Statement

Mr. Heidar Ali Balouji

First Counselor

of the Permanent Mission of the Islamic Republic of Iran to the United Nations

at the UNGA OEWG on ICTs

All Agenda Items

6-10 March 2023, New York/ the United Nations

In the Name of God, the Most Compassionate, the Most Merciful

Existing and Potential Threats

Mr. Chair,
My delegation joins others to express our continued support for your leadership and the efforts of your team as well as the secretariat in heading the Open-Ended Working Group on Security and the Use of Information and Communication Technologies. We are committed to engaging constructively to achieve a positive outcome for the OEWG.

Mr. Chair,
Throughout the previous and current OEWG, some States, including mine, have suggested specific threats emanating from the misuse of ICTs which were not reflected in the 2021 OEWG final report and the first APR of the current OEWG.

My delegation would like to take this opportunity to once again refer to the following threats, and we hope that they will get reflected in the next Annual Progress Report:

1. Use of ICTs to destabilize and interfere in the States' domestic systems and processes and create conflict among nations, races, and ethnic minorities;
2. Unilateral coercive measures against States in the ICT domain;
3. Disinformation campaigns, fabricated image-building, and xenophobia against States through the use of ICTs;
4. Lack of responsibility of the private sector and platforms with extraterritorial impact in the ICT domain.

Last but not least, my delegation would like to express appreciation for a number of relevant proposals put forth by some delegations. We reserve the right to provide proper feedback on these proposals or others to be made in due course.

Mr. Chair,

On another note, we reject the unsubstantiated allegations made by the US delegate against Iran. We would like to highlight that it is irresponsible for a country that besides an offensive cyber program, it has maliciously initiated and supported numerous cyber-attacks against different Iranian facilities, including by the notorious Stuxnet malware causing the first ever cyber-Hiroshima in the world, to raise such accusations. The US must be held accountable for its malign activities in the cyber domain and other fora.

Finally, we will share our statements at the end for your consideration.

++++++++++++++++

Norms, Rules and Principles

Mr. Chair,
Resolution 75/240 entrusts the OEWG to prioritize the further development of rules, norms, and principles for the responsible behavior of states, and to

introduce changes or additional rules if necessary. We note that the norms in the 2015 GGE report are insufficient for regulating the ICT environment comprehensively. Therefore, it is crucial to continue developing a universal, comprehensive list of rules, norms, and principles. The first OEWG's Chair's Summary annex proposes additional norms, which highlights the incomplete work on norms in the past, as recognized in paragraph 80 of the previous OEWG's final report.

We believe that implementing rules of behavior prematurely will not have the expected effect unless they have universal and obligatory character. In response to your guiding questions, we believe that a comprehensive and conflict-free cyberspace requires a set of universal, binding norms and we have been persistently supportive of the idea of a legally binding instrument at the global level. The sooner the better and in this vein, before any discussion on operationalizing the norms, the OEWG needs to agree on the final and comprehensive list of them. The OEWG should also elaborate on ways to regulate IT companies in the digital sphere and formulate rules for responsible behavior on digital platforms, social media and networks, as well as the stakeholders. The private sector and social media platforms should observe the rules, norms, and policies of the countries where they operate. States should consider ways to hold them responsible.

In addition to our submissions in 2020 during the previous OEWG, and echoing some other delegations, we propose the following norms:

1. Enhance the role of states in governing the ICT environment, including policy and decision-making, at the global level, while maintaining state sovereignty and respecting states' rights to make decisions for the development, governance, and legislation models in the ICT environment.
2. Prohibit states from intervening through cyber means, directly or indirectly, in the internal or external affairs of other states.
3. Condemn and prevent all forms of interventions, interference, or attempted threat against political, economic, social, and cultural systems, as well as the cyber-related critical infrastructure of the states (UNGA resolution 2131 of 21 December 1965).
4. Prohibit states from using ICT advances as a tool for economic, political, or coercive measures, including limiting and blocking measures against targeted states (UNGA resolution 2131 of 21 December 1965).

5. Ensure that the private sector with extraterritorial impacts, including platforms, is held accountable for their behavior in the ICT environment.
6. Hold states responsible for knowingly intervening in the national sovereignty, security, and public order of other states if they fail to exercise due control over their companies and platforms under their jurisdiction and control.
7. Refrain from and prevent the abuse of ICT supply chains developed under their jurisdiction and control to create or assist in the development of vulnerabilities in products, and services, and maintain compromising sovereignty and data protection of the target states.

