Republic of Korea
Comments on the pre-draft of the OEWG Report

April 14, 2020

General Comments

1. The Republic of Korea (ROK) considers that the OEWG, where all Member States participate, has offered an opportunity to increase common understandings among States, and its transparency and openness contributed to promoting an open, secure, stable, accessible and peaceful cyberspace. In this regard, the ROK would like to commend the Chair's efforts in leading discussions by encouraging States' participation and carefully listening to each States' views.

2. This initial pre-draft, encapsulating what has been discussed through the previous OEWG sessions in a comprehensive way, properly reflects all States' commitment to making an open and secure cyberspace. The ROK would like to suggest additional ideas to develop or complement the recommendations on the pre-draft as follows.

International Law

3. The ROK supports the idea of exchanging national views and practice on how international law applies in cyberspace. In addition to the suggestions already reflected in the pre-draft—generally focused on the exchanges at the multilateral level—the ROK intends to propose further engagement at the bilateral and regional levels as below:

   - (Paragraph 68.a) Member States be encouraged to exchange national views and practice on how international law applies to State use of ICTs at bilateral, regional and sub-regional levels in order to converge on shared understandings and facilitate such efforts at the multilateral level.

Rules, Norms and Principles for Responsible State Behaviour

4. The ROK strongly upholds 11 voluntary, non-binding norms agreed in the 2015 UNGGE report and recognizes its value in promoting responsible State behaviour in cyberspace. In this light, the ROK's views that further emphasis on these norms and their implementation should be put in the final report of the OEWG as well. The following is the ROK's suggestion:

   - (Paragraph 68.b) Member States be urged to promote awareness and implementation of the existing norms, in particular the 11 voluntary, non-binding norms agreed in the 2015 UNGGE report, and in order to support their operationalization, further guidance on the implementation of norms of responsible State behaviour be developed and widely disseminated at national, regional,

interregional and global levels including through the United Nations. States in a position to contribute expertise or resources to the development and dissemination of such guidance are encouraged to do so.

5. Simultaneously, the ROK seeks to clarify and concretize 11 agreed norms so that States can share common understandings and further implement the norms. Among others, the ROK is interested in the principle of due diligence. In efforts to raise awareness on this norm and encourage its implementation, the ROK would like to propose ways to implement the norm in the paragraph 13(c) of the 2015 UNGGE report. Please see the attached document for further details[1].

Confidence-Building Measures

6. In the face of the increased threats from the malicious ICT activities, we should be keen on building confidence to respond such treats. The ROK suggests the following recommendation to be included in order to promote further cooperation among States:

   - (Paragraph 68.c) Member States be encouraged to share lessons and practices from responding to serious ICT incidents in order to prevent as well respond to any similar incidents in a coordinated manner.

7. Furthermore, given the nature of cybersecurity, all stakeholders such as the private sector, academia and civil society should work together to make an open and secure ICT environment. The ROK thus would like propose the following recommendation in order to encourage States to recognize the importance of confidence-building among multi-stakeholders:

   - (Paragraph 68.c) Considering the importance of confidence-building among all stakeholders in cyberspace, Member States be encouraged to explore mechanisms for sharing their lessons, practices and experiences among multi-stakeholders.

Principles for Capacity Building

8. Many States echoed the importance of capacity through discussions and urged that previous efforts in building capacity should be implemented in a more coordinated way. In this context, the ROK suggests that the four principles agreed at the 2011 Busan Partnership for Effective Development Co-operation could be adopted as a useful

[1] In terms of organization, the ROK believes that any "additional proposals by Member States for new norms" can be collected and better placed as an Annex rather than consolidated in the paragraph 39 of the pre-draft.

guideline in improving capacity building efforts in regard to cybersecurity (in the paragraph 68.d of the pre-draft):

- **Ownership**: Developing countries should take a lead in their own development programs in close coordination with partner countries in line with the whole process including the identification of priorities and the implementation of projects.
- **Focus on results**: Capacity building programs on cybersecurity should have a sustainable result which can contribute to social and economic development of recipient countries.
- **Inclusive partnerships:** all multi-stakeholders such as industries, think-tanks, academia, civil societies and others should join and contribute to capacity building programs to make an open and secure cyberspace.
- **Transparency and shared accountability:** Technical assistances on cybersecurity should be transparent and accountable to all citizens of the recipient and donor countries.

9. Also, the ROK welcomes additional principles specifically tailored to the ICT environment.

Regular Institutional Dialogue

10. The ROK believes that further discussions on cybersecurity at the UN level can provide an opportunity to deepen our cooperation in cyberspace. In order to fully enjoy benefits from those processes, they should work closely with distinguished mandates to prevent the duplication of works. In this regard, the ROK would like to suggest a recommendation as follows:

- (Paragraph 68.e) Such new OEWG and GGE should be designed and operated in a complementary and mutually reinforcing way, considering, in particular, that the OEWG can be of value in universalizing and implementing what has been already agreed in the previous GGEs.

11. The ROK's view is that future processes, regardless of its format, should encourage further interactions among not only States, but also other stakeholders, such as the private sector, academia and civil society. It would be useful to include other recommendations suggesting States to consider continuing informal inter-sessional consultative meetings where multi-stakeholder can participate.

Others

12. Para.19 considered the health sector as an instance for the critical infrastructure. The ROK is well aware of the difficulties in defining the critical infrastructure, as each State

has different prerogatives and priorities. However, given the current situations in amidst of COVID-19, the ROK views that this issue raised by the para.19 has been raised in a timely manner and is worthy of drawing many States' attention at this critical time. In that vein, the ROK endorses the ICRC's suggestion that "States should not conduct or knowingly support activity that would harm medical services or medical facilities, and should take measures to protect medical services from harm."

(Attachment)

The ROK's suggestion for guidance on due diligence principle from the 2015 UNGGE report

The principle of due diligence is one of essential elements for responsible behavior of States in cyberspace. This principle is embodied in the paragraph 13 (c) of the 2015 UNGGE report as below:

> *States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;* **(2015 ¶ 13(c))**

The ROK believes that the international community should embark on discussions to review the legal status of due diligence to be elevated as a legal obligation. However, the ROK also recognizes that States' views on this matter may vary and it will take more time to come to an agreement. In order to effectively respond to increased cyber threats in the meantime, it is necessary to concretize and clarify what is already agreed. The ROK sees that further elaboration of the principle will serve as guidelines for voluntary implementation of responsible State behavior in cyberspace and as a safety net for the affected States. Hence, the ROK suggests following ways to implement the norm in the paragraph 13 (c).

- When an affected State notifies another State that ICT incidents has emanated from or involve the notified State's territory with qualified information, the notified State should, in accordance with international and domestic law and within their capacity, take all reasonable steps, within their territory, to cause these activities to cease, or to mitigate its consequences.
- It should be understood that said notification does not imply responsibility of the notified State for the incident.
- The minimum requirement of qualified information may include Indicator of Compromise (IoC), such as IP address, location of perpetrators and computers used for malicious ICT acts and malware information.

Additional or other requirements for qualified information can be further discussed. Ideally, it would be better that if the OEWG can come up with a universal template for notification and establish the relevant national point of contact as well.