Open-ended working group on:

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

Second substantive session- February 2020

Second submission by the Islamic Republic of Iran

The Islamic Republic of Iran appreciates leadership of Ambassador Lauber in the OEWG process. We also appreciate his take-away from the first substantive session. However, the Islamic Republic of Iran would like to highlight the following observations:

There were views expressed by the delegation of Iran in the first substantive session which are not reflected in the Chair's take-away. These, among others, include:

- The imperative of peaceful nature of ICT environment which is guaranteed through observing principles such as non-interference in internal affairs, refraining from the threat or use of force in international relations, peaceful settlement of disputes, adhering to the well-established principle of peaceful coexistence of States, and preventing ICT environment from weaponization.
- The sovereign rights of the states and equality among them in the ICT environment.
- The need for a common understanding around concepts and terms used in the OEWG process, including through avoiding differences of terminology.

Furthermore, there was emerging consensus among participants in the first substantive session that OEWG is the first inclusive intergovernmental body dealing with the mandate given under Resolution 73/27; a process to engage all countries. It was also agreed that all UN-related bodies and processes need to contribute to OEWG work, ensuring a consensus-based comprehensive outcome.

This is also noticed that part of the OEWG's mandate, specified under resolution 73/27 is not given due attention in the Chair's working paper. For example, as regards "rules, norms and principles of responsible state behaviour", the OEWG is mandated "to further develop the rules, norms and principles of responsible behaviour of States listed in paragraph 1 above, and the ways for their implementation; if necessary, to introduce changes to them or elaborate additional rules of behaviour". While the OEWG does not start from the scratch, nothing prevent it from further work on the GGE findings. Accordingly, the Islamic Republic of Iran expects OEWG, as priority, to discuss and further develop, change, or add to the 13 rules, norms and principles as contained in paragraph 1 of the Resolution.

A. <u>Existing and potential threats</u>

As was generally agreed by the participants in the first substantive session of OEWG, ICT environment entails enormous opportunities and capacities for social and economic development, as well as safety, security and stability of the states. It is obvious that a peaceful ICT environment can enforce international security and stability. This requires a more comprehensive approach to threats in the context of international security. OEWG needs to contemplate on a range of existing and potential threats which in one way or another put at risk the peaceful, human and secure nature of the ICT environment.

We support the proposal by the distinguished Chairman of the OEWG to discuss in the second substantive session any other existing or emerging threats that have not been considered so far. A "peaceful" and

"development-oriented" approach to international security also requires OEWG to re-visit the threats already identified by other fora, including GGEs.

As regards other existing and emerging threats, the followings deserve careful attention by OEWG:

1. **Threat or use of force in 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 ICT environment. However, a number of states are developing ICT's capabilities for weaponization purposes which is reinforced by their offensive hybrid doctrines aimed at resorting to cyber and kinetic operations. This has made ICT environment prone to become a new arena of battlefield, a potential threat to the prohibition of the threat or use of force against the territorial integrity or political independence of other states.

2. **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 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 ICT environment.

In the recent history, states with subversive aims attempt to overtly or covertly use ICT environment to intervene in the political, economic and social affairs of other nations with a view to destabilizing and interfering in their domestic systems and processes; creating conflicts among nations, races and ethnic minorities. All in all, the ultimate goal is to create "information colonialism".

3. **Unilateral coercive and other measures in ICT environment**

Enforcement of national rules and jurisdiction with extra-territorial impacts, monopoly, and double standard in policy and decision making in internet governance have given rise to unilateral discriminatory and coercive measures against other states. This has in turn entailed, among others, limiting and blocking measures as well as discriminatory policies in terms of access to ICT-related science, investment and technologies, including operational technologies and systems.

4. **Threats arising from "contents"**

There is a great concern over the use of ICT environment through, inter alia, digital platforms and social media for the purpose of hostile propaganda against target countries which may intervene in their internal affairs, violate sovereignty, and undermine their national security, national identity, integrity, culture and values, and public order.

5. **Hostile Image-building and fabricated attribution in ICT environment**

The anonymity in ICT environment has given rise to possibility of fabricated attribution. Some states are relying their offensive doctrines, policies, measures and operations against target states on fabricated image-building and xenophobia, with an ultimate goal of hostile policies and fabricated attribution. This poses a major threat against peaceful nature of ICT environment as well as international security.

