EU-ROK CYBER CONSULTATIONS

RESILIENCE AND TRUST IN CYBERSPACE

Introduction

Cybersecurity has become a critical aspect of successfully managing the economic, political, and societal repercussions of the coronavirus pandemic. The European Union (EU) and the Republic of Korea (ROK) have recognized the need to address the immediate and long-term cybersecurity challenges by enhancing cybersecurity resilience and intensifying international cooperation. To build on existing institutional settings to achieve targeted results for greater resilience and trust in cyberspace, the EU Cyber Direct project and the National Security Research Institute (NSR) organized the Track 1.5 "EU-ROK Cyber Consultations: Resilience and Trust in Cyberspace" on October 6-7, 2020.

Including high-level officials from across EU and EU member state institutions and ROK ministries and agencies as well as non-governmental experts from Europe and South Korea, the consultations also helped build bridges across the multiple stakeholders and facilitate non-governmental input in government-dominated cyber norms-building processes. The consultations offered an informal space to exchange views and forge common understanding on pertinent issues related to 1) cyber resilience and the protection of critical infrastructure, 2) cyber conflict prevention and confidence-building measures (CBMs), 3) the geopolitics of 5G, and 4) cybercrime.

1. Cyber Resilience

- Participants exchanged best practices on protecting critical infrastructures (CIs) in the EU and the ROK. In South Korea, since the 2014 cyber-attack against a nuclear power plant, cybersecurity policy was focused on recovery rather than resiliency. The ROK is intending to develop and implement cybersecurity policies that include the concept of resilience. In the EU, the Network and Information Security (NIS) Directive and Cybersecurity Strategy are currently both being reviewed to reflect new priorities in the protection of CI. Participants suggested that both sides would need to develop a balanced mix of risk management, strategic partnerships, and the provision of global common goods, which carefully measures the benefits and costs of resilience, including for fundamental rights.
- Stakes and vulnerabilities in the finance sector were estimated as particularly high, and therefore resilience measures in this sector have evolved as a priority in both the EU and the ROK. In addition, participants noted a joint sense of urgency and parallel efforts to increase resilience in the global health sector.
- Both sides recognized the need for a more global approach regarding the protection of CI and identified various areas for increased EU-ROK cooperation, including increased information sharing related to risk management (e.g., standardizations of metrics), joint tabletop exercises and scenario planning, and investment in joint research projects.
- It was noted that cooperation on CI should not be limited to like-minded states; and that EU member states had hosted an Arria-Formula meeting at the UN Security Council on "Cyber-attacks against Critical Infrastructures" in late September.

This event is co-organised with

NSR 국가보안기술연구소 National Security Research Institute

Implementing organisations

ISS European Union Institute for Security Studies

G|M|F The German Marshall Fund of the United States STRENGTHENING TRANSATLANTIC COOPERATION

Stiftung Neue Verantwortung

This project is funded by the European Union.

- The EU and the ROK can use the high-level political recognition of the need of global cooperation on cyber resilience in the context of the coronavirus pandemic to double down on their efforts to protect CIs.

2. Cyber Conflict Prevention

- There was a high degree of convergence between both sides in the field of cyber conflict prevention, in particular regarding positions on the applicability of international law, the need to focus on the implementation of norms of responsibility state behavior, and CBMs. Participants called for a 2020 equivalent to a "red telephone", i.e., direct communication channels for cyber crisis situations.
- Whereas the EU imposed cyber sanctions for the first time in July, cyber sanctions and public attribution were perceived as "high risk" in the Northeast Asian environment given the ROK's enduring rivalry with the DPRK and an asymmetric rivalry with China. Speakers from the ROK warned against potentially counterproductive consequences of "naming and shaming" and suggested further developing diplomatic tools that are non-restrictive, including CBMs.
- Participants highlighted the need to build cyber capacity as a prerequisite for effectively implementing CBMs, including the development of national cybersecurity legislation and strategies to share information on national priorities and structures; the promotion of common cybersecurity terminology at the national level across agencies to facilitate dialogue with international partners; and the need for public-private and multi-stakeholder partnerships.
- It was suggested that prospective EU-ROK collaboration could coordinate more closely on the work at the Open-Ended Working Group (OEWG), align the CBM development and implementation efforts of regional organizations such as the ARF and OSCE, and enhance cyber capacity building collaboration tied to the goal of preventing conflict escalation, building on existing cooperation between the EU and the ROK's Global Cybersecurity Center for Development (GCCD) and Cybersecurity Alliance for Mutual Progress (CAMP).

