In the Name of God

Iran's submission

to the seventh substantive session of the Open-Ended Working Group on the security of and in the use of information and communications technologies 2021-2025 (OEWG)

4 - 8 March 2024, United Nations Headquarters (UNHQ), New York

On

International Law

Mr. Chair,

In response to your guiding question about identifying further convergences on topics contained in the non-exhaustive list in sub-paragraphs 29(a) and (b) in the Second APR, I would like to highlight that discussions in the OEWG have clearly demonstrated that significant convergence has already been achieved within the international community concerning the topic outlined in subparagraph 29(b)(i) regarding the development of additional legally-binding obligations. The rationale behind this assertion is that the Non-Aligned Movement which is a forum of 120 countries (two-thirds of UN Member States) in its Working Paper submitted to the first OEWG has acknowledged the need to identify legal gaps in international law through the development of an international legal framework specific to the unique attributes of the ICT

environment.[1] I wish to recall that NAM includes two-thirds of UN Member States and as highlighted by one colleague in a separate meeting, almost 70 percent of Oxygen in any room within the UN is generated by NAM.

In the sixth substantive session of the Open-Ended Working Group (OEWG), my country as a victim of the first well-known cyber weapon, called Stuxnet, and as one of the proponents of such a legally binding instrument, thoroughly detailed the rationale and addressed the concerns articulated by those in opposition. I take this opportunity to kindly invite other delegations to study this document which is available on the OEWG website.

We would also like to highlight that a proposal, presented by the Russian Federation and co-sponsored by a group of countries, is reflected in annex D of the Second Annual Progress Report (APR), titled "Updated Concept of the Convention of the United Nations Ensuring International Information Security."

Mr. Chair,

[1] Paragraphs I.4(a) and II.11 of the “NAM Working Paper for the Second Substantive Session of the Open-ended Working Group on developments in the Field of Information and Telecommunications in the Context of International Security (OEWG)”, April 2020.

We are of the view that a scenario-based discussion mentioned in your guiding questions constitutes a fruitful approach for fostering a deeper understanding of the necessity to develop a legally binding instrument related to Information and Communication Technology (ICT) security. Through the presentation of hypothetical scenarios, States can scrutinize the adequacy of existing legal frameworks and deliberate on whether a more comprehensive and legally binding instrument on ICT security is imperative. scenario-based exploration allows for an inclusive assessment of the current legal landscape and facilitates informed discussions on the need for enhanced measures in addressing ICT security challenges.

Mr. Chair,

The application of the Purposes and Principles of the UN Charter extends to the domain of Information and Communication Technologies (ICTs). My delegation seeks to share additional insights into the principles of sovereignty, sovereign equality, and non-intervention in the internal affairs of other States, as outlined below, to enhance our common understanding and facilitate the identification of additional convergences about those principles contained in the non-exhaustive list in subparagraph 29(a) in the second APR.

Sovereignty:

- Territorial sovereignty and national jurisdiction apply over cyberspace and all its elements, including States' cyberinfrastructure (CI & CII), cyber equipment, and data originating or ending in their territory or the devices under its control or in their adjacent area;
- Any use of cyber coercion with physical or non-physical effects - or having such potential – which is a threat to national security or may lead to political, economic, social, and cultural destabilization, constitute a violation of the State sovereignty, whether committed by states or other actors. Therefore, 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 do not undermine national security, identity, integrity, culture and values, and public order of other states.

Sovereign equality:

- The customary rule of sovereignty is not limited to Article 2 (1) of the UN Charter which articulates one aspect of sovereignty;

- All States, regardless of size, wealth, or strength, are equal before the law and have the right to participate on an equal footing in international ICT affairs, including Internet governance.

Non-intervention:

- The prohibited intervention also includes situations in which the measures (cyber/non-cyber) are implemented in order to interfere in internal and/or external ICT affairs of the other state;
- All forms of overt, subtle, and highly sophisticated techniques of coercion, subversion, and defamation (cyber/non-cyber) aimed at disrupting the political, social, cultural, or economic order of other States is unlawful;
- Every state enjoys the inherent right to fully develop its information system without interference and to use its information system in order to promote its interests. Any measures that impede, interrupt, or limit the operation of information transmission means and systems, utilized for the control and exercise of the state's sovereignty, are considered unlawful.

Mr. Chair,

We assert that the ICT environment, encompassing the internet in its entirety, constitutes a common heritage of mankind (CHM). As a result, we advocate for the application of principles such as non-

appropriation and shared governance, integrity, the intrinsic right of states to access, preservation, and utilization for peaceful purposes, fair distribution of resources, and transfer of technology.

Thank you, Mr. Chair.