6. **Imbalance between role and responsibility of states and those of private sector**

The decreased role of the States in ICT environment vis-à-vis the role and effectiveness of the private sector pose a great threat to the ICTs security, safety and integrity.

Lack of rules, norms and principles governing activities of private sector, including companies and platforms, have made their activities a major potential threat against national sovereignty, security and public order as well as societal rights and interests of the states where they operate; trust and integrity (of data, process and components); as well as privacy of end users.

In their activities in the ICT environment, including operational technologies and systems, private sector could also be abused by their national governments, including as proxies, to impose their policies against other countries.

7. **Abuse of emerging technologies**

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

8. **Abuse of ICT supply chains**

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

B. <u>Norms, Rules and principles for the responsible state behaviour</u>

The OEWG, as the first inclusive intergovernmental body dealing with the mandate given under Resolution 73/27; has provided countries, particularly those whose voice had not been yet heard, with an opportunity to contribute into identification of "***norms, rules and principles***" for the responsible state behaviour. Accordingly and as specified under paragraph 5 of the resolution 73/27,[1] while the OEWG does not start from the scratch

[1] "to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States listed in paragraph 1 above, and the ways for their implementation; if

as stressed in Chair's working paper, nothing prevent it from further work on the GGE findings.

By the same logic, prior to any discussion on "awareness-raising" and "operationalization" of envisaged norms, the OEWG needs to agree on the final and comprehensive list of the norms. The Islamic Republic of Iran expects OEWG, as mandated by paragraph 5 of the resolution 73/27, to discuss and further develop, change, or add to the 13 norms contained in paragraph 1 of the resolution 73/27. In doing so, the Islamic Republic of Iran proposes to structure discussions on the 13 norms in the upcoming sessions of the OEWG around the following lines:

1. **Ambiguities:** To "***further develop***" the norms, OEWG should address ambiguities associated with the understanding of the identified norms.
2. **Terminology:** To understand better, and avoid further ambiguities, OEWG may work on a list of agreed terms.
3. **Introduction of changes:** To ensure a comprehensive consensus-based OEWG's outcome on the norms, and given the fact that most of the OEWG's participating states were absent in the previous processes, it is necessary for the OEWG to allocate sufficient time on re-visiting each and every single 13 identified norms. The Islamic Republic of Iran will submit its proposed changes in due course.
4. **Elaboration of additional norms:** As partly reflected in the Chair's working paper, there are issues not sufficiently covered by the 13 identified norms. Therefore, OEWG needs to focus on the additional norms necessary to address other areas of responsible behaviour.

necessary, to introduce changes to them or elaborate additional rules of behaviour;"

As regards **implementation**, the Islamic Republic of Iran deems it premature for OEWG at this stage to discuss "Implementation" of norms-under-discussion. This is obvious that only a comprehensive consensus-based list of norms can lead to "implementation" stage.

The Islamic Republic of Iran will actively contribute into OEWG discussions on the above-mentioned lines. These include, among others, concrete proposals on additional norms such as:

- *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 global level. The envisaged governance should be realized in a manner which strengthen state sovereignty and shall not affect rights of the states in making their choice of development, governance and legislation models in the ICT environment.*
- *States should refrain from the threat or use of force against the territorial integrity or political independence of any state within and through ICT environment.*
- *No state has the right to intervene through cyber-related ways and means, directly or indirectly and for any reason, in the internal or external affairs of other states. All forms of intervention 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 tools 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 with a view to making private sector with extra-territorial impacts, including platforms, accountable for their behaviour in the ITC environment. States must exercise due control over ICT companies and platforms under their*

jurisdiction, otherwise they are responsible for knowingly violating national sovereignty, security and public order of other states.

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

In order to ensure a peaceful, fair, moral and development-oriented ICT environment which is also free from crimes, violation and conflict, OEWG should stimulate an ICT environment discourse evolving around the "ICT peaceful nature" as its nodal point.

The above proposed norms along with any other norms to be identified in OEWG process should evolve around this nodal point. Accordingly, discussions on issues such as prohibition of threat or use of force, non-interference in internal affairs, and cyber capabilities for weaponization of ICT environment should contribute in this regard. This requires that, among others and as first step, those states with offensive cyber strategies or policies revert to this discourse. These states, either those who have declared such capabilities or those with evidence to this effect, shall unilaterally declare to refrain from offensive use of ICTs.