3. The geopolitics of 5G

- The EU and South Korea both try to reconcile trade and risk management imperatives while building a form of strategic autonomy. While Brussels is implementing March 2019 recommendations on a concerted EU approach and has published a coordinated risk assessment on cybersecurity in 5G networks and a toolbox for mitigating risks as first steps of this process, Seoul delegated the decision of which technology to use for new 5G systems to its network operators. Participants highlighted that the ROK's economy would be particularly vulnerable to Chinese economic retaliation.
- While the EU's adoption of the toolbox on risk-mitigating measures on 5G in January 2020 was a unique example of coordination among member states, a European Commission report on its implementation published in July 2020 demonstrated that the EU would need to double down on its efforts.
- Participants emphasized the need for increased information sharing regarding certification schemes for ICT products.
- Both sides stressed the need for improved technical cooperation between the EU and ROK, proposing a multidisciplinary platform for both technical and political experts to discuss such issues. As a leading country in emerging technology fields such as AI and 6G networks, the ROK will continue to strengthen cooperation with the EU in this field.

4. Cyber Crime

- While the ROK decided to join the Budapest Convention in 2019, concerns remain about the specific requirements for adapting domestic legislation. Participants outlined the multi-level efforts underway in the ROK to meet the prerequisites to join the convention, including related to the storage of evidence, access to encrypted communication, and the ability to answer requests for evidence, which could benefit from conducting further comparative analyses with legislation in EU member states such as Germany, France, and Spain.
- Cross-border access to data remains a key priority for exchange, and both sides have invested increasingly in the issue.
- It was suggested that prospective cooperation can build on existing initiatives such as the “No More Ransom” initiative, the “Safer Internet Day” initiative, and dialogue between the ROK and the Council of Europe. Future cooperation could focus on bringing together diplomats and law enforcement agencies between like-minded countries to develop a strong position on protecting human rights and civil liberties in the ongoing negotiations at the UN General Assembly’s 3rd Committee; the development of a common approach for cybercrime capacity building work at UN negotiations and in the United Nations Office on Drugs and Crime (UNODC); and operational cooperation, such as joint projects and investigation teams (with Europol).
- Yet, participants noted that the pandemic also underlined that collaboration on cybercrime cannot be decoupled from discussions on data protection and privacy. While South Korea's use of surveillance technologies to mitigate the pandemic might complicate ongoing negotiations on its adequacy status, societies in Europe are likely to further turn inward. Building a secure cyberspace that is free and open will require the persistent engagement of multiple stakeholders in the diverse cyber policy landscape in Europe and South Korea.

Conclusion

During the EU-ROK Cyber Consultations, the need for enhanced cooperation between the EU and ROK in the fields of cyber resilience, cyber conflict prevention, 5G, and cybercrime was reiterated. The EU has been perceived in the ROK as an actor that, like itself, is seeking a “neutral” role in the evolving China-U.S. tensions. Although both sides expressed different perspectives on issues such as the use of restrictive measures in cyberspace, participants pointed to high levels of convergence in areas such as international law, the implementation of norms of responsible state behavior, and CBMs. Participants from the EU and the ROK also uniformly underscored the value of engaging non-government experts in bilateral, regional, and multilateral efforts to build resilience and trust in cyberspace. It was suggested that these recommendations are further considered at the upcoming EU-ROK Cyber Dialogue, tentatively scheduled for late November 2020.

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 Defence 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 Centre (CSTEC), and IT Security Certification Centre (ITSCC).