Republic of Korea

Ⅰ. General Appreciation of the issues of information security

Cyberspace offers infinite opportunities for economic and social development and greater global prosperity. An open and secure cyberspace is essential to increase human accomplishments and promote democratic participation. However, given that cyberspace is anonymous and is globally interconnected, it is giving rise to greater number of challenges such as cyber crime, cyber terrorism, and cyber attacks. And, the recent controversy over mass surveillance has sparked a global debate on what constitutes the right balance between privacy and security.

Against this backdrop, the government of the Republic of Korea has been making efforts to raise the awareness on the need to enhance international cooperation on cyber security and to seek ways to promote practical ways of cooperation.

The Republic of Korea believes that strengthening international cooperation on cyber security is essential to reap the potential benefits of cyberspace, while addressing the mounting threats. In particular, it is imperative for the international community to agree on international norms that are applicable to cyberspace, strengthen law enforcement cooperation and find solutions to prevent the malicious use of ICT by states and non-state actors.

In this regard, the Republic of Korea welcomes the report of the 3rd UN Group of Governmental Experts (GGE) on developments in the field of information and telecommunications in the context of international security, including the agreement that existing international law is applicable in cyberspace. And we look forward to discussing concrete ways to apply existing international law in cyberspace during the 4th UN GGE. Korea is of the view that it is necessary to find common ground on cyber issues in a constructive and practical way, rather than focusing on the different positions.

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

In recent years, the Republic of Korea has been subject to several major cyber attacks. There was a cyber attack against major broadcasting and banking systems in March 2013, and government websites in June 2013. In order to effectively address such cyber threats, the Korean Government adopted the 'National Cyber Security Comprehensive Countermeasures' in July 2013, which sets out, among others, to establish a system for relevant government agencies to respond to cyber attacks, build a system to share information on cyber threats, strengthen cooperation with the private sector, expand the scope of Critical Information Infrastructures (CII) subject to protection, raise awareness of information security in the private sector and promote training programs on information security.

The Republic of Korea is currently holding bilateral cyber consultations with a number of countries, including the US, Russia, EU, India and Australia, while actively taking part in

regional and international discussions on cyberspace, such as the ASEAN Regional Forum (ARF) and the UN.

More recently, the Republic of Korea hosted the Seoul Conference on Cyberspace on 17-18 October 2013, following the London Conference in 2011 and the Budapest Conference in 2012. With the participation of a total of 1,600 representatives, including 43 ministers and vice-ministers of 87 countries and 18 international organizations, the conference helped to raise the awareness on the need to strengthen international cooperation and found common ground on major cyber issues. The participating countries agreed on a *Seoul Framework for and Commitment to Open and Secure Cyberspace*, as part of the Chair's summary. The document represents the understanding on where international consensus has been reached on major cyber issues to date. Korea hopes that it can be used as a basis in moving the international discussions forward.

The Republic of Korea will continue to actively participate in international discussions on cyber issues, including the next Conference on Cyberspace, which will be held in the Netherlands in April 2015, and contribute to building trust and identifying or establishing norms in cyberspace.

Ⅲ. The content of the international concepts aimed at strengthening the security of global information and telecommunication system

One important area in the international cyber discussions is agreeing on a set of norms that are applicable to cyberspace. In parallel to the efforts of the international community, the Republic of Korea is committed to constructively participating in the discussions on how international law can be applied to governing state behavior in cyberspace.

Establishing confidence building measures (CBMs) bilaterally, regionally and globally is critical to ensuring cyber security and stability, as was also set out in the 3rd UN GGE report. The Republic of Korea takes note that in June 2013 Russia and the United States agreed on a set of bilateral CBMs in the area of cyber security, including a mechanism for information sharing between their CERTs. The Republic of Korea is also making efforts to set up cyber CBMs both bilaterally and multilaterally.

For practical means of implementing CBMs, the Republic of Korea is of the view that joint research by the UN and relevant international mechanisms to gather information on best practices, hacking cases, and other technical analysis can be useful in guiding the international discussions forward. And sharing senior-level contact points would be helpful to alleviate tension and miscalculation between states.

Ⅳ. Possible measures that could be taken by the international community to strengthen information security at the global level

To strengthen cyber security at the global level, the international community should share information and strengthen cooperation in the international fora, such as in the UN, ARF, the OSCE and the Conference on Cyberspace. The international community should

prioritize on agreeing on terms and norms applicable to cyberspace and developing confidence building measures (CBMs) to ensure the security and stability of cyberspace.

The Republic of Korea, particularly, notes the OSCE's decision on an initial set of CBMs to reduce the risk of conflict stemming from the use of information and communication technologies in December 2013. The OSCE's CBMs can be a good basis for advancing relevant discussion in other regions and internationally.

Given that cyber threats transcend national boundaries and require sophisticated technical expertise, cooperation among CERTs is becoming increasingly important to cope with cyber incidents. Therefore, we should find ways of intensifying CERT cooperation among the varying CERTS, including FIRST (Forum of Incident Response and Security Team, 64 countries) and APCERT (Asia-Pacific CERT, 19 countries).

In addition, many cyber attacks originate in or are carried out through developing countries with weak cyber infrastructure and limited resources and technologies to deter cyber attacks. Therefore, it is important that the international community increase their assistance to these developing countries in their efforts to build cyber capacity. This will pave the way for a more secure and open cyberspace in the years to come. /END/