Ø. General questions that States may wish to address during the general exchange of views:

1) Many States have called for an action-oriented approach. How can the OEWG be an action-oriented process and deliver tangible results to States while building on previous outcomes?
   First and foremost, referring to the “Many States” at the beginning of this question is a factual departure from previous outcomes. We are of the firm view that a selective approach would not facilitate our discussion in this important forum which has been established as an open, transparent, and all-inclusive UN body.
   The last OEWG report, including the Chair’s summary, reflects the fact that there are other States with different views on essential issues that have to be discussed comprehensively and agreed as the most important prerequisite before exerting to any action-oriented mechanism. We shall avoid impulsiveness at this stage and give ample opportunity to this new OEWG during its 5-year timetable to saturate its deliberation on unresolved core topics, including existing and potential threats, new norms, terminology, the applicability of international law, etc.
   It goes without saying that previous outcomes are clearly indicative of the fact that a large number of States support legally binding obligations to ensure the security and stability of the ICTs environment which is stated in paragraph 80 of the OEWG’s final substantive report. All proposals should be further considered in this OEWG established pursuant to General Assembly Resolution 75/240.

2) Are there specific issues that require urgent attention and early outcomes, bearing in mind the need to address all issues on the agenda in a balanced and comprehensive manner?
   - Since the lack of common understanding of terms and concepts constitutes a major potential source of mistrust in the ICT environment, we believe that the new OEWG should prioritize the pending issue of terminology. To this end, according to Resolution 75/240, a sub-group could be established early in the process to work on this important issue of terms, concepts, and terminology as a practical step for furthering international cooperation and building trust. We have explained in detail why the elaboration of
terminology as the element for describing the definition and criteria to deal with ICT security is absolutely needed in our submissions to the previous OEWG (Para. 29 of A/AC.290/2021/CRP.3* 10 March 2021)

- According to the UNGA resolution 75/240, the primary mandate of the new OEWG is to continue, as a priority, to further develop the rules, norms, and principles of responsible behavior of states and the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behavior.

- In the first OEWG’s discussions, many countries had put forward specific language proposals on the rules, norms, and principles of responsible State behavior which were contained in the Annex to its final substantive report as the Chair’s Summary for further consideration in this new OEWG as stated clearly in paragraph 80 of that report.

- It is Iran’s priority to formulate new norms in light of the 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 stand ready to exchange views and work for consensus with all parties in this regard in the new OEWG process.

3) **Given the unique role that stakeholders play in cyberspace, how can the OEWG engage them meaningfully and substantively in order to support discussions by Member States and deliver tangible results?**

The “intergovernmental” character of the OEWG should be preserved and respected with a view to availing all UN member states of the opportunity for interaction. Any contribution from the private sector, civil society, and academia to this intergovernmental mechanism can be made through informal consultative meetings with stakeholders, as occurred during the previous OEWG.

**I. Continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security,**
inter alia, data security, and possible cooperative measures to prevent and counter such threats:

1) Noting the extensive discussions on existing and potential threats, what are some examples of urgent and challenging existing and potential threats that States are facing?

A peaceful ICT environment can enforce international security and stability. This requires a more comprehensive approach to threats in the sphere of information security which addresses not only the digital infrastructure but also the content and information itself. Some examples of urgent and challenging existing and potential threats that States are facing are as follow:

1. Monopoly and hegemony in the internet governance;

2. Actions in the ICTs environment aimed at violating national sovereignty, interfering in the internal affairs, and undermining the political, economic, and social systems of other States, inter-alia through disinformation;

3. Threat or use of force against the sovereignty and territorial integrity or political independence of any state within and through ICT environment;

4. Unilateral coercive measures (UCM), including limiting and blocking, in ICT environment;

5. Excessive and politically motivated and fabricated attribution of attacks in ICT environment;

6. Lack of responsibility of private companies and platforms;

7. Applying double standards in safeguarding cyber security;

8. Manipulating of ICT supply chains, including through implanting back-doors, in order to create vulnerability in products, services, and maintenance compromising sovereignty, data protection, and data security of the target states;
9. Lack of a legally binding international instrument to regulate states and other stakeholders’ behavior in ICT environment;

10. Imbalanced development of different areas of international law in the ICTs environment, such as governance, cybercrimes, data protection, and data security.

2) **What capacities and structures are needed at the national level to prevent, detect, and respond to existing and potential threats? What can the OEWG do concretely to facilitate the building up of such capacities at the national level?**

States can exercise responsible behavior, realize their rights, and accomplish their obligations in cyberspace if and when required capacities exist.

