STATEMENT BY TURKEY

Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies
(29 March 2022)

Mr. Chair,

At the outset, allow me to express my Delegation’s appreciation for your efforts to steer our work in the Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies.

Turkey attaches great importance to this OEWG, as a unique platform having a universal membership and valuable potential for trust and confidence-building in cyber space. Indeed, we fully share the assessment that this Group itself constitutes a confidence-building measure, provided that its potential is duly utilized.

Concerning the issue of existing and potential cyber threats, I would like to highlight the following points:

-In today’s world, peace, security, human rights and economic development are increasingly impacted by the use of ICTs. Parallel to advances in technology, cyber risks and threats are rapidly growing in volume, complexity and severity.

-This has particularly been the case since the outbreak of the pandemic, which revealed the correlation between increasing dependency to ICTs and vulnerabilities to cyber risks. In our view, tackling threats and risks in cyber space is essential in order to achieve an open, free, stable and secure cyberspace at the international level.

-We have been observing a dramatic increase in the cyber-attacks targeting critical infrastructure, such as electronic communication, energy, finance, transportation, water management and other essential public service sectors.

-These attacks have reached a level to threaten international security and stability as well as socio-economic development.

-Turkey is highly concerned with the malicious ICT activities, which go against the norms of responsible state behavior in cyber space.

-The final report of the previous OEWG had indicated that the use of ICTs in future conflicts between States is becoming more likely. Recent developments have just warranted that concern. We have witnessed malicious use of cyber tools as part of aggression against Ukraine. We firmly reject such violations of international law and the UN Charter.
A key element in achieving security and stability in cyberspace is respect for international law, including the UN Charter, as well as international humanitarian law and international human rights law.

Turkey strongly supports the effective implementation of the UN framework for responsible state behavior developed through the work of successive Groups of Governmental Experts and reaffirmed by the previous OEWG.

For its part, Turkey has been working through successive National Cyber Security Strategies and Action Plans to develop measures to tackle cyber threats. Our National CERT is constantly communicating information regarding malicious cyber activity or possible vulnerabilities to institutional and sectoral CERTs and the public. Protection of critical infrastructures and increasing resilience has been identified as a strategic objective in our National Cyber Security Strategy.

However, we recognize that the level and sophistication of cyber security, digitalization, cyber resilience and infrastructure varies significantly among member states. Therefore, every state has its peculiar experience in cyber realm.

In our efforts to enhance cyber resiliency and ensuring security for all, a good step forward would be working to reduce technical and policy gaps among member states by identifying appropriate methods.

We must be able to make informed decisions regarding capacity-building efforts that cover a wide range of areas at the technical and policy levels.

For this purpose, we can utilize the criteria used by the International Telecommunication Union’s Global Cybersecurity Index (GCI). This Index is considered an important tool to determine different levels of resilience among countries in the cyber domain. It can give us a clear picture regarding potential areas of improvement, especially among developing countries, in terms of cyber security.

In addition, the “National Survey of Implementation” proposal, which Turkey supports, would also be an important tool for having an informed assessment of global cyber threat landscape and the required work to increase cyber resilience.

Furthermore, increasing exchange of information among Member States and establishing platforms that would serve as communication channels in emergency situations while also enabling sharing of information and resources would be crucial in our efforts to tackle cyber threats. To this end, we support establishing Points of Contact (PoC) networks and a global directory of PoCs.

Similarly, sharing experiences and best practices, developing guidelines for regulatory frameworks, conducting international exercises to increase cyber security preparedness and response capacities as well as awareness raising activities are also important concrete measures that we can apply in addressing cyber threats.
In conclusion, we stand ready for cooperation to identify and minimize threats and risks in cyberspace and welcome the concrete ideas and proposals presented by previous delegations towards this objective.

Thank you.