VUB ies INSTITUTE