This is, however, not realized unless technological, infrastructural, and informational needs are met, including through de-monopolization and facilitation of access to and transfer of new ICT-related science and technologies.

Restrictive measures against other States in the ICT environment, such as limiting and blocking IP addresses, restrictions to the registration of domain names, and removal of popular apps from app marketplaces, seriously affect existing capacities and efforts to build and develop the required capacities. Internet is a global resource and digital sanctions have affected investment in ICT infrastructures as well as access to digital technologies, equipment, and digital resources such as IPs and DNS systems and networks and digital forensic tools which constitute barriers for achieving national ICT-related development goals.

OEWG should focus on components of global architecture for capacity building under the auspices of the UN. This should guarantee a balanced, non-discriminatory, and demand-driven global cooperative arrangement for ICTs-related to capacity building ensuring also security, safety, and integrity of ICT supply chains.
II. Further develop the rules, norms and principles of responsible behavior of States and the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behavior:

1) Based on States’ experience in implementing the norms and taking into account previous OEWG and GGE reports, is there a need to further elaborate the existing norms or to consider the development of additional norms over time? If yes, what are the key issues that the OEWG should address?

The views of the Islamic Republic of Iran, in this very critical issue, has been elaborated in detail in our second submission dated 20 February 2020, in which we have indicated that prior to any discussion on the operationalization of any envisaged norms, as mandated by Para 5 of the resolution 73/27, further discussion is necessarily needed to further develop change or add to the 13 norms contained in Para 1 of the 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 terminology for their understanding on the list of terms, also the introduction of change to the identified norms to re-visit all those 13 norms and also the elaboration of additional norms.

We are of the view that significant reforming of current internet governance, open, fair, and non-discriminatory access of States to ICTs technologies, and a reliable cyber security supply chain are essential requirements for responsible behavior of States in the ICT environment.

Additional norms as we have indicated in our second submissions are including inter alia:
- The roles of States, with the primary responsibility for maintaining a secure, safe and trustable ICT environment, should be enhanced in ICT environment governance, including policy and decision making, at the global level. The envisaged governance should be realized in a manner that strengthens state sovereignty and shall not affect the rights of the states in making their choice of development, governance, and legislation models in the ICT environment.

- The principle of State sovereignty and international norms and principles that flow from sovereignty should be respected in ICT environment;

- 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;

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

- 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);

- States should ensure appropriate measures to make the private sector with extraterritorial impacts, including platforms accountable for their behavior in the ICT environment.

- States must exercise due control over its companies and platforms under their jurisdiction and control, otherwise, they are responsible for knowingly intervening in national sovereignty, security, and public order of other states;

- States should refrain from and prevent abusing ICT supply chains developed under their jurisdiction and control, to create or assist the development of vulnerabilities in products, services and maintain compromising sovereignty and data protection of the target states.

- Ensuring the balance between rights and responsibilities of States in the ICT environment.
Consequently, We regard that the implementation of the norms is yet premature as the new OEWG has to discuss above mentioned key issues to come up with a comprehensive consensus-based list of norms that may lead to the implementation stage.

III. How International law applies to the use of information and communications technologies by States:

1) How can the OEWG facilitate the further study of and discussions on how to deepen common understanding on how international law applies to State use of ICTs? Which specific rules and principles of international law applicable to State ICT use merit further study?

As cyber-enabling behavior differs from behavior in the physical world, the international law applicable to the use of ICTs may be different; however, nothing prevents the application of general principles of the UN Charter in the ICT environment. What is left is a legally binding instrument to fill the legal gaps arising from unique features of ICTs, including the wider possibilities for its use and misuse, from one side, and the other side, the limitations of existing international law. Such a binding framework may lead to more effective global commitments and a strong basis for holding actors accountable for their actions.

I. R. of Iran as a victim of the first well-known cyberweapon called Stuxnet, and as a country constantly experiencing cyber-attacks against its critical infrastructure, supports the establishment of an international legally binding framework to ensure prevention of the use of ICTs, including the internet for malicious purposes. The existing international law should be adjusted in a way to become applicable to the ICT environment.

