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

General Observations,
Existing and Potential Threats

In the name of God, the Compassionate, the Merciful

Mr. Chair,
Thank you for your able leadership. We did not object to your proposal to convert the meeting's status to informal, but we especially count on your clarification on the meeting's report, which should reflect the views of all member states. About the topic under discussion, my intervention consists of some introductory remarks about the guiding questions and narrative summary followed by our position on the existing and potential threats.

First and foremost, it is highly expected that within the mandate of the OEWG, the Group will start negotiations rather than merely deliberate on all six chapters of its mandate. This is, however, not going to proceed until and unless the thematic-focused discussions are organized in order to avoid an undesirable situation for the delegations regarding the final outcome of the OEWG to either take it or leave it. Thus, we appeal to the distinguished Chair to modify the method of work and to also establish the subgroups based on resolution 75/240. We are hopeful that this approach will bridge the gap among delegations as we take on the long process ahead of us.

Secondly, it seems that the narrative summaries as well as the guiding questions mainly reflect a partial view of the group of States and have yet to be more balanced by adequately reflecting the views of the NAM or other
individual member states. The importance of an inclusive approach should not and must not be overlooked.

Thirdly, the Chair’s summary attached to the final report of the previous OEWG, as its integral part, reflects different views of the membership on essential problems that have to be negotiated, hammered out and agreed upon as the most important prerequisite before exerting any action-oriented initiative. During the previous OEWG as well as in the first substantive session of the current OEWG, my delegation has had plenty of written submissions, including concrete proposals, that reflect our views on all subjects in detail. Our internal agencies correctly believe that these views should also be reflected in any conclusion, including the narrative summaries.

Having said that, some other guiding questions could be considered as follows:

1. Given the rapid development of ICTs and their impact on daily life, what are the existing and potential threats stemming from actions in the ICT environment aimed at undermining the political, economic and social system of states, such as disinformation, fake news, false and fake accusations and attributions that are against the politically independent and sovereign rights of states? Furthermore, how can the neutrality of states be ensured?

2. What contributions of states reflected in the Chair’s summary of the first OEWG can be used to further review the 13 rules, norms and principles of responsible behavior in accordance with UNGA resolution 73/27?

3. How can the principle of state sovereignty be preserved while ensuring global security of information space?

4. How can the access to technologies, infrastructure and information be available to all countries, in particular to developing countries, while ensuring a secure, safe and stable ICT environment by all stakeholders as governments taking lead?

5. How do certain states use subversive attempts in violating states’ sovereignty and internal affairs, and how this can be prevented together with intervening in the political, economic and social affairs as well as systems of other states?

6. How can the weaponization of the ICT environment be addressed through the norms of responsible behavior?
7. What are the ways and means that states can hold other stakeholders and social media platforms and private sectors responsible for their behavior?

8. How can management and the global governance of the Internet be ensured by relevant CBMs in a way where the monopoly (in management and anonymity of persons and things) as a main source of mistrust in internet governance can be addressed?

Now, concerning the issue of threats, the Islamic Republic of Iran presented its views on the existing and potential threats emanating from the malicious and irresponsible use of ICTs in its written submissions as well as its oral contributions during the first OEWG sessions and the first substantive session of this new OEWG.

The new OEWG needs to anticipate a range of existing and potential threats that have not been considered thus far and, in one way or another, put at risk the peaceful, human and secure nature of the ICT environment. This requires a more comprehensive approach to the threats in the sphere of information security which addresses not only the digital infrastructure but also the content and information itself.

Notwithstanding the risks emanating from the existing monopoly in internet governance and the need for a new architecture, this issue has not yet been effectively discussed in the United Nations system since the World Summit on the Information Society (WSIS) held in in Tunis in 2005 (Articles 29 to 82 of the Tunis Agenda for the Information Society). It is unfortunate that Internet Governance Forum (IGF) refuses to discuss this issue and refers it to the OEWG while the OEWG considers it beyond its mandate to discuss internet governance and refers it to the IGF. As a result, the international community was unable to achieve a consensus with regard to the global governance of the Internet which would thereby remove the current monopoly over the governance of the Internet. The international community must outline a better solution for internet governance within the OEWG shortly which will safeguard the stability and security of the ICTs environment.