This should also be highlighted that this discourse, while addressing the notion of human rights and fundamental freedoms in ICT environment, should strike a balance between rights and freedom of individuals with States' national security and interests, social ethics, and public order.

C. <u>International Law</u>

The applicability of existing international law in cyber-related areas is still an unclear domain. OEWG should continue to shed more light in this regard in a way that ensures interests and meets concerns of all states. The envisaged international law should provide a legal multilateral and inclusive framework for the peaceful ICT environment discourse as

explained above. Pending realization of principles and primary rules of such international law, this is premature to discuss secondary rules. This is also imperative to observe that the existing international law should not be open to biased interpretation which negatively affects the peacefulness of the ICT environment.

Notwithstanding the noble principles of 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, there is a strong need for developing complementary cyber-specific international law which addresses the issues such as jurisdiction and conflict of laws.

The internet as a whole is the result of accumulation of science, knowledge, innovation, investment and techniques developed by all nations through recent history thus a common heritage of mankind (CHM).

As other common heritages 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.

The envisaged international law should also support regional and international cooperation to disseminate fairly and effectively the ICTs-based opportunities and interests and development dividends. This should be based on the principle of common but differentiated responsibilities (CBDR).

D. Confidence-building measures

The OEWG should first and foremost address the very sources of mistrust in ICT environment, including in internet. The monopoly (in

management) and anonymity (of persons and things), offensive cyber strategies and policies , hostile image-building and xenophobia leading to unilateral coercive measures, and lack of responsibility of private companies and platforms and their national states for extra territorial activities are among the main sources of mistrust in ICT environment which requires remedial actions. For example, the departure point is to realize a multilateral, fair and transparent governance. Besides, those states with offensive cyber strategies shall unilaterally declare to refrain from offensive use of ICTs.

Some regions have already started to implement some regionally developed measures for building confidence. This is not, however, prelude to any perceived global arrangement. At this stage, states should in return focus on bilateral arrangements and agreements.

E. Capacity-building

ICTs-related capacity building has yet to experience a balanced, non-discriminatory and demand-driven approach. This is against the fact that capacity building is among the few areas where meaningful cooperation can be developed at bilateral, regional and global levels. The discussions in the first OEWG substantive session attested to this conducive cooperative context.

At the global level, UN and its specialized agencies are expected to take the lead role in capacity building in ICT environment and applications, and those ensuring security, safety and integrity of ICT supply chains. This should entail planning, monitoring and implementing capacity building schemes. At regional level, despite a range of schemes with specific components and scope, there are still countries and sub-regions which have been ignored.

UN should facilitate and encourage sub-regional and regional schemes with the widest participation of demanding states. Having in mind the "positive discrimination" approach, the Islamic Republic of Iran has the capacity to engage in programmes at regional, sub-regional and bilateral

levels, including through contribution into programmes for disadvantaged countries and regions.

F. Regular institutional dialogue

The Islamic Republic of Iran continues to support the central role of the UN in addressing challenges and opportunities of ICT environment, including through devising a fair, transparent and global architecture for internet, including its development and management. Accordingly, any institutional dialogue should be inclusive and consensus-based. The OEWG is the first multilateral and inclusive intergovernmental experience to compensate asymmetric and fragmented efforts so far made through other foras.

The "intergovernmental" character of the OEWG or any alternative institutional mechanism should be preserved and respected with a view to availing UN member states of the opportunity for interaction. Any contribution from private sector, civil society and academia into intergovernmental machinery shall come through other mechanisms such as Internet Governance Forum (IGF).

As the establishment of OEWG has been widely welcomed by the UN member states and given the wide scope and diversity of its mandate, the OEWG needs to continue its work until and unless another inclusive institutional UN mechanism is agreed. Accordingly, we expect the distinguished OEWG Chairman to present, as part of his report to the 75th session of the General Assembly a roadmap for beyond 2020. The envisaged roadmap may foresee establishment of subsidiaries to facilitate and expedite its work. Moreover, there is also a need for OEWG to receive contribution from other UN-related bodies and processes to ensure a consensus-based comprehensive outcome.

February 2020