We need the OEWG to discuss these proposed norms, address any ambiguities in terminology, and make necessary changes while also introducing additional norms to ensure a comprehensive list.

++++++++++++++++++++++++

International Law

Mr. Chair,
When discussing international law and cyberspace, some countries claim that existing international law can be applied to cyberspace, rejecting the need for new laws. However, opinions differ on how to apply international law to cyberspace and whether it is adequate. Despite repeated arguments, a definitive answer to this issue remains elusive. Furthermore, the prevalence of cyber-attacks raises serious questions and doubts about the sufficiency of current international law in addressing these issues.
To address this, a legally binding document is required to define and compile necessary terminology, including cyber weapons, cyber-attacks, the responsibility of non-state actors in cyberspace, prevention of use or threat to use of force, peaceful settlement of disputes, attribution and last not least, the topic of international cooperation. Beside many advantages including contributing to a concrete safe cyber space, this will lead to a common understanding of the issue.
Mr. Chair,
During the first annual progress report of the OEWG, States proposed an open and non-exhaustive list of topics for further discussion under international law. It was recommended to engage in focused discussions on

these topics from the non-exhaustive list, as well as proposals contained in the 2021 OEWG report and Chair's summary, where relevant, during the fourth and fifth sessions of the OEWG.

To implement this recommendation, the OEWG must ensure all topics of the non-exhaustive list, as well as proposals contained in the 2021 OEWG report and the Chair's summary, are discussed in a balanced and equal manner. A selective approach to these topics is not acceptable.

Therefore, by the non-exhaustive list of topics adopted in the Annual Progress Report in paras. 15 a, 15 b, and statements made under the agenda item "international law," as well as national positions published by Member States, we suggest that the following topics be prioritized for further focused discussions during the 2023 sessions of the OEWG:

1. The possibility of additional legally binding obligations: The Non-Aligned Movement, with 120 member states, 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 in its Working Paper[1] submitted to the first OEWG. Therefore, this topic deserves further consideration.
2. Principle of Sovereignty guided and aligned with by the principles of sovereign equality; States territorial sovereignty and national jurisdiction over their cyberspace, ownership, leadership and taking into consideration States' national priorities in policy making.
3. Principle of non-intervention in the internal affairs of other States: Views on what constitutes a violation of the principles of sovereignty and non-intervention in cyberspace differ, and therefore, it needs further discussion in the OEWG.

Finally, regarding the suggestion to convene hybrid meetings, my delegation cannot support any proposal that contradicts the modalities adopted for the OEWG and the UN practice, which emphasize the importance of holding formal meetings in person.

++++++++++++++++++++++++

[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.

CBMs

Mr. Chair,
I will have another statement on POCs when you open that agenda item.

In the meantime, and in response to your first guiding question on confidence-building measures, my delegation would like to point out that producing a consensus glossary of terminology is one of the concrete and specific CBMs. Some regional organizations have adopted a similar approach in the ICT security domain. This experience could be universalized in an inter-governmental context.

The idea and the value of developing a universal terminology in the field of ICT security have been discussed and highlighted during the current and previous OEWG as a practical step for furthering international cooperation and building trust.

The first annual progress report of the OEWG has invited the States to share their national views and definitions of technical ICT terms to promote mutual understanding.

While we welcome this recommendation of the ARP as an initial and first necessary step, we believe that to reduce the risk of misunderstandings in the absence of an agreed terminology, the OEWG could take more concrete steps forward and incorporate it into its future Annual Progress Report the recommendation of developing a universal terminology in the field of ICT security.

Mr. Chair,
From our viewpoint, a step-by-step approach highlighted by you and many delegations at the informal inter-sessional meetings in December 2022 as well as the current substantive session could also be applied to the elaboration of a universal terminology in the field of ICT security. The OEWG could start by preparing a list of terms used in consensus UN documents and then proceed to agree upon definitions of the basic terms from this list (for example, ICTs, ICT infrastructure, ICT environment, malicious use of ICTs, etc.).

