EU-ROK CYBER CONSULTATIONS
RESILIENCE AND TRUST IN CYBERSPACE

October 6-7, 2020

Cybersecurity has become a critical aspect of successfully managing the economic, political and societal repercussions of the COVID-19 pandemic. The pandemic underscored the benefits of digital technologies but also amplified societies' vulnerabilities to the malicious use of cyberspace from phishing and malware distribution campaigns to distributed denial-of-services attacks. Criminals and other malicious actors have efficiently exploited the crisis-induced digital vulnerabilities in home networks and critical infrastructures, including hospitals and medical research institutions, to pursue their commercial and political goals.

The European Union (EU) and the Republic of Korea (ROK) have recognised the need to address the immediate and long term cybersecurity challenges by enhancing cybersecurity resilience and intensifying international cooperation, including at the bilateral level. Both sides established a Joint Committee on Scientific and Technological Cooperation already in 2007 and a Cyber Dialogue in 2013, institutionalizing working level collaboration on digital economy and foreign and security issues respectively. In 2020, the conversation can build on this existing institutional setting to achieve targeted results for greater resilience and trust in cyberspace. To this end, the EU Cyber Direct project and the National Security Research Institute (NSR) have joined forces to organize the Track 1.5 *EU-ROK Cyber Consultations 2020*.

The consultations seek to create a trusted space to (1) enhance mutual understanding of the evolving cyber diplomacy postures in the EU and the ROK with regard to CBMs, critical information infrastructure protection, 5G and cybercrime, (2) identify convergences in the diplomatic positions on ongoing cyber-related international processes, and (3) build bridges between multiple stakeholders in European and South Korean cyber diplomacy by including non-governmental voices in the governmental norms-building processes.

As the consultations will take place in parallel to ongoing negotiations at the United Nations (UN) Open-Ended Working Group (OEWG) and the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, they will offer an opportunity to exchange views on how to best create a sustainable and inclusive global dialogue on a normative framework on responsible state behaviour in cyberspace.

This event is co-organised with

Implementing organisations

This project is funded by the European Union.

Agenda

October 6

Session 1: Building Resilient Critical Infrastructures in Crisis

As a response to the proliferation of cyber-attacks against healthcare facilities during the coronavirus pandemic, in April 2020 the EU's High Representative committed to reinforce global cooperation at the technical, operational, judicial and diplomatic levels to protect critical infrastructures against malicious cyber activities. Internally guided by its Network and Information Security Directive and its Cybersecurity Strategy, both currently under revision, the EU increasingly seeks to protect its critical information infrastructure by also strengthening resilience globally, including in partnership with the ROK. After the hack of its nuclear plant operator in 2014, Seoul has further ramped up its national and regional capacities to protect its critical infrastructures against cyber-attacks. Additionally, in April 2020, South Korea endorsed a suggestion by the International Committee of the Red Cross to include a voluntary agreement on non-targeting of health sector institutions in the OEWG report. What best practices on protecting critical infrastructures have European and South Korean institutions developed, and how robust are these in crisis situations? What roles do public and private actors play, and how can they collaborate? Finally, how can Brussels and Seoul cooperate to make critical infrastructures in Europe and East Asia resilient against cyber-attacks?

9:00-11:00 [CEST]
16:00-18.00 [KST]

Welcome

Gustav Lindstrom
Director of the EU Institute for Security Studies
H.E. Castillo Fernandez
Ambassador of the Delegation of the European Union to the Republic of Korea

Chair

So Jeong KIM
Manager, Cybersecurity Policy Department, NSR

Opening Inputs from Berlin and Seoul

H.E. Regine GRIENBERGER
Special Representative for Cyber Foreign Policy and Cyber Security, Germany
Mr. SON
National Cyber Security Center (NCSC), ROK

Panelists

Paul TIMMERS
Visiting Research Fellow, Oxford University, and former Director, Digital Society, Trust and Cybersecurity, European Commission
Jong In LIM
Professor, Korea University Graduate School of Information Security
Ian WALLACE
Senior Fellow, The German Marshall Fund of the United States

