Republic of Korea

Implementation of the 2015 UNGGE Norms

The Republic of Korea (ROK) has been actively engaging in international efforts to make an open, safe, stable, accessible and peaceful cyberspace. As one of such efforts, the ROK hereby submits the working paper on the implementation of 11 norms agreed in the 2015 UNGGE report. It is the ROK's belief that the paper, composed of the ROK's best practices, would contribute to promoting transparency, confidence and common understanding among States, as well as would shed light on how norms can complement the international law applied in cyberspace.

(Norm 1) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;

Considering the cross-border nature and ripple effects of cyber threats, it is essential to forge a strong partnership responding to malicious cyber activities. Recognizing this, the Republic of Korea (ROK) has placed a great deal of importance on establishing cooperative mechanisms.

・Launch of the National Cybersecurity Strategy[1]

In order to set a course of action with a more strategic and systematic approach, the ROK launched the National Cybersecurity Strategy in April 2019. The Strategy presents the ROK's vision and goals in cybersecurity and outlines strategic tasks at the individual, industry and government levels as follow:

- ✓ Explore means for practical cooperation, both bilateral and multilateral, and establish mutual assistance systems by holding consultations on cyber policies, strengthening partnership with international organizations, and acceding to international agreement.
- ✓ Promote cooperation in sectors such as national defense, intelligence, and law enforcement, as well as exchange with the private sector to respond to cybersecurity threats, including acts of war, terrorism, and crime.
- ✓ Provide mechanisms to allow relevant agencies to propose policy directions for the government and share collected information throughout the process of international

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

cooperation.

- ✓ Increase participation in the process of establishing international norms on cybersecurity and take the lead in disseminating international rules and best practices.
- ✓ Actively engage in discussions regarding trust building to prevent escalation between States due to any misunderstandings in cyberspace.
- ✓ Expand foreign assistance projects for cybersecurity capacity building to developing countries in a reciprocal manner and share cybersecurity technologies and systems.

・Bilateral/Trilateral Cooperation

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 threats. Specifically, in 2019, the ROK conducted bilateral consultations with several countries including the Czech Republic, Poland and the EU and a trilateral consultation with Japan and China.

・Multilateral Cooperation

At the multilateral level, the ROK has participated in four rounds of the UN Group of Governmental Group (GGE) on ICTs and contributed to its achievement. In particular, the ROK put a great emphasis on the "due diligence" principle that States should not knowingly allow their territories to be used for internationally wrongful acts using ICTs. As the newly founded Open-ended Working Group (OEWG) on ICTs has initiated its discussions, the ROK reaffirms its commitment to making an open and secure cyberspace by actively participating in the UN process.

In October 2019, the ROK co-hosted the Warsaw Process Working Group on Cybersecurity with the United States and Poland. More than 120 officials from around 50 countries attended the Working Group to discuss how to promote responsible State behavior in cyberspace and how to develop and implement practical cooperative measures.

・Regional Cooperation & Confidence-Building Measures (CBMs)

Cooperating with the Organization for Security and Co-operation in Europe (OSCE), the ROK hosted the Second Inter-Regional Conference on Cyber/ICT Security in May 2019 to discuss measures on how to enhance regional cooperation against cyber threats, while sharing its experiences with the OSCE.

Moreover, recognizing the importance of establishing confidence building measures (CBMs) in the field of ICTs, the ROK actively participated in discussions at both the ASEAN Regional Forum (ARF) Inter-Sessional Meeting (ISM) on Security of and in the Use of ICTs and the Open Ended Study Group (OESG) on Confidence Building Measures to Reduce the Risks of Conflict Stemming from the Use of ICTs. The ROK welcomed major five

confidence building measures, suggested and adopted at the ISM, and prepared itself to implement and develop the measures in cooperation with ARF Participants.

・Capacity building efforts at the international, regional and bilateral levels

Countries with lower cyber security capacity are often targeted to be used as a transit route, and the ROK views capacity development as one of top priorities in promoting ICTs security. In line with the matter, the ROK included capacity building as a major item on the agenda for the Global Conference on Cyber Space in Seoul in 2013.