Mr. Chair,

Let me take this opportunity to highlight that restrictive measures against other States in the ICT environment pose serious threats to trust and confidence in the ICTs environment. It is an important confidence-building measure that States refrain from adopting any measure to restrict or prevent universal access to the benefits of ICTs.

++++++++++++++++++++++++++

Capacity Building

Mr. Chair,
Despite the conclusion of paragraph 61 of the 2021 OEWG report in which States recalled the need for a concrete, action-oriented approach to capacity-building, it is very regretful that during the third substantive session of the OEWG, the capacity-building section of the 2022 APR was significantly undermined and reduced to mere coordination among existing initiatives.

Mr. Chair,
Considering the essential role of the UN in the efforts to ensure the security of and in the use of ICTs, existing capacity-building initiatives in this area should complement the work done at the OEWG, not vice versa.

Therefore, we still believe that the idea of establishing a well-funded "permanent mechanism for capacity-building for ICTs within the UN" does have considerable merits which should be discussed by the current OEWG. We suggest that this be reflected in the upcoming APR, with an emphasis on initiating administrative work in the immediate financial program of the United Nations. We agree with your enlightenment that given the urgent needs in this area, there is no need to delay any further.

This mechanism which is fundamental to enabling developing countries in the ICT domain could include, inter alia, some concrete measures which have been already identified by consensus in paragraphs 59 to 61 of the 2021 OEWG report. These measures are as follows:

1. Development of national cyber security strategies;
2. Providing access to relevant technologies - in this regard, my delegation would like to recall that the need to facilitate access to technology is also one of the capacity-building principles identified by the 2021 OEWG report;

3. Support to Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs);
4. Establishing specialized training and tailored curricula including “training the trainer” programs and professional certification;
5. Establishing platforms for information exchange including legal and administrative good practices;
6. Building expertise across a range of diplomatic, legal, policy, legislative, and regulatory areas;
7. Developing diplomatic capacities to engage in international and intergovernmental processes;
8. Enabling States to identify and protect national critical infrastructure and to cooperatively safeguard critical information infrastructure;
9. Deepen States understanding of how international law applies to the cyber domain; and
10. Contributions of other relevant stakeholders - including developed countries, industry, academia and private sector- to capacity-building activities with a demand driven basis and in an adequate, accessible and sustained manner.

We appreciate all valuable initiatives, including the UN - Singapore fellowship program in promoting capacity building for developing countries. Further, we are of the view that the OEWG could also consider the potential of the International Telecommunication Union (ITU) as the United Nations specialized agency for information and communication technologies, tasked to leverage capacity-building besides its other functions.

Mr. Chair,
Lastly, restrictive measures against other States in the ICT environment, such as limiting and blocking of IP addresses, restrictions to the registration of domain name, and removal of popular apps from app markets, pose serious threats to ICTs development, security, and trustability and affects existing capacities and efforts to build and develop the required capacities. The damaging health impacts of these sanctions during covid-19 pandemic have been widely acknowledged, including in UN reports. Therefore, there is a need for concrete actions to remove the existing restrictive measure, including unilateral coercive measures, against countries and their possibility in the future.

++++++++++++++++++++

RID

Mr. Chair,
According to resolution 75/240 which was acknowledged by consensus resolution 76/19, establishing a regular institutional dialogue with the broad participation of States, under the auspices of the United Nations, is one of the key mandates of the current OEWG.

Paragraph 77 of the 2021 OEWG and paragraph 18 (b) of the APR acknowledge that a variety of proposals for advancing responsible State behavior in the use of ICTs were put forward. According to the First annual progress report recommendation, States should continue exchanging views at the OEWG on regular institutional dialogue and on proposals by States to facilitate regular institutional dialogue on the security in the use of ICTs. Therefore, the Programme of Action should be discussed within the OEWG on an equal footing with other States' proposals.

Mr. Chair,
It is our well-known position that replicating the model of the UN PoA on Small Arms & Light Weapons, which has not yet proven its effective value in preventing, combating, and eradicating the illicit trade of SALWs, does not serve the purpose of the ICT security. Procedural approaches such as POA are inherently challenging and instead, we should move towards legally binding instruments on cyber security. 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.