Our delegation underlines that the following specific elements and principles, among others, merit further study:

- The envisaged cyber specific body of law should not be open to manipulation and biased interpretation by those who have dominance in the ICT environment, especially states with offensive cyber strategies and capabilities;
- States have rights and responsibilities in the ICT environment. On this basis, we believe the OEWG needs to highlight the rights of States with respect to the use and governance of ICTs;
- In their use of ICTs, States are committed to observing the applicability of the general principles of international law, including respect for State sovereignty, sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the sovereignty and territorial integrity or political independence of any State, or in any manner inconsistent with the purposes of the UN, and non-intervention and non-interference in the internal affairs of other States;
- The application of state sovereignty and international norms and principles that flow from sovereignty in ICT-related activities is crucial for safeguarding the peaceful and secure use of ICTS. The principle of State sovereignty in the use of ICTs should be elaborated in all dimensions.

2) What are other aspects the OEWG should consider with regard to this topic?

Cyberspace as a common heritage of mankind: The internet as a whole is the result of an accumulation of science, knowledge, innovation, investment, and techniques developed by all nations through recent history thus as a common heritage of mankind (CHM). As other common heritage of mankind, the envisaged international law should address, among others, its non-appropriation and shared governance; its integrity and states’ intrinsic right to access; its preservation and utilization for peaceful purposes; fair distribution of resources, including through multilingualism; and commitment to transfer of technology.

Responsibility and accountability of private sector: States have primary international responsibility for national and international activities of their private sectors and platforms under their jurisdiction or control with extraterritorial impact to ensure that those activities are carried out with the required authorization and supervision of the State; and don not undermine national security, identity, integrity, culture and values, and public order of other states.
IV. Confidence-building measures

1) What are other aspects the OEWG should consider with regard to this topic?

Trust and confidence-building measures (TCBMs) shall be built in the ICT environment to ensure maintaining its inherent peaceful and development-oriented nature. Measures to this effect shall be customized to the unique features of cyberspace.

ICT environment is a peaceful space and should be kept aside from the disarmament context. Reference to resolution 43/78 (H) may leave a false impression that cyberspace is recognized as a battlefield. CBMs have weaponry and military history and connotation and shall not be applied in cyberspace.

The OEWG should address the main sources of mistrust in the ICT environment, particularly the monopoly in the internet governance, anonymity, offensive cyber strategies, hostile image-building and xenophobia leading to unilateral coercive measures, and lack of responsibility of private companies and platforms and their national states for extraterritorial activities. For example, the departure point is to realize multilateral, fair, and transparent internet governance. Besides, those states with offensive cyber strategies shall unilaterally declare to refrain from offensive use of it.

Trust and Confidence building’s scope should be extended to areas such as national security; limiting, blocking, and coercive policies and measures against other states; crypto-currencies; ICT products, services, and contents; etc.

V. Capacity-building

1) Which areas of capacity-building support should be prioritized for early action or urgent implementation?

States can exercise responsible behavior, realize their rights, and accomplish their obligations in cyberspace if and when required capacities exist.
This is, however, not realized unless technological, infrastructural, and informational needs are met, including through de-monopolization and facilitation of access to and transfer of new ICT-related science and technologies. Restrictive measures against other States, including the limiting and blocking ones, in the ICT environment and internet, pose serious threats to ICTs development, security, and trustability and affects existing capacities and efforts to build and develop the required capacities.

Unilateral digital sanctions have been intensifying against some countries with direct negative impacts on their economic growth and development as well as the wellbeing of their people. The damaging health impacts of these sanctions during the covid-19 pandemic have been widely acknowledged including in UN reports.

Accordingly, in response to the above-mentioned question, our delegation is of the firm view that providing an open, fair, and non-discriminatory access to ICTs security-related science, technologies, products, and services should be prioritized for early action in the area of capacity-building and be included as a principle in the section of capacity building of any outcomes. Security should never be used as a pretext to hamper international cooperation on ICTs for peaceful purposes.

VI. Regular institutional dialogue

1) In the long term, how can a future regular institutional dialogue support action-oriented measures in view of the evolving peace and security threats posed by State use of ICTs?

The Islamic Republic of Iran continues to support the central role of the UN in advancing security in the ICT environment through international cooperation. The “intergovernmental” character of any regular institutional dialogue should be preserved and respected to avail all UN member states of the opportunity for inclusive, transparent, and open-ended participation, similar to the current OEWG.
We are of the view that a conflict-free, development-oriented, transparent, fair, moral, and peaceful cyberspace requires a legally binding instrument to fill the legal gaps arising from its unique features. Such a legally binding framework would lead to more effective global implementation of commitments and a strong basis for holding actors accountable for their actions.