Open-ended working group on:

Developments in the field of information and telecommunications in the context of international security

Submission by the Islamic Republic of Iran

I. Open Ended Working Group (OEWG)

1. The Islamic Republic of Iran supported, and welcomes, the establishment of the Open-ended working group on developments in the field of information and telecommunications in the context of international security. OEWG was long awaited to involve all State-actors in an issue with overarching influence on all aspects of human life. This intergovernmental process is a place to comprehend, in an inclusive and transparent manner, the outcomes and products of other mechanisms, including the GGEs, and align them with the international community's will and aspirations.

2. We appreciate efforts made to implement GA resolution 73/27 of December 2018 and its preceding ones since 1998, including through GGEs. However, and as we enter the era of OEWG, we see no need and justification to have a parallel GGE to work on the same mandate. This is why the Islamic Republic of Iran did not support resolution 73/266 of January 2019. The OEWG is currently the sole multilateral and inclusive intergovernmental body to address mandate under paragraph 5 of the resolution 73/27.

3. We welcome Swiss chairmanship of the OEWG, congratulate Ambassador Jurg Lauber on his election as our Chairman and assure

him of full support of the Islamic Republic of Iran to make the first OEWG a promising step forward.

4. In its work, OEWG should take into account that:

   i) ICTs environment, including internet, is a common heritage of mankind and need to be treated and governed through most inclusive States-led arrangements;
   ii) ICTs contribute to enhanced prosperity and development, culture, integrity, and security at all levels and shall be used properly and responsibly;
   iii) Malicious ICTs use generate threats not only to international relations and security but also to States' sovereignty, internal affairs, political stability, economic and social systems, national and cultural values, social integrity, etc.;
   iv) Security in cyberspace shall not undermine public order, moral and security of the societies;
   v) The existing international law should be adjusted in a way to become applicable to ICT environment;
   vi) Any rules, norms and principles aimed at ensuring responsible behaviour of States in ICT environment shall not undermine sovereign rights and jurisdictions of the States;
   vii) Private sector and social media platforms should be also accountable for their behavior in ICT environment;
   viii) Monopoly and restrictive measures against other States in ICT environment and internet pose serious threats to ICTs security and trustability and needs confidence-building measures;
   ix) Regional and international cooperation as well as national efforts to harness ICTs intrinsic benefits and advantages should be at the top of the agenda of any envisaged UN-led process(es), focusing, *inter alia*, on access to the technologies, infrastructures

and information needed by the countries, giving due account to the principle of common but differentiated responsibilities.

II. ICTs: opportunities and threats

5. Information and communications technologies (ICTs) entail enormous abilities and capacities for the common good of humankind, including for social and economic development of the countries, regions and the planet as a whole. Identically, failure to use ICTs peacefully presents serious threats to security and stability as well as economic development and prosperity of the nations. In other words, ICTs' realized opportunities enforce peace and security.

6. To the extent ICTs have influenced the individuals and societies, it has been influenced by values, cultures, knowledge, innovation and attitudes of different societies. This means that ICTs, including internet has been established on human platforms.

7. Accordingly, this is the sovereign right of all UN member States to invoke their rights and responsibilities to increase ICTs' incredible benefits and advantages and mitigate destabilizing impacts emanating from their malicious use.

8. The development-related dimension and the security-related concerns of ICTs shall be addressed in a balanced manner. While access to new information and communications science, technologies and techniques should be available to all countries, ensuring a secure, safe and stable ICT environment remains a shared but differentiated responsibilities of all stakeholders, with the governments taking the lead.

9. The rapid pace of their developments makes ICTs and ICTs-dependent critical infrastructures prone to sophisticated risks and threats which must be addressed technologically and legally through international cooperation between States with a view to finding effective and practical solutions that reduce risks and avert potentially catastrophic consequences.

10. The diverse and multiplied cyber actors and users have made the ICT environment a challenging one. This makes malicious use of ICTs a serious and impending threat of violating States' sovereignty and internal affairs. A number of States with subversive aims attempt to overtly or covertly use cyberspace to intervene in the political, economic and social affairs and systems of other States.

11. ICT environment is prone to weaponization if and when designed or used to inflict damage on the infrastructures of a State. Iran is among the first targets when attacked in Stuxnet case. Certain States with offensive doctrines violate the prohibition of the use of force against other countries as enshrined in the UN Charter. They shall assume responsibility for their acts which will undoubtedly result in the eruption of use of force by States in the not too distant future.

12. There is a dire need to address the existing and potential such threats including, but not limited to, through multilateral instruments and arrangements with a view to preventing conflicts and ensuring security aspects of ICT environment.

III. International Law applicable to the use of ICTs

13. We should recall that the development of existing international law preceded the advent of ICT environment and cyber warfare. Therefore, many questions exist on how to apply existing international law on

cyber activities that need to be clarified. This has to be done in an inclusive process with the participation of all States.

14. Those countries who have an explicit policy of seeking dominance and superiority in cyberspace aspire to maintain the status quo. They reject any step forward towards developing international legal norms as it would limit their freedom in the application of their offensive cyber capabilities against other States.

15. As a victim of cyber weapon, Iran rejects the status quo and supports the establishment of international legal rules and norms to ensure prevention of the use of ICTs, including internet for malicious purposes. The existing international law should be adjusted in a way to become applicable to ICT environment. The legal gaps should be filled by new international legal rules and norms.