Taking a step further, the ROK implemented various capacity building projects with developing countries by setting the Global Cybersecurity Center for Development (GCCD) in 2015 and the Cybersecurity Alliance for Mutual Progress (CAMP) in 2016. Through the projects, the ROK provided policy advice, consultations and trainings on cyber-security measures to developing countries. Moreover, since 2015, the GCCD has hosted capacity building seminars in 13 countries to offer practical information to the participants and relay the ROK's experience. The said CAMP, composed 59 agencies of 45 countries as its members, has hosted four congresses and five regional forums so far.

(Norm 2) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;

The ROK set up its own cross-governmental system to respond to future cyber threats. Under the leadership of the Presidential Office, the Ministry of Science and Information (MSIT) is in charge of responding to cyber threats targeting the private sector, whereas the National Cyber Security Center (NCSC) manages the public sector, and the Ministry of National Defense (MND) has a responsibility of the national defense.

In accordance with the National Cyber Security Management Regulation, the NCSC operates the joint cyber threats response system by which relevant information is shared in real time, and threat warnings and response guidelines are issued accordingly. Weekly cyber threats index is also updated and notified to government institutions. Similarly, relevant agencies have their own cybersecurity monitoring centers to detect and promptly respond to cyber threats.

In efforts of considering all relevant information in case of ICT incidents, the ROK has encouraged private entities to share information through public-private consultation meeting in responding to ICT incidents since 2016 and the network of the Cyber Threats Intelligence since 2014. The Cyber Security Big Data Center was also established by the Korea Internet & Security Agency (KISA) in 2018. Thanks to its well-established network between the public and private sectors, 260 companies reported and shared over 200 million cases on cyber threats only in 2019.

(Norm 3) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

The ROK does not knowingly allow its territory to be used for internationally wrongful acts using ICTs.

Our concrete efforts to ensure the statement are as following:

・Countering Cybercrime

The Korean National Policy Agency (KNPA) has exerted its efforts to promote the nation's capabilities to counter cybercrime through training programs, sets of investigation manual, and research on investigation techniques, and more. If certain websites are turned out to be utilized for cybercrime like in distribution of malware, the police authority shall shut the websites at the initial stage.

・Deterring and responding to cyber threats

The KNPA operates counter-cyberterrorism teams all across the country. For now, 30 teams with 160 officers are tasked with responding to cyber threats and addressing cybercrime.

Since 2012, the KISA has operated bug bounty programs to encourage individuals to report bugs and vulnerabilities in software. Since its implementation, 1,466 bugs and vulnerabilities have been reported. Major vulnerabilities reported through the programs are publicly announced online, which allows the developers to resolve the issues and other CERTs to respond.

Now, the national CERT under KISA (KrCERT/CC) eagerly cooperates with international Computer Emergency Response Teams (CERTs), including Asia Pacific Computer Emergency Response Team (APCERT) by sharing information on cyber threats. In 2019, the KrCERT/CC shared ICT incidents information with relevant authorities of other members.

・Promoting the principle of due diligence

The ROK has constantly demonstrated its commitment in light with the 2015 UN Group of Government Experts (GGE) Report through public statements at the regional and international forums. It is equally expected that other States should not knowingly allow its territory to be used for internationally wrongful acts using ICTs. The ROK has keen interests in promoting the principle of due diligence, reflected in norms identified in the 2015 UN GGE Report, and hopes that this norm be elevated on a firmer footing.

(Norm 4) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;

・Cyber policy consultations

The ROK has convened bilateral and trilateral cyber policy consultations with partner countries in order to develop and implement cooperative measures. See above **Norm (a)** for more information.

・CERT Cooperation

To promote CERT cooperation, the KISA has entered into Memorandums of Understanding (MOUs) with partner countries. Since joining as a member of the Global Forum of Incident Response and Security Teams (FIRST), the ROK has shared its case studies of ICT incidents and collected information on hacking incidents in Korea from other global CERTs and security firms at the annual conferences.

・Cooperation on countering cybercrime

Recognizing that international cooperation is crucial to combat cybercrime, the ROK invites over 1,000 experts and delegates on a yearly basis to discuss how to strengthen global cooperation against cybercrime. Every year, the KNPA convenes the International Symposium on Cybercrime Response (ISCR), which has also proven effective in investigating and prosecuting malicious activities in cyberspace concerning child pornography, gambling, etc. In addition, the ROK joined the G7 24/7 cybercrime network.

The ROK places a great emphasis on strengthening bilateral cooperation on counter-cybercrimes. For example, to promote cooperation among law enforcement agencies, the ROK's Supreme Prosecutor's Office (SPO) convenes regular meetings with the U.S. FBI. Also, in 2019, the SPO visited the Federal Criminal Police Office (BKA) in Germany and European Cybercrime Centre (EC3) in Netherlands to address global cybercrime. Moreover, given the fact that Internet Service Providers (ISP) are becoming important partners to secure electronic evidences, the SPO operates the Government Security Program (GSP) jointly with Microsoft.

・Capacity building programs

Currently, the ROK is actively engaging in capacity building programs for developing countries. For instance, the KNPA has sent experts on cybercrime investigation and digital forensic to developing countries since 2012. In 2019, 12 experts were sent to six countries and helped to improve their capabilities.

In order to promote regional resilience, the ROK has been focusing on building capacities in Asia Pacific countries. In this regard, the Asia-Pacific Cybercrime Capacity-building Hub Secretariat was established in 2020 with trilateral MOU among Global Forum on Cyber Expertise (GFCE), the World Bank Group, and the SPO. The Secretariat is located in Seoul and will serve as a hub network, providing cybercrime response trainings and investigation assistances to different regions in developing countries.

(Norm 5) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolution 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;

・Support for human rights resolutions

The ROK strongly supports human rights online. The ROK co-sponsored the Human Rights Council Resolution 20/8 and 26/13 concerning the promotion, protection and enjoyment of human rights on the Internet. The UN General Assembly Resolution 68/167 and 69/166 on the right to privacy in digital age were adopted without vote, and the ROK further supports the full respect for human rights in line with such resolutions, including the right to freedom of expression.

・Emerging technologies and human rights

The ROK has played a leading role in promoting and raising awareness on human rights in the digital era. For example, the ROK drafted and proposed the 41st Human Rights Council Resolution 41/11 – New and Emerging Digital Technologies and Human Rights in 2019, co-sponsored by 86 countries and adopted by consensus. The ROK also successfully implemented recommendations on human rights (Rec.3A/B) and was identified as “champion” by the UN High-level Panel on Digital Cooperation. In collaboration with the UN and other multi-stakeholders, the ROK continues actively participating in discussions to yield fruitful and concrete results.

・Legal Framework

At the domestic level, the ROK has legal frameworks to protect human rights in the use of ICTs. The Personal Information Protection Act (PIPA), enacted in 2011, regulates the personal data handled by the private and public sectors. Specifically, the law regulates the mandatory measures for each stage of handling of personal data by the personnel and protects the entity of information.

(Norm 6) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

The ROK does not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure available for use by the public. The ROK has consistently expressed this commitment with public statements at the regional and international forums.

(Norm 7) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructure, and other relevant resolution;

・Legal Framework

The ROK established the Act on Protection of Information and Communications Infrastructure in 2009. The purpose of the Act is to operate main information and communications infrastructure in a stable manner by formulating and implementing measures that concert to the protection of such infrastructure, in preparation for intrusion by electronic means, thereby contributing to the safety of the nation and the stability of the life of people.

・Designation and protection of critical ICT infrastructure

In accordance with the aforementioned Act, the ROK has selected and designated facilities as critical ICT infrastructure in each sector. Many resources have been invested to protect 11 main sectors so far, including electronics, transportation, finances, and water purification. The list of main sectors is to be updated. The Committee for Protection of Information and Communications Infrastructure is annually convened to review and monitor the protective measures for around 400 critical ICT infrastructure facilities.

・Awareness raising efforts

The ROK believes the awareness raising efforts to be crucial to prevent cyber threats against critical infrastructures. In this regard, the ROK declared the second Wednesday of July each year as “Information Protection Day” and its month as “Information Protection Month” in 2012. Information Protection Day seeks to draw people’s attention of the threats related to identity theft and cyberattacks. In July, multiple events such as the International Information Protection Conference and the Job Fair for Information Protection are regularly organized.

When it comes to the public, the MSIT has promoted 10 basic rules for securing information to raise awareness of internet users on information protection. The rules show useful steps to prevent ICT incidents: setting the passwords, using vaccine programs, and deleting emails from unknown users.

The Ministry of Education has also developed learning programs on ICT security and applied to school curriculum from elementary to secondary schools. Through these educational tools, users can understand the cyber ethics and contribute to a healthy culture of cybersecurity globally.

(Norm 8) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;

・CERT Cooperation

The KrCERT/CC has cooperated with international CERTs, including Asia Pacific Computer Emergency Response Team (APCERT) by sharing information on cyber threats. To promote CERT cooperation, the KISA has entered into several MOUs with partner countries, thereby establishing the points of contact with 10 countries for swift ICT incident responses.

Since joining as a member of the Global Forum of Incident Response and Security Teams (FIRST) in 2006, the KrCERT/CC has shared its case studies of ICT incidents and collected information on hacking incidents in Korea from other global CERTs and security firms at the annual conferences. As such, the ROK is willing to respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts.

・Establishment of the point of contact (POC)

The ROK acknowledges that international cooperation is necessary to respond to cyber threats, which are borderless and transnational in nature. To facilitate its cooperation, the proper channel should be established in advance to exchange requests and responses from partner countries. The ROK currently participates in points of contact directory, voluntarily submitted by ARF Participants, and, furthermore, convenes bilateral and trilateral cyber policy consultations to update points of contact among relevant departments and agencies on a regular basis.

(Norm 9) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

・Promoting 5G security

The ROK established the 5G Mobile Communication Industry Development Strategy in 2016, envisioning a leading nation in the 5G network communications. In the same context, considering the fact that the 5G security needs to be addressed for garnering its socio-economic benefits, the ROK formed a 5G security technological advisory council with security experts in 2018 to help telecom firms to carry out security monitoring more effectively and support the security technologies.

・Launch of the Internet of Things (IoT) authentication service

With the expansion of IoT devices connecting people's daily lives, the security vulnerabilities have also increased. To address the issue, the ROK has managed the IoT security authentication service since 2017. The authentication is processed on a rolling basis, so tech firms, telecom companies, and other private actors can get an authentication for its IoT devices or synced mobile applications.

(Norm 10) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

In accordance with the National Cyber Security Management Regulation, the NCSC operates cyber threats response system by which relevant information is shared in real time, threat warnings and response guidelines are issued accordingly. Weekly cyber threats index is updated and notified to government institutions. Similarly, relevant agencies have their own cybersecurity control centers to detect and promptly respond to cyber threats.

The ROK encourages private entities to share information on cyber threats. Since 2012, the KISA has operated bug bounty programs to encourage individuals to report bugs and vulnerabilities in software. Since its implementation, 1,466 bugs and vulnerabilities have been reported. In 2014, the KISA established the Cyber Threats Analysis System (C-TAS) where information on cyber threats can be shared among information security users. A member, accredited by the government, can get an access to the information for free and be bound to share its information.

The KrCERT/CC has uploaded major vulnerabilities on its websites on a regular basis in order to share relevant information with other CERTs and international cybersecurity firms. Also, the KrCERT/CC is actively engaging in cooperation with other CERTs by sharing relevant information when necessary.

(Norm 11) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

The ROK does not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams of another State. Also, the ROK does not use authorized emergency response teams to engage in malicious international activity.

・CERT Cooperation

The ROK cooperates with international CERTs, including Asia Pacific Computer Emergency Response Team (APCERT) by sharing information on cyber threats. In 2019, the ROK participated in the APCERT Incident Handling Drill, a simulated exercise of cyberattacks in scenario, and checked the readiness of cyber threat response and its organized cooperative system.

To promote CERT cooperation, the ROK has entered into several MOUs with partner countries, thereby establishing the points of contact with 10 countries for swift ICT incident response. Since joining as a member of the Global Forum of Incident Response and Security Teams (FIRST), the ROK has shared its case studies of ICT incidents and collected information on hacking incidents in Korea from other global CERTs and security firms at the annual conferences.