Mr. Chairman,

My delegation aligns itself with the statement on cybersecurity delivered by Canada on behalf of a group of states and would like to make some additional remarks.

The advance of information and communications technologies (ICTs) has presented us a new domain of boundless opportunities, creating unprecedented economic and social benefits. At the same time, however, it also has brought unprecedented challenges with them. The entire world today is facing mounting threats in cyberspace, with malicious actors ceaselessly plotting offensive activities using ICTs, targeting not only individuals and businesses but also national critical infrastructure. As a result, cyber security has now emerged as a key issue of international security agenda. In addressing these challenges, my delegation believes it important to put priorities on the following three aspects.

First, it is crucial to step up our efforts to deepen our commitment to apply international law in cyberspace and implement norms of responsible behavior of States. In this vein, the ROK wishes to stress the value of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security established by this very Committee. It served as a unique and valuable global-level platform to seek
common international principles and guidelines to be applied in the cyber domain. In its consensus reports of 2013 and 2015, the GGE reaffirmed that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment. Furthermore, the 2015 GGE report offered valuable recommendations for 11 voluntary, non-binding norms, rules or principles of responsible behavior of States. The ROK firmly believes that continuing the GGE process would greatly contribute to the concerted efforts toward open, secure, stable, accessible, and peaceful environment in cyberspace. We hope that the First Committee agrees on re-establishing the Group of Governmental Experts, building upon its previous achievements.

Secondly, it is essential to develop and implement practical confidence-building measures to enhance transparency and reduce risk of conflict stemming from misunderstanding and miscalculation. In this regard, the ROK recognizes the importance of inter-regional cooperation and dialogue in developing CBMs. We therefore support and welcome the efforts taken at regional settings, including ARF, OSCE, and OAS. It was in this context that the ROK organized the Inter-Regional Conference on Cyber Security in April 2017 in cooperation with the OSCE. It offered a valuable venue to share views and experiences in building regional cyber CBMs. The ROK considers that this inter-regional approach could be a good starting point for exploring the way of cooperation by sharing information and best practices. We plan to hold The 2nd Inter-Regional Conference on Cyber Security next year.

Thirdly, it is essential to bridge the gap in cyber security capacity among countries. When the ROK hosted the 2013 Seoul Conference on Cyberspace, we sought to facilitate international cooperation in capacity building by incorporating it into the agenda of the conference. Building upon this initiative, the ROK launched in 2015 the Global Cybersecurity Center for Development (GCCD) as part of our efforts to share expertise and experience.

Mr. Chairman,
Considering the cross-border nature and ripple effects of cyber threats, no single country is immune to this looming threat, and no single country can tackle this concern single-handedly. Having participated in four rounds of the UN GGE, my delegation would like to reaffirm our commitment to continue to play constructive role in developing cooperative measures to address existing and potential threats in cyberspace. Thank you.