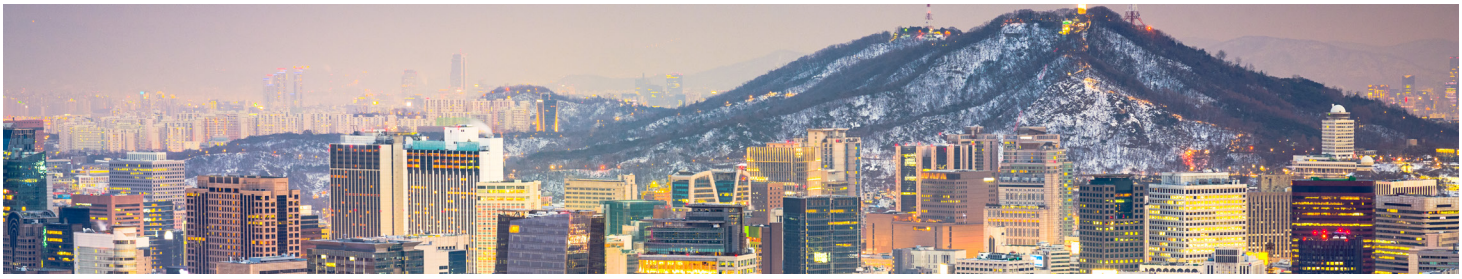
G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Transatlantic Take



The United States and the EU Should Not Underestimate Cyber Champions like South Korea

By Laura Groenendaal

The rapid digitalization of everyday life has brought cybersecurity to the forefront of international relations as states face increasingly sophisticated cyberattacks. As developments in cyberspace blur national borders and distinctions between state and non-state actors, states are making efforts to build a global framework to regulate cyberspace. So far, however, they have failed to reach a consensus.

Amid the rivalry between the West, Russia, and China in this field, it is easy to overlook the role of smaller states. However, the United States and the European Union should not overlook the importance of a country like South Korea, for example, with its digital prowess, extensive experience in cyber resilience, and strategic positioning in its region. It will be much needed for the West's aim to promote and maintain a free and open cyberspace, while Russia and China justify information controls for reasons of national security.

South Korea was not selected as member of the next UN Governmental Group of Experts (UNGGE) 2019-2021 on the use of information and telecommunications in the context of international security, whose 25 members will discuss issues such as the application of international law and norms for responsible state behavior in cyberspace. However, the Unites States and the EU should continue to enhance cooperation on cybersecurity and Internet governance with South Korea because of the country's digital prowess, extensive experience in cyber resilience and strategic positioning in the region.

Digital Prowess

South Korea is a front-runner in the field of cyber and digitalization. It digitalized incredibly fast. In 1995 less than 1 percent of the population used the Internet; by 2017 99.9 percent of households had access to it.1 This makes South Korea a global leader in connectivity and Internet access. Today, it has the world's fastest Internet and a highly developed information and communications technology sector. In April 2019 the country was the first to launch the 5G network nationwide.

Under what is called "the Fourth Industrial Revolution," the administration of President Moon Jae-In prioritizes innovative growth as part of economic policy and has promised to invest €1.7

1 ITU, "Korea (Rep. of) Profile", 2018.

billion by 2022 in technologies such as artificial intelligence, big data, and blockchain. Therefore, it is important for the United States and the EU to foster cooperation with South Korea in this field. In addition to the annual U.S.-Republic of Korea Information and Communication Technology Policy Forum and the recently established EU-Republic of Korea Digital Economy Dialogue, meetings between officials should take place more regularly and jointly funded research and development programs should be expanded.

Extensive Experience in Cyber Resilience

South Korea's digital prowess has also highlighted vulnerabilities to cyberattacks. Since 2009, it has suffered from an increasing number of cyberattacks, from distributed denial-of-service attacks on media corporations and government websites to ones for espionage purposes and financially motivated ones on financial institutions and cryptocurrencies—

> *"The academic community and civil society actors in the United States, the EU, and South Korea should be systematically involved in the debate and bring new ideas and perspectives through Track 1.5 dialogues and other formats.*
> *r*

some of which have been attributed to North Korea. As the conflict between South Korea and North Korea increasingly takes place in cyberspace, cyber resilience has become a matter of national security for the former, which has developed advanced legal frameworks, institutional structures such as a cyber warfare command, and educational programs to counter these attacks.

The United States and the EU, which face similar cyberattacks on critical infrastructure, would benefit substantially from exchanges of best practices with South Korea. They could also undertake cooperation or joint exercises between the U.S. Cybersecurity and Infrastructure Security Agency, the European Union Agency for Network and Information Security, and South Korea's National Cyber Security Center.

Strategic Positioning

As China's cyber edge in the region grows, South Korea finds itself compelled to hedge between its traditional ally the United States, on whom it historically has relied for security, and China as the emerging cyber power whose support is needed for a successful rapprochement toward North Korea.

This balancing act was displayed in the UN vote in December 2018 on the Russia- and China-supported resolution to establish an alternative to the UNGGE that would be open to all UN member states: the Open-Ended Working Group on "Developments in the field of information and telecommunications in the context of international security." While the United States and EU voted against the resolution, South Korea abstained.

The United States and the EU should discuss China's role in the region during official cyber dialogues with South Korea and address issues that might drive the latter away from those states promoting a free and open cyberspace. The United States and EU should also coordinate their approach toward South Korea in this regard, given that U.S. military power is an important factor for Seoul and the EU has the reputation in Seoul of being a stable and reliable diplomatic partner . Finally, the academic community and civil society actors in the United States, the EU, and South Korea should be systematically involved in the debate and bring new ideas and perspectives through Track 1.5 dialogues and other formats.

While the focus when it comes to the cyber domain is on large powers and UNGGE members, smaller states such as South Korea should not be forgotten. Persistent cooperation with these can provide significant benefits to the United States and the EU in terms of research and development, expertise, and strategic value that are highly needed in the competition for creating a global framework in cyberspace.

On March 18-22 Hannes Ebert and Laura Groenendaal conducted a research mission in Seoul as part of the EU Cyber Direct Project, an EU-funded project that aims to contribute to the development of a secure, stable, and rules-based international order in cyberspace in dialogue with strategic partners and regions.

The views expressed in GMF publications and commentary are the views of the author alone.

About GMF

The German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan. GMF does this by supporting individuals and institutions working in the transatlantic sphere, by convening leaders and members of the policy and business communities, by contributing research and analysis on transatlantic topics, and by providing exchange opportunities to foster renewed commitment to the transatlantic relationship. In addition, GMF supports a number of initiatives to strengthen democracies. Founded in 1972 as a non-partisan, non-profit organization through a gift from Germany as a permanent memorial to Marshall Plan assistance, GMF maintains a strong presence on both sides of the Atlantic. In addition to its headquarters in Washington, DC, GMF has offices in Berlin, Paris, Brussels, Belgrade, Ankara, Bucharest, and Warsaw. GMF also has smaller representations in Bratislava, Turin, and Stockholm.

1744 R Street NW
Washington, DC 20009
T 1 202 683 2650 | F 1 202 265 1662 | E info@gmfus.org
http://www.gmfus.org/