Check against delivery

Statement by the Delegation of Ukraine under agenda item 5 (a) of the Open-Ended Working Group on security of and in the use of information and communication technologies (2021-2025)

Mr.Chair,

The voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. Norms set standards for responsible State behaviour, help to prevent conflict in the ICT environment, as well as contribute to its peaceful use to enable the full use of ICTs to increase global social and economic development.

It is of utmost importance for all States to be guided in their use of ICTs by 11 norms. Ukraine believes that we should focus our efforts on advancing the implementation of these norms that will allow to assess the activities of States in cyberspace in order to prevent conflict and increase stability and security. In our view, both norms and confidence building measures are crucial for maintaining peace and preventing conflict.

In connection with guiding questions provided by you, Mr. Chair, we would like to recall a norm 13 (g), according to which States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199. This norm reaffirms the commitment of all States to protect critical infrastructure under their jurisdiction from ICT threats and the importance of international cooperation in this regard.

In this context, we would like to stress that being a target of regular cyber-attacks and considering global trends in the rise of malicious use of ICTs, including against the critical infrastructure, Ukraine has been developing an effective cybersecurity ecosystem within its territory.

In particular, since 2016, the National Security and Defense Council of Ukraine (NSDC) has been coordinating and controlling the activities of the security and defense sector entities that ensure cybersecurity of Ukraine through the National Cyber Security Coordination Center (NCSCC).

The National Cyber Security Coordination Center plays a crucial role in Ukraine's national cybersecurity ecosystem, as well as coordinates the work of all government cybersecurity agencies.

The NCSCC has been actively forming and improving mechanisms for assessing the current state of cyber protection of State’s information resources

and critical infrastructure facilities, identification of threat factors aimed at strengthening of cybersecurity of the State.

Today, the NCSCC is the primary national hub for cooperation between the public and private sector. Therefore, an important task of the NCSCC is to unite the efforts of the state, the private sector, foreign partner companies and countries to build joint and effective cooperation.

In September 2020, a new National Security Strategy of Ukraine was enacted by the Decree of the President of Ukraine. This document contains the government's vision of threats to the national security and steps to minimize (or neutralize) them.

Later on, the new Cyber Security Strategy has been adopted. The document is fully aligned with the National Security Strategy and based on such key principles as deterrence, cyber resilience and cooperation.

Thank you, Mr.Chair