Some examples of the urgent as well as challenging existing and potential threats that have been raised by my Country and other States during the previous discussions are as follows:
1. **Violation of cyber sovereignty**
   The I.R. of Iran believes that the territorial sovereignty and national jurisdiction of States should be extended over cyberspace and all its elements. Any coercive use of cyber tools with physical or non-physical effects -or those that have such potential- poses a threat to national security or may lead to political, economic, social and/or cultural destabilization, constituting a violation of the state sovereignty whether committed by states or other actors.

2. **Threat or use of force in the ICT environment**
   All States should refrain from the threat or use of force against the territorial integrity or political independence of any state within and through the ICT environment. However, some states are developing ICT’s capabilities for weaponization purposes which are reinforced by their offensive hybrid doctrines aimed at resorting to cyber and kinetic operations. This has primed the ICT environment to become a new arena for the battlefield and a potential threat to the prohibition of the threat or use of force against the territorial integrity or political independence of other states.

3. **Interference and ICT’s abuse for illegitimate geopolitical goals**
   The international community has already condemned all forms of overt, subtle and highly sophisticated techniques of coercion, subversion and defamation aimed at disrupting the political, social or economic order of other States (Paragraph 4, UNGA resolution 31/91 December 1976). The letter and spirit of this paragraph certainly covers those related to the ICT environment.

   In recent history, states with subversive aims attempt to overtly or covertly use the ICT environment to intervene in the political, economic and social affairs of other nations in order to destabilize and interfere in their domestic systems and processes, sometimes even creating conflicts among nations, races and ethnic minorities. All in all, the ultimate goal is to create “information colonialism”.

4. **Unilateral coercive and other measures in the ICT environment**
   Restrictive measures against other States in the ICT environment and internet, such as: limiting and blocking IP addresses, restrictions to the registration of domain names and removal of popular apps from app marketplaces, also pose serious threats to the ICTs’ security,
confidence, trustability, use of technological dominance by some States in the global information space. It monopolizes the ICTs’ environment to limit other States’ access to advanced technologies, to increase their technological dependence and deepen information inequality, which all represent a serious threat.

States can exercise responsible behavior, realize their rights and accomplish their obligations in the ICTS environment if and when required capacities exist. This is, however, not realized unless technological, infrastructural and informational needs are met, including through the de-monopolization and facilitation of access to and transfer of new ICT-related science and technologies. The internet is a global resource, and digital restrictions/limitations have affected investment in ICT infrastructures as well as access to digital technologies, digital resources such as IPs and DNS systems and networks, all constituting as barriers for achieving national ICT-related development goals.

The current pandemic undoubtedly revealed the destructive effects of the irresponsible behaviors of state and non-state actors, including the use of platforms, for the individual and collective attempts by crisis-affected countries. A range of limiting and blocking measures and other coercive measures by those states and platforms that dominate the ICT environment and internet management have been in place for years targeting critical sectors such as energy, transport and banking. What’s more, the limiting and blocking measures are continued during the pandemic against Iranian public and private sectors, medical institutions, media, universities and research institutes, banking and telecommunications companies and operators in total violation of international law, principles of the Charter and human rights, including the right to development.

5. Threats arising from “contents”

There is a great concern over the use of the ICT environment through, inter alia, digital platforms and social media for hostile propaganda, misinformation, disinformation and cognitive operations against targeted countries which may intervene in their internal affairs, violate sovereignty and undermine their national security, national identity, integrity, culture and values as well as public order.
6. False flag operation in ICT environment (Hostile image-building and fabricated attribution)
   The anonymity in the ICT environment has given rise to the possibility of fabricated attribution. Some states are using fabricated image-building and xenophobia against targeted states with the ultimate goal of hostile policies and fabricated attribution. This poses a major threat against the peaceful nature of the ICT environment as well as international security.

7. Private sector conduct an ICT environment
   The decreased role of the States in the ICT environment vis-à-vis the role and effectiveness of the private sector poses a great threat to the ICTs' security, safety and integrity.

   States should ensure that the appropriate measures are taken to hold the private sector with extra-territorial impacts accountable for their behavior in the ITC environment, including its platforms. States must exercise due control over ICT companies and platforms under their jurisdiction. Otherwise, they are responsible for knowingly violating the national sovereignty, security and public order of other states.

8. Abuse of emerging technologies
   Attempts to abuse new and emerging science and technologies tend to cast a shadow over the peaceful applications of such technologies. This has revealed a range of potential risks and threats for individuals, societies, states and the international community.

9. Manipulating of ICT supply chains
   Manipulating ICT supply chains, including through implanting back-doors, to create vulnerability in products, services and maintenance constitutes a threat to state sovereignty and data protection.

Thank you!