Session 2: Building Trust to Prevent Cyber Conflict Escalation

Since the publication of the Seoul Framework for and Commitment to Open and Secure Cyberspace in 2013, the ROK has consistently highlighted the importance of confidence-building measures (CBMs) to reduce the risk of escalation of conflict in cyberspace by enhancing transparency, crisis cooperation, and restraint, including through regional organizations such as the ASEAN Regional Forum (ARF) – most recently in its comments on the OEWG report pre-draft. Also in 2013 and 2016, the Organization for Security and Cooperation in Europe (OSCE) adopted sixteen voluntary cyberspace CBMs that subsequently shaped the global debate, and ARF and OSCE representatives met twice to exchange best practices. In 2015, the UN GGE also recommended states to adopt a set of voluntary CBMs and agreements, and international and regional institutions are now jointly working toward multi-level implementation. This panel will discuss how Europe and the ROK tailor CBMs to their specific contexts to prevent conflict and de-escalate tensions, from creating transparency and channels of communication to ensuring compliance with confidence-building agreements and engaging in joint exercises, including multiple stakeholders. What lessons can the ROK share with Europe on the promotion of bilateral and regional CBMs, and what role can the EU play to support CBMs on the Korean Peninsula and in East Asia? How have Brussels and Seoul involved the multiple stakeholders in building confidence in cyberspace and ensured multistakeholder information sharing? Finally, how can both sides cooperate to shape the OEWG final report's recommendations related to CBMs?

11:15-13:15 [CEST]
18:15-20.15 [KST]

Welcome

Sang Woo CHO
Director, Infrastructure Security Technology Division, NSR

Chair

Hannes EBERT
Senior Advisor, The German Marshall Fund of the United States

Opening Inputs from Brussels and Seoul

Joanneke BALFOORT
Director, SECDEFPOL DMD Security and Defence Policy, European External Action Service

H.E. Jong-in BAE
Ambassador for International Security Affairs, Ministry of Foreign Affairs, ROK

Panelists

Nohyoung PARK
Professor, School of Law, and Director, Cyber Law Centre, Korea University

Carmen GONSALVES
Head of International Cyber Policy, Ministry of Foreign Affairs, Netherlands

Joonkoo YOO
Research Professor, Korea National Diplomatic Academy, ROK

Caitriona HEINL
Director, The Azure Forum for Contemporary Security Strategy & Adjunct Research Fellow, School of Politics and International Relations, University College Dublin

October 7

Session 3: Managing the Geopolitics of 5G

Technical discussions on 5G telecommunications networks recently transformed into broad and contentious political battles over how to ensure future competitiveness while maintaining trust and security in strategic infrastructures around the world. Citing espionage and intellectual property concerns, the US and several of its Asian partners decided to look for alternatives to Chinese products within their mobile networks, especially critical infrastructure. Meanwhile, the EU and South Korea have been on the fence, as both try to reconcile trade and risk management imperatives and build strategic autonomy. The EU is currently implementing March 2019 recommendations on a concerted EU approach, and has published a coordinated risk assessment on cybersecurity in 5G networks and a toolbox to mitigating risks as first steps of this process, without explicitly naming a country or company and leaving the decision to restrict or exclude high-risk 5G vendors to Member States. Seoul delegated the decision which technology to use for new 5G systems to its network operators. Brussels and Seoul can build on a track record of strategic cooperation on joint 5G research and global interoperability and standards for 5G since a joint declaration in 2014. How can both deepen this cooperation amidst the persistent geopolitical uncertainty and exchange best practices on how to build a resilient 5G architecture and increase global supply chain security? Which joint measures can both develop to effectively mitigate cybersecurity risks related to 5G? And how can both work together and with industry to develop global cybersecurity standards to pave the way for a global 6G and an interoperable Internet of Things?