16. In consideration of the applicable international law, the Islamic Republic of Iran's delegation underlines that the following elements, among others, should be taken into account:
    i. The applicable international law on ICT environment should not be open to interpretation.
    ii. 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.
    iii. In their use of ICTs, States are committed to observe the principles of the UN Charter, including respect for sovereign equality, the settlement of international disputes by peaceful means, the prohibition of the threat or use of force in any manner inconsistent with the purposes of the UN, respect for human rights and fundamental freedoms, and non-intervention and non-interference in the internal affairs of States.

IV. Rules, norms and principles for the responsible behaviour of States

17. States have a primary responsibility for maintaining a secure, safe and trustable ICT environment. This is why that discussions on common understandings on the nature and scope of the responsible behaviour in the ICT environment shall be guided by the principle of "state sovereignty" and rights, duties and jurisdictions that flow therefrom.

18. OEWG is currently the sole multilateral intergovernmental body in this regard. The OEWG should comprehend, in an inclusive and transparent manner, the inputs from previous attempts, including the GGEs, and align them with the international community's will and aspirations.

19. Any set of rules and norms of responsible behaviour of States should be developed in the context of their commitments to observe principles of the UN Charter, including respect for sovereign equality, settlement of international disputes by peaceful means, prohibition of the threat or use of force in any manner inconsistent with the purposes of the UN, respect for human rights and fundamental freedoms, and non-intervention and non-interference in the internal affairs of the states.

20. The envisaged rules and norms for responsible behaviour should strengthen international relations and security and prevent any threats and damage to States' sovereignty, internal affairs, political stability, economic and social systems, including the critical infrastructures, national and cultural values and social integrity.

21. Any set of rules and norms governing responsible behaviour of the States should be as effective as preventing cyber conflicts between

States, including legitimization of use of force, and weaponization of ICT environment.

22. Respect for human rights and fundamental freedoms helps ensure secure, stable and trustable ICT environment. However, these rights and freedoms should reinforce societal rights and values as well as public order, moral and security of the societies. Human rights and security of individuals in ICT environment should not be used as a disguise for violating rights and values of the States. Accordingly, the notion of human rights and fundamental freedoms in ICT environment should be developed in a way to ensure values and security of individuals, societies and States.

23. Rules and norms of responsible behaviour should be seen in way to balance "security" and "development" of nations. All States should have the right to supply chains, including ICT-related R&D as well as manufacturing, utilizing and transferring ICT products and services. Development of Technology, infrastructure, information and platforms should be done as per principle of "common but differentiated responsibilities".

24. Stakeholders rather than States also need to be observing principles, rules and norms for their responsible behaviour in ICT environment. Private sector and social media platforms should observe rules, norms and policies of the countries where they operate. States should also consider ways and means to hold them responsible.

25. Accordingly, serious substantive discussions are required to explore ways and means of developing international principles, rules and norms for maintaining a secure, safe, trustable, fair and ethical ICT environment.

V. Confidence-building measures

26. The Islamic Republic of Iran's delegation welcomes discussions on confidence-building measures in OEWG. We believe that cooperation in ensuring ICTs security may include voluntary CBMs in different forms and levels. This should take seriously into account the main sources of mistrust in ICT environment, including in internet.

27. We are of the view that the monopoly (in management) and anonymity (of persons and things) are the main sources of mistrust in internet, necessitating relevant CBMs. The first and foremost is to address the shortfalls and downsides of the current internet governance system with a view to realizing the long awaited fair internet governance.

28. ICT environment, including internet is the result of accumulation of science, knowledge, innovation and techniques developed by all nations through recent history, a clear manifestation of common heritage of mankind. Accordingly, there is a need to reverse the current situation in terms of governance through, *inter alia*, effective CBMs.

29. ICTs-based and ICTs-enabled limiting and blocking measures against other States constitute another source of mistrust which also affect effectiveness of CBMs. Besides the CBMs targeting monopolization of internet, we need CBMs and other measures to prevent and remove such restrictive policies and practices.

VI. International cooperation for Capacity-building

30. International cooperation on ensuring a secure, stable and safe ICT environment requires level playing field and conducive environment where States are in the position to exercise a responsible behaviour, realize their rights and accomplish their obligations. This attests to the

imperative of capacity building and capacity development schemes in ICT environment. This is not realized unless technological, infrastructural and informational needs are met, including through demonopolization and facilitation of access to and transfer of new information and communications science, technologies, etc.

31. Restrictive measures against other States, including the limiting and blocking ones, in 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. There is a need for concrete measures to remove the existing restrictive measure against countries and their possibility in future.

32. While taking into account the principle of common but differentiated responsibilities, capacity building and capacity development schemes should be demand–driven and need to be responded positively.

VII. Regular institutional dialogue

33. The ICTs and especially the internet is an inherently multilateral domain. In 1998, the first GA Committee began to discuss ICTs impacts on international peace and security. In parallel, the UN-sponsored negotiations on governance, technical and development aspects of ICTs, including internet, got momentum in ITU and WSIS Geneva and Tunis summits. The limited membership GGEs seemed to have been a deviation from the original international community's tendency to deal with this important global issue in the most inclusive manner. The OEWG is a promising step to bring back the issue on the right track, a UN-wide platform.

34. As we enter the era of OEWG, we see no need and justification to have a parallel GGE, with limited membership, to work on the same mandate. The OEWG is currently the sole multilateral intergovernmental body to address mandate under paragraph 5 of the resolution 73/27. This mechanism within the UN would allow all States to participate in the process of international norm-setting and rule-making, with respect to the security aspects of the use of ICTs.

35. The Islamic Republic of Iran supports the central role of the UN in upgrading security in ICT environment through international cooperation. Accordingly, any institutional dialogue to this effect should be inclusive and consensus-based. This is why we continue to support OEWG to fulfill its mandate.

September 2019