Check against delivery

Statement by the Delegation of Ukraine at the First Committee Thematic Debate under Cluster 5 'Other Disarmament Measures'
(24 October 2022, New York)

Mr. Chair,

Ukraine aligns itself with the statement delivered by the European Union. Now we would like to make a statement in our national capacity.

Rapid development of information and communication technologies progressively led to the "re-formatting" of internet space: nowadays it is no longer a comfortable platform for communication, but also real weapon, which becomes more and more dangerous in hands of hackers, criminals, some state actors and their proxies.

Unfortunately, despite existing legal norms and institutional mechanisms established to combat cyberattacks on national, regional and international levels, the advantages of modern digital world are too often been abused, with cyber-attacks on the rise, having become a new method of warfare.

Ukraine is the state where cyber-attacks since 2014 became one of the major elements of the external attempt to undermine our sovereignty. Throughout the period of 2014-2021 Ukraine has faced an unprecedented number of cyber-operations against vital objects of our critical infrastructure. The most notable one involved the launch of the NotPetyamalware cyber-attack in June 2017. Most of those attacks were carried out by hacker groups being controlled from the Russian Federation.

Since the beginning of Russia's full-scale military aggression against Ukraine on 24 February 2022, cybercriminals attacked the Government and local authorities. Also among the main targets are commercial and financial institutions, security and defense sector, the energy sector, transport industry - all infrastructure that works for the livelihood of the population.

In fact, Ukraine became the first in the world to become a participant in a full-fledged cyber war. Since the Second World War, humanity has never faced such serious challenges as today, when Russia attacked our country. For cyberspace, war is a completely new challenge.

During 8 months of the war, the Government Computer Emergency Response Team of Ukraine CERT-UA registered more than thousand cyberattacks.

Mr.Chair,

Despite Russia's military aggression, Ukraine further strengthens its cybersecurity system, with the material and advisory assistance of Western partners.

The national cybersecurity system put in place by the Cybersecurity Strategy of Ukraine is based on the Ministry of Defence, the State Service of Special Communications and Information Protection, the Security Service, the National Police, the National Bank. It ensures collaboration between all government agencies, local authorities, military units, law enforcement agencies, research and educational institutions, civil groups, businesses, and organizations, irrespective of their form of

ownership, that deal with electronic communications and information security or are owners of critical information infrastructure.

The Center has a supervising function and undertakes tasks related to analyzing the state of national cybersecurity and its preparedness for combating cyber threats, as well as forecasting and detecting relevant potential and actual threats.

The purpose of the current Cybersecurity Strategy of Ukraine, established for the period 2021–2025, is to create conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and the State. The document is based on the principles of deterrence, cyber resilience and interaction.

On the international level, we emphasize that a particular attention should be placed on elaboration of unified standards in combating cyber threats, sharing best practices, building mutual trust in the field of cybersecurity, preventing the use of cyberspace for political, terrorist and military purposes, as well as providing financial and technical assistance to enhance national capacities to withstand cyber threats, mitigate the risks and strengthening resilience.

In addition, the issue of ensuring accountability in cases of identification of a particular state or state actors behind preparation or exercising targeted malicious use of ICTs or dissemination of lies for hostile purposes is especially important.

After all, international efforts made in this domain are simply in vain if there are no reliable mechanisms to detect, punish and bring to justice individuals and relevant states, responsible for coordinating and financing illicit activities in the global cyberspace.

Mr. Chair,

As one of co-sponsors, Ukraine fully supports the establishment of a UN Programme of action on Advancing Responsible Behavior in Cyberspace, which aims at establishing a permanent, inclusive, actin-oriented mechanism within the United Nations.

We share the key goals of this initiative aimed at ensuring support for States in the implementation of the framework for responsible state behavior in cyberspace and increasing dialogue and cooperation with relevant stakeholders.

In this regard, our delegation strongly support the relevant draft resolution tabled by France within the First Committee.

Thank you.