alia, data security, and possible cooperative measures to prevent and counter such threats [from para 1, GA resolution 75/240]

The influence of ICT in all spheres of activity of the state, organizations, and civil society is increasing every day.

Regarding specific measures to counter new threats, we believe that the theoretical discussions of experts are important, but the emphasis should be on the practical cooperation of our technical specialists with the involvement of experts from the private sector.

We believe that practical cooperation will increase the level of countering new threats.

Kazakhstan has established a coordinating advisory council with the participation of cybersecurity specialists from all government departments to discuss cases and make practical decisions.

And in conclusion, the proposal to create contact points for responding to computer incidents is a concrete measure that will allow us to strengthen cooperation, including practical.

Confidence-building measures [from para 1, GA resolution 75/240]

A good example of practical interaction between countries is the OSCE Informal Working Group on ICT Security.

Within the OSCE, there are 16 confidence-building measures to reduce the risks of conflict arising from the use of ICTs.

Under CBM 4, participating States voluntarily share information about the measures they have taken to ensure the openness, interoperability, security and reliability of the Internet. Since 2019, representatives of Canada and Kazakhstan have supervised this MD.

According to CBM 8, the participating States define points of contact (political and technical) to facilitate communication and dialogue on security issues in the use of ICTs and ICTs themselves. This measure is very important in order to establish interaction between countries.

According to CBM 16, participating States encourage, on a voluntary basis, responsible reporting of vulnerabilities in the use of ICTs and how to address them.

In principle, we believe that these confidence-building measures should be used at the global level.

Capacity-building [from para 1, GA resolution 75/240]

Kazakhstan actively interacts with the private sector on improving the provision of public services, the development of ICT and cybersecurity.

For example, today a number of popular public services are available on private digital platforms of banks.

For its part, the state has established requirements for private platforms to ensure information security and protection of personal data.

As part of capacity building in the field of cybersecurity, together with private specialized organizations, we are working to raise citizens' awareness of cybersecurity threats, improve national legislation, train specialists, and jointly ensure the protection of the country's infrastructure.

For example, together with a Kazakh company, the BugBounty vulnerability detection program was launched, where researchers receive appropriate rewards for discovering vulnerabilities in systems/websites.

More than 1,200 independent cybersecurity experts from around the world have already registered on the BugBounty site, from which more than 1,700 reports of vulnerabilities have been received, some of which are critical.

Public-private partnership allows you to use the competence and experience of a private company, be flexible in the implementation of projects, apply modern methods and technologies, and develop the competence of the state.