Republic of Korea, 26th July 2022 (check against delivery)

Third Substantive Session of the 2nd Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security

[Introduction]

Mr. Chair,

Let me begin by thanking you the Chair and the Secretariat for organizing this session, and for the effort in drafting the Open-ended Working Group's first annual progress report that reflects our lengthy discussions during the last two sessions.

As my delegation highlighted at the first session of this OEWG, this five year process is at once a continuation of our past achievements as well as a new chapter for further progression. In this regard, we believe the revised draft dated 20th July serves as a good basis for our deliberations during this week.

We welcome the introductory paragraphs 1 to 6 of the Draft, in particular their mentioning of the *acquis* of cyberspace including the 11 norms of responsible state behavior, the OEWG's commitment to meaningful stakeholder engagement, and recognition of the role of regional organizations as well as participation of women delegates in its discussions.

Lastly, my delegation would like to extend a warm welcome to the multi-stakeholders present at this third session. My delegation notes the efforts made by the OEWG to provide greater opportunities for their participation, and looks forward to further engaging them in a more meaningful and substantial manner, so that we can incorporate in our discussions the valuable and varied expertise and experience of these stakeholders.

[Existing and Potential Threats]

Mr. Chair,

The last two sessions were a valuable opportunity for all member states to understand how each of us perceives threats in the ICTs environment.

We believe that paragraph 7 reflects the concerns raised by States regarding the growing and evolving nature of threats in the cyberspace in an appropriate manner, as well as the importance of fostering stronger cooperation between cyber emergency response teams, also known as CERTs.

We also support various member states' proposal to include examples of threat elements such as ransomware and critical infrastructure attacks, as there is value in raising awareness on technical aspects of the threats.

On this note, my delegation would like to reiterate the importance of understanding the human elements of cyber security threats. The fact that the most persistent threat and vulnerability in cyberspace stems from human behavior is often overlooked, and merits greater attention from the international community.

In this regard, we would like to suggest adding to the list in paragraph 7.b, "Measures to enhance understanding the human elements of ICT threats."

[Norms, Rules and Principles]

Mr. Chair,

As my delegation highlighted in previous sessions, it has been well established through discussions at various international fora that there is no vacuum of legalities in the cyberspace, as the international law including the UN charter in

its entirety applies to cyberspace.

The fact that the norms agreed to at the 2015 GGE reports and other subsequent GGE and OEWG reports have a non-binding and voluntary nature does not imply that states enjoy optionality in conforming to these norms.

This does not rule out the possibility of additional norms developing over time, as paragraph 8.b. duly elaborates. Regarding this, my delegation would like to stress that it is important that these additional norms develop in a way that will complement, not challenge or substitute, existing laws and norms in cyberspace.

Moreover, we believe that discussions to develop additional norms must focus on providing concrete protection to states affected by cyber attacks, and ways to promote implementation of existing norms in that regard.

We support the voluntary national survey of implementation of norms, mentioned in paragraph 8.d, as a useful mechanism for stocktaking the current state of norms implementation in the international community. Republic of Korea has submitted the national survey in March 2020, which we will update and share with the Open-ended Working Group in due course.

[International Law]

Mr. Chair,

Let me first begin by welcoming that the draft report includes “due diligence” in the list of specific topic of international law to be discussed in future sessions in paragraph 9.a. Due diligence is becoming increasingly important in both preventing and responding to cyber incidents. Promoting deeper understanding of this principle will also go a long way in enhancing the implementation of the

agreed norms, as many of them are pertinent to the principle of due diligence.

Equally welcomed in the same list is the explicit mentioning of International Humanitarian Law, the importance of which has been echoed by many during our discussions.

Regarding this, we would like to suggest reinstating the deleted clause in the paragraph 9.a. mentioning briefings from ICRC, as we believe it will greatly help enhance member states' understanding of the IHL in the context of ICTs security.

We hope to see these elements retained in the final outcome.

On the other hand, we suggest deleting the phrase "development of common understanding remains the exclusive prerogative of States" in paragraph 9.a., since such understanding can also be further developed by other entities such as the academia through legal interpretation of the international law.

A useful way of developing such common understanding is through voluntary sharing of national views on how international law applies in the use of ICTs, as mentioned in paragraph 9.b. We appreciate that many states have submitted their national views, and we plan to submit our own in the second half of this year.

Lastly, The ROK also strongly supports the importance of capacity building on international law, and therefore welcomes the expression in paragraph 9.c. We are committed to promoting better understanding of how international law applies to cyber space through such efforts as ROK-Netherlands Joint Webinar on the Application of International Law in Cyberspace. We also take interest in improving mechanisms for mutual legal assistance regarding malicious use of ICTs mentioned in the same paragraph, and look forward to further discussions in this area.

[Confidence Building Measures]

Mr. Chair,

The ROK is committed to developing and operationalizing CBMs in UN and regional fora. We believe a functioning and effective POC network at the UN level can be a useful starting point for global confidence building. To this end we are participating in the joint effort to establish a UN Cyber POC Network, and believe that it is important to foster greater coordination between such efforts at the UN and those at regional level such as ARF and OSCE. We welcome the paragraph 10.a. and recommended next steps 2 in this regard.

We also believe in the utility of UNIDIR Cyber Policy Portal as a means to promote confidence building, and therefore support its mentioning in paragraph 10.b.

Lastly, we would like to share that ROK is engaged in efforts to enhance CBMs in regional and cross-regional fora, including through co-chairing the ARF Inter-sessional Meeting on ICTs security, and participation in the Cross-regional CBMs group. We hope these regional and cross-regional efforts for CBMs yield concrete results that build and reinforce mutual confidence in cyberspace.

The cross-regional CBMs group is hosting an event on the sideline of this session, and we welcome participation of many member states.

[Capacity Building]

Mr. Chair,

The importance of narrowing the digital divide in making of a safer cyber space has been echoed by delegations across the board during our previous sessions,

and the role of capacity building in this regard has gained unequivocal support.

However, a significant gap still exists between the international community's will for capacity building and concrete mechanisms on which it can rely to that end.

A permanent mechanism dedicated to capacity building efforts to be potentially established within the UN, as mentioned in paragraph 10.d. and recommended next steps 2, is a welcome step in the right direction.

In these paragraphs, we would like to suggest adding PoA as a concrete example of such mechanisms, considering many member states, co-sponsors and others, have recognized its potential role in enhancing capacity building. We suggest adding to the end of paragraph 10.d the phrase "states noted that PoA, among other proposals, could be a possible example of such a mechanism."

Lastly, the ROK is also actively engaged in capacity building efforts in regional fora such as the ARF and ASEAN, including through proposing Workshops on Fostering Cyber Security Professionals. We are committed to continuing these efforts in and outside of UN.

[Regular Institutional Dialogue]

Mr. Chair,

As a co-sponsor of the Program of Action for advancing responsible State behavior, the ROK shares the same position with other co-sponsors.

We believe that PoA, as a permanent and organized mechanism, can serve as a practical way for operationalizing the various proposals put forward at the OEWG.

We welcome mentioning of PoA in paragraph 12.c. of the draft, and look forward to further discussions and development of the proposal. /end/