View and Assessment of the Republic of Korea on the Questions

Resolution 73/266

Ⅰ. Introduction

Pursuant to the adoption of General Assembly Resolutions 73/27 and 73/266, two consultative mechanisms begin this year. The Open Ended Working Group (OEWG) will be newly organized and the sixth (6th) Group of Governmental Experts (GGE) will continue its deeper discussions on developments in the field of information and telecommunications in the context of international security. The Republic of Korea (ROK) welcomes such efforts of the States to move the discussions on international norms in cyberspace forward.

However, considering their similar mandates provided by the above-mentioned Resolutions, the ROK believes that complementarity is important at this juncture. In this regard, the discussions of the OEWG should be built on the progress made so far in the previous GGEs. Recalling the GGE report adopted in 2015, the ROK would like to highlight the importance of promoting the rule-based cyber security governance, transparent confidence building measures (CBMs), and meaningful capacity building for international cooperation.

Upon request of the UNGA resolution 73/266, the ROK hereby submits the national position paper on the issue of Information and Communications Technologies (ICTs) security, which is mainly based on the enclosed *Seoul Framework and Commitment to an Open and Secure Cyberspace*, a document containing notions and views identified in the preparatory stage of the Seoul Conference on Cyberspace 2013 and in the Conference itself.

Ⅱ. Efforts taken at the national level to strengthen information security and promote international cooperation in this field

The ROK recognizes that it is essential to forge a strong partnership among stakeholders in order to build an open, secure, stable, accessible, and peaceful cyberspace. As cyber security cannot be adequately addressed single-handedly by any state alone, regional and international cooperation in cyberspace is of utmost importance. In order to set a course of action with a more strategic and systematic approach, the ROK launched the National Cybersecurity Strategy[1] in April 2019. It outlines how the ROK will ensure our society's continuance of reaping benefits and lowering risks deriving from ICTs with six strategic pillars: 1) secured national critical infrastructure, 2) enhanced cyberattack defense capabilities, 3) trust-and-cooperation-based governance, 4) cybersecurity industry growth, 5) well-fostered cybersecurity culture, and 6) strengthened international cooperation.

1) http://www.boho.or.kr/filedownload.do?attach_file_seq=2162&attach_file_id=EpF2162.pdf

Furthermore, the ROK has put great emphasis on strengthening cybersecurity and promoting international cooperation with the following efforts.

At the regional level, the ROK has put forth a great amount of effort and resources in cybersecurity, especially in establishing CBMs. In this context, the ROK has actively participated in discussions at the ARF Inter-Sessional Meeting (ISM) on Security of and in the Use of ICTs, as well as the ARF Open Ended Study Group (OESG) on Confidence Building Measures to Reduce the Risks of Conflict Stemming from the Use of ICTs. In 2017 and 2019, the ROK hosted, in cooperation with the OSCE, the First and Second Inter-Regional Conferences on Cyber/ICT Security to discuss measures to enhance both inter- and intra-regional cooperation against cyber threats by sharing its experience with the OSCE. The ROK believes that this biennial Conference would contribute to promoting regional CBMs, as well as to feeding them into the UN level discussions.

At the global level, the ROK has participated in four rounds of the UN GGE on Developments in the Field of ICTs in the Context of International Security (2004-05, 2009-10, 2014-15, 2016-17) and contributed to its achievements. In 2013, the ROK hosted the 3rd Global Conference on Cyberspace in Seoul, during which capacity-building was highlighted in cyber-related international fora as a major item on the agenda. In 2017, the ROK echoed the international community's emphasis on national critical ICT infrastructure and hosted the 14th Meridian Conference in Seoul. Also, upholding the multi-stakeholder approach in cybersecurity, the ROK joined the Paris Call for Trust & Security in Cyberspace in 2018. In October 2019, the ROK will host the First Cybersecurity Working Group meeting of Warsaw Process in Seoul in order to enhance regional cybersecurity capacity and build support for the established framework of responsible state behavior in cyberspace.

In addition, the ROK has been holding a series of bilateral and trilateral cyber policy consultations with a view to discussing potential steps for cooperation and strengthening the concerted response to cyber threat. To raise awareness and promote common understanding across countries, areas and sectors, the ROK has been convening various annual international events such as the Seoul Defense Dialogue Cyber Working Group (SDD CyberWG) since 2014, International Symposium on Cybercrime Response (ISCR) since 2000, the International Conference on Building Global Cyber Peace Regime (GCPR) since 2014, annually since 2017, and the Jeju Forum for Peace and Prosperity since 2001.

The ROK's efforts in capacity building are also continuous and vigorous. The ROK has operated the Global Cyber Security Center for Development (GCCD) since 2015 and the Cybersecurity Alliance for Mutual Progress (CAMP) since 2016 with a view to sharing practical knowledge and exchanging experiences in responding to cyber threats. Combatting Cybercrime, a project with the World Bank first implemented in 2014, is more focused on responding to cybercrime.

Ⅲ. The content of the concepts mentioned in the reports of the Group of Governmental Experts

The ROK believes that it is crucial to deepen the understanding of the application of existing international law in cyberspace and concretize voluntary and non-binding norms, rules and principles of responsible behavior of States agreed in previous GGEs. The ROK recognizes the particular importance of 2013 and 2015 GGE reports, which made, among others, the following significant conclusions:

- ✓ International law, in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment.
- ✓ State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.
- ✓ States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. States must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts.

To build on the progress made so far, further deliberations and consultations among States are necessary on how these principles can be applied to state behavior in cyberspace. In particular, the ROK recognizes that further discussions on the following items should be pursued to yield meaningful and concrete results.

- ✓ Implementation of 11 non-binding and voluntary norms such as cooperation among States for cybersecurity, exchanges of information, respect for human rights, and protection of critical information infrastructure, in paragraph 13 of the 2015 GGE report, which the ROK reaffirms its commitment to
- ✓ The right to self-defense and international humanitarian laws (IHL) which are fundamental to international law and are applicable in the context of cyberspace
- ✓ International legal responsibility by States for a cyber activity that constitutes an internationally wrongful act and that is attributable to the State
- ✓ States' response to requests for assistance by another State

Enclosed: Seoul Framework and Commitment to an Open and Secure Cyberspace

/END/