Please check against delivery

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

New York, 25 – 30 July 2022

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 the adoption at the end of the current session of the interim report 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.

A. Introduction

Kazakhstan has international treaties and carries out practical interaction within the framework of the Shanghai Cooperation Organization, the Collective Security Treaty Organization and the Commonwealth of Independent States, and also actively participates in the discussion of issues related to ICT security within the OSCE, the Conference on Interaction and Confidence Building Measures in Asia (CICA).

In particular, within the framework of the informal working group in the field of OSCE cybersecurity, Kazakhstan, together with Canada, supervises 4 confidence-building measures, within which it is envisaged that the participating States will, on a voluntary basis, share information on the measures they have taken to ensure openness, interoperability, security and the reliability of the Internet.

Within the framework of the Conference on Interaction and Confidence-Building Buildings in Asia (CICA) in 2021, a new confidence-building measure «Security and use of ICT» was approved, which is currently chaired by Kazakhstan. In October 2022, at the next summit of the Conference on Interaction and Confidence Building Measures in Asia, it is planned to adopt a statement by the heads of state.

Along with this, in order to build the capacity and improve the skills of domestic specialists in the field of countering the use of ICT for criminal and other illegal purposes, Kazakhstan actively cooperates with the bodies of the UN system - the Office of Counter-Terrorism, the Office on Drugs and Crime and others.

In view of the foregoing, we note the importance and timeliness of point A in the context of international and regional cooperation.

B. Existing and Potential Threats

Kazakhstan is taking comprehensive measures to counter cybersecurity threats at the national and international levels. The state policy in this area is implemented within the framework of the “Kazakhstan Cyber Shield” Concept, which provides for the qualification of threats and specific measures to level them.

Realizing that the influence of ICT is increasing in all spheres of activity of the state, organizations, civil society, work to strengthen cybersecurity will continue.

b) (i) Cooperation and assistance to establish and strengthen Computer Emergency Response Teams (CERTs);

Incidents, as a rule, are of a cross-border nature and equally threaten the security of the infrastructure of each of the countries, we believe it is important to support the point on cooperation and strengthening of computer incident response teams, this, in our opinion, will allow establishing direct contacts between national Computer Incident Response Services.

For its part, the National Computer Incident Response Service of Kazakhstan (KZ-CERT) has already concluded 26 memorandums with international organizations.

b) (vi) Undertaking international exercises and technical training including law enforcement officials.

As an enhancement of practical experience, we annually conduct cyber exercises, as well as practical conferences.

This year, on September 14-16, Almaty, Kazakhstan, the international practical conference KazHackStan 2022 will be held, which will be devoted to topical issues of cybersecurity.

A cyber polygon will be organized to imitate a critically important object of informatization.

Moreover, within the framework of this conference, the International Telecommunication Union of the United Nations will organize Interregional cybersecurity exercises for the CIS region and the Arab States.

We believe that such events will increase practical experience in responding to computer incidents, as well as strengthen international cooperation, which generally corresponds to paragraph 6 (VI) of international exercises and technical training.

b) (x) Measures to safeguard the general availability and integrity of the Internet.

We also want to support point 10 (X), as Kazakhstan pays great attention to creating a safe Internet from malware, phishing, etc.

In particular, in order to protect the Kazakhstan segment of the Internet, together with a private company, all websites with .KZ domain names were given a free opportunity to be protected by the WebTotem system.

It should be noted that more than 8,000 foreign clients use this system.

In addition, 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 1,100 independent cybersecurity experts from around the world have already registered on the BugBounty platform from which more than 1,200 reports of vulnerabilities have been received, some of which are critical.

d) States could consider strengthening interactions with interested stakeholders, including businesses, non-governmental organizations and academia, through the exchange of knowledge and best practices on the protection of CI and CII.

One of the most important issues of global digitalization is information security.

To address these issues, the Cyber Shield of Kazakhstan Concept is being implemented, within the framework of which a set of measures was taken on cyber security issues, which positively reflected in the UN Global Cyber Security Rating, where Kazakhstan is ranked 31st.

In particular, in order to develop a culture of cybersecurity, measures are taken on an ongoing basis to raise public awareness of cybersecurity threats. According to the results of a sociological survey, the level of public awareness is 75%.

For 5 years, the number of educational grants in the specialty of information security has been increased by 43 times.

In addition, the Information Security Management System is being actively developed, headed by the National Coordinating Center for Information Security of the country.

33 private SOC have been created to protect government agencies and critical informatization facilities.

There is an industry operational information security center in the financial sector, which coordinates the cybersecurity centers of second-tier banks.

Thus, we face the common task of ensuring cybersecurity. Not a single state is able to independently counteract modern threats.

In this regard, Kazakhstan is ready to participate in the process of exchanging experience in building an international cybersecurity system.

C. Rules, Norms and Principles of Responsible State Behaviour

c) Information exchange on best practices and cooperation could be enhanced, potentially drawing from models of information sharing in other fields, and could include topics such as innovation, vulnerability disclosure, the protection of critical infrastructure and cooperation between CERTs.

Since 2009, the country has been operating the Computer Incident Response Service, which is a single center for users of national information systems and the Internet segment, which provides the collection and analysis of information on computer incidents, advisory and technical support to users in preventing computer security threats.

Advisory and technical support to users, including foreign ones, is provided through the 1400 call center, email, telegram channel, and also through social networks. There is also a 24-hour emergency service.

As part of the international exchange of information for the current year, more than 360 notifications were sent to 40 states, and 361 notifications were received from 31 states.

Today, ICT plays an important role in all spheres of life. In this regard, we consider the proposal to expand the exchange of information between CERTs as a very important initiative.

E. Confidence-Building Measures

Thank you for opportunity to speak. I would also like to thank you for your efforts in preparing the document we are currently working on. We would like briefly touch on chapter E “Confidence-Building Measures”.

Kazakhstan generally supports the initiative to create a global register of contact persons on ICT issues under the auspices of the UN at the level of foreign policy, authorized, technical departments for operational interaction, indicated in paragraph A of chapter E “Confidence building measures”.

Also, Kazakhstan considers it important to exchange information on the adopted strategies and documents in the field of cybersecurity, for its part, we are ready to provide the adopted legislative acts and concepts in the field of cybersecurity, indicated in paragraph B of chapter E “Confidence building measures”.

In turn, Kazakhstan intends to send information to the UN Secretary General about the efforts being made at the national level to strengthen information security and promote international cooperation in this area.

We also generally support the proposed initiatives in chapters D “International law” and F “Capacity Building”.