Mr. Chair,
In response to your guiding question, we believe that any future mechanism for regular institutional dialogue on the ICT security within the UN should be intergovernmental, consensus-based, democratic, transparent, and non-political and should take into account the concerns and interests of all States through equal State participation in a fair and balanced manner.

It would also be essential to resume the practice of paragraph-by-paragraph negotiation exercises on any outcome document on the regular institutional dialogue in the field of ICT security.

Interaction with non-state actors within the future body should be consultative and informal; only accredited non-state actors will be able to

participate, upon invitation and without the right to vote, in formal sessions as observers.

++++++++++++++++++++++

POCs

Mr. Chair,
My delegation would like to thank you for preparing the new version of the non-paper on the key elements for the development of the POC Directory which could facilitate our discussions during the current session of the OEWG.

Mr. Chair,
We welcome the revised non-paper which has been significantly improved compared to the previous one. However, to make the POC Directory more efficient, we have the following comments.

We note that the new para 2bis reflects some working principles for the future global POCs directory. This important element could be extended to include some other principles which have been proposed by States throughout the previous sessions of the OEWG, as well as through the written inputs to the Secretariat.

These working principles could include, inter alia, the following:

1. Functions of the POC Directory will be guided by the principles of non-intervention in the internal affairs of other States, along with sovereign equality, States territorial sovereignty and national jurisdiction over their cyberspace as a fortiori all its elements, as well as peaceful settlement of disputes;
2. Given that ICT incidents can emanate from or involve third States, it is understood that notifying a State about malicious cyber activity emanating from its territory or cyberinfrastructure, does not imply the responsibility of that State for the incident. It is particularly important given the fact that many cyber-attacks are carried out under “false flags”;

3. Acknowledging the receipt of this notice does not indicate concurrence with the information contained therein;
4. Notification from an affected State must be made in good faith and should be accompanied by all relevant supporting information. Supporting information may include sharing possible Indicators of Compromise (IoCs), such as IP addresses and computers used for malicious ICT acts and malware information;
5. A State that becomes aware of harmful ICT activities emanating from its territory but cannot respond, is not responsible based on the principle of common but differentiated responsibilities (CBDR) and should be assisted by technology transfer and forensic tools to combat the ICT malicious activities;
6. The PoCs and their resources should not be subject to restricting and blocking measures, including UCMs (unilateral coercive measures);
7. Concerning the activities of the PoCs Directory, States will take into account the needs and requirements of developing States taking part in such collaborations;

Mr. Chair,
Since States may, voluntarily, provide both diplomatic and technical POCs to the directory, to avoid inconsistency and duplication of work, we believe that the revised non-paper should contain a clear reference to the specific functions of each diplomatic and technical POCs.

Mr. Chair,
Regarding the information protection that has been reflected in para 4 (b) of the non-paper, we think that the password protection would not be sufficient to ensure the security of the POC directory and other protection methods such as Multi-factor Authentication (MFA) should also be used.

Mr. Chair,
Last but not least, we welcome the improvement of a capacity-building section in your revised non-paper. Capacity-building is an essential element of the POC Directory and is required for the effective functioning of this mechanism.

Considering that operationalization of the POC directory may not immediately be possible, in particular for developing countries until they acquire adequate capacity and functional equivalence, we propose the following amendments:

In para 9 (e), it would be more appropriate to request the UN Secretariat to seek views from States on (a) capacities required for effective participation of POCs in the POC Directory; and (b) suitable mechanisms and actions for building such capacities and then produce a background paper on these views. This background paper needs to be prepared by the end of June 2023 for consideration at the fifth session of the OEWG.

We believe that proposed focused discussions in para 9 (g) on potential follow-up actions drawing upon the information presented in the Secretariat's background paper could not be postponed till forthcoming sessions of the OEWG and should take place and finalize during the fifth substantive session of the OEWG in July 2023. Also, the interjectory statement "if any" in the same sub-paragraph is a prejudgment about the outcomes of the proposed focused discussions on the background paper and should be deleted.

I would like to express my delegation's gratitude for all the constructive proposals that were presented during this week's proceedings. As stated in my initial statement, we reserve the right to provide comprehensive feedback at an appropriate time.

In addition, I would like to reiterate that we will be submitting all of our statements in writing for your consideration and posting them to the relevant portals and websites.

I thank you, Mr. Chair.