9:00-11:00 [CEST]
16:00-18.00 [KST]

Welcome

Ilsun YOU
Professor, Department of Information Security Engineering, Soonchunhyang University

Chair

Patryk PAWLAK
Brussels Executive Officer, EU Institute for Security Studies

Opening Inputs from Brussels and Seoul

Jakub BORATYŃSKI
Director, Digital Society, Trust and Cybersecurity, European Commission
Hwan Kuk KIM
Professor, Sangmyung University

Panelists

Jaesuk YUN
Korea Internet & Security Agency, ROK
Wiktor STANIECKI
Head of Cyber Policy Division, European External Action Service
Intaek HAN
Director-General, Jeju Forum Secretariat; Research Fellow, Jeju Peace Institute
Mareike OHLBERG
Senior Fellow, The German Marshall Fund of the United States

Session 4: Combatting Cybercrime

Criminals targeting health facilities to extort ransom during the coronavirus pandemic have triggered a broad international outcry and underscored the need for effective global cooperation against cybercrime. Meanwhile, a process launched by the UN resolution 74/247 adopted in December 2019 risks duplicating efforts under the Budapest Convention and to pre-empt the conclusions of the existing UN Open-ended intergovernmental expert group meeting on cybercrime (IEG) commissioned to study the threat of cybercrime and how UN member states should respond. The EU and South Korea have opposed the creation of a new global instrument. How do Brussels and Seoul promote and implement collective efforts on developing the capacity and skills of law enforcement and judicial authorities to apply cybercrime legislation? How can both sides make viable progress in bilateral, regional and interregional cybercrime cooperation?

11:15-13:15 [CEST]
18:15-20.15 [KST]

Welcome

Peter CHASE
Senior Fellow, The German Marshall Fund of the United States

Chair

Keun Won YANG
Professor, Korea University, ROK

Opening Inputs from Brussels and Seoul

Cathrin BAUER-BULST
Head, Unit Cyber Crime, DG Migration & Home Affairs, European Commission
Gi Bum KIM
Professor, Sungkyunkwan University, ROK

Panelists

Young Jin SONG
Professor, Korean National Police University
Heli TIIRMAA-KLAAR
Ambassador at Large for Cyber Diplomacy, Ministry of Foreign Affairs, Estonia
Hae-Sung YOON
Director, Korean Institute of Criminology
Tatiana TROPINA
Assistant Professor in Cybersecurity Governance, University of Leiden

13:15-13:30 [CEST]
20:15-20:30 [KST]

Conclusions

So Jeong KIM
Manager, Cybersecurity Policy Department, NSR
Hannes EBERT
Senior Advisor, The German Marshall Fund

About EU Cyber Direct & Its Partners

The EU Cyber Direct works to broaden the European Union's dialogues on cyber resilience, norms and CBMs with strategic partners, including South Korea. The project conducts research and facilitates dialogues among governmental and non-governmental cyber experts by organizing workshops in Europe and partner countries to discuss in an informal setting effective ways to jointly build a free, open, and secure cyberspace. It also seeks to disseminate knowledge on the EU's cybersecurity and internet governance policies and build bridges across regions and sectors. The project is funded by the European Commission under its Partnership Instrument Action *International Digital Cooperation – Trust and Security in Cyberspace*. It is jointly implemented by GMF, the European Union Institute for Security Studies and Stiftung Neue Verantwortung.

The National Security Research Institute (NSR) is a leading government-funded, national cybersecurity research institute, which was founded in 2000 by bringing together components related to information security and cryptography from the Agency for Defense Development (ADD) and Electronics and Telecommunications Research Institute (ETRI). It is responsible for the development of national cybersecurity policy and strategy, cryptography, encryption devices, cyber security products and technologies for the public and military sector as well as critical infrastructures. It is composed of 5 research divisions covering such missions along with Cyber Security Training and Exercise Center (CSTEC), and IT Security Certification Center (ITSCC).