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

New York, 28 March – 1 April 2022

Rules, Norms, and Principles

In the name of God, the Compassionate the Merciful

Mr. Chair,

The OEWG’s involvement with all State-actors regarding an issue with overarching influence on all aspects of human life was long-awaited. This intergovernmental process is a place to comprehend the outcomes and products of other mechanisms and align them with the international community’s will and aspirations in an inclusive and transparent manner.

Therefore, while the OEWG does not start from scratch, nothing prevents it from further working on the previous findings.

In fact, resolution 75/240 has entrusted the OEWG to continue, as a priority, to further develop the rules, norms and principles of the responsible behavior of states and, if necessary, to introduce changes to them or elaborate additional rules of behavior. We recall that the norms contained in the GGE report in 2015 are not comprehensive.

Since the rules of behavior agreed in the past are not sufficient for the full-scaled regulation of the ICT environment in line with the attributes of ICTs and the needs of the evolving situation, it is necessary to continue to develop
a comprehensive universal list of rules, norms and principles for the responsible behavior of States. The annex to the Chair’s Summary of the first OEWG on additional proposed norms allude to the incomplete work previously done on norms. It has been clearly recognized in paragraph 80 of the substantive report of the previous OEWG. This should be the initial basis for the Group discussions on this topic.

In our view, the idea of implementing rules of behavior is premature and will not have the expected effect if the list of rules, norms and principles will not have universal and obligatory character. Prior to any discussion on the operationalization of the said norms, the OEWG needs to agree on the final and comprehensive list of the norms.

In the framework of norm-making activities, it would be reasonable for the OEWG to elaborate on possible ways of regulating the activities of IT companies in the digital sphere and formulate rules of responsible behavior of business in the information space. Any list of norms will not be completed if it lacks norms on the behavior of digital platforms/companies and social media networks in the ICT environment, either by their own responsibilities or responsibilities of their respective governments. Stakeholders rather than States also need to observe the principles, rules and norms for their responsible behavior in the ICT environment. The private sector and social media platforms should observe the rules, norms and policies of the countries where they operate. States should also consider ways and means to hold them responsible.

The views of the Islamic Republic of Iran regarding this critical issue have been elaborated in detail in our second submission dated 20 February 2020 wherein we have indicated that prior to any discussion on the operationalization of any envisaged norms, further discussion is needed to develop, change or add to the 13 norms contained in Para 1 of the UNGA resolution 73/27.

We also indicated the need for the structured discussion on the 13 norms around their ambiguities associated with the understanding of the identified norms, the need to agree on the terminology for their understanding on the list of terms as well as introduce change to the identified norms in order to re-visit all 13 norms and elaborate on additional norms.
It is the I.R. of Iran’s priority to formulate new norms in light of existing and potential threats in the ICT environment. During the previous OEWG, our delegation has put forward specific proposals on new rules related to threats arising from content, unilateral coercive measures and the responsibility of the private sector and other stakeholders, among others. We are ready to engage in detailed discussions, perhaps in a sub-group format, with a view to reaching consensus on a set of concrete norms as mentioned in the Chair’s summary attached to the final report of the previous OEWG.

Those additional norms, including inter alia, are as follows:

1. The roles of States, with the primary responsibility for maintaining a secure, safe and trustable ICT environment, should be enhanced in the ICT environment governance, including policy and decision making, at the global level. The envisaged governance should be realized in a manner that strengthens the state sovereignty and shall not affect the rights of the states in the decision-making for the development, governance and legislation models in the ICT environment;

2. No state has the right to intervene through cyber means, directly or indirectly, and for any reason in the internal or external affairs of other states;

3. All forms of interventions and interference or attempted threat against political, economic, social and cultural systems as well as the cyber-related critical infrastructure of the states shall be condemned and prevented (UNGA resolution 2131 of 21 December 1965);

4. States shall not use ICT advances as a tool for economic, political or any other type of coercive measures, including limiting and blocking measures against target states. (UNGA resolution 2131 of 21 December 1965);

5. States should ensure that appropriate measures are taken to ensure that the private sector with extraterritorial impacts, including platforms, is held accountable for their behavior in the ICT environment.

6. States must exercise due control over their companies and platforms under their jurisdiction and control, otherwise they are responsible for knowingly intervening in the national sovereignty, security and public order of other states;
7. States should refrain from and prevent the abuse of ICT supply chains developed under their jurisdiction and control to create or assist in the development of vulnerabilities in products, services and maintained compromising sovereignty and data protection of the target states.

Further to our previous proposals, my delegation would like to propose structured discussions on the 13 norms around the following lines:

1- **Ambiguities:** To “further develop” the norms, the OEWG should address ambiguities associated with the understanding of the identified norms.

2- **Terminology:** The OEWG may work on a list of agreed terms to improve understanding and avoid further ambiguities. It is necessary to highlight that the elaboration of norms requires a cybersecurity terminology that is accepted by all the Member States.

3- **Introduction of changes:** To ensure a comprehensive consensus-based OEWG outcome on the norms and given the fact that most of the OEWG’s participating states were absent in the GGE processes, it is necessary for the OEWG to allocate sufficient time on re-visiting each and every one of the 13 identified norms.

4- **Elaboration of additional norms:** There are issues not sufficiently covered by the 13 identified norms. Therefore, the OEWG needs to focus on additional norms necessary to address other areas of responsible behavior.

We believe that a conflict-free, development-oriented, transparent, fair, moral and peaceful cyberspace will not be guaranteed only through a set of voluntary, non-binding norms. It requires a legally binding instrument that would, among others, specify the commitments and responsibilities of those States that have dominance in technology and cyber-related resources vis-a-vis their own behavior as well as the behavior of companies and platforms registered under their jurisdiction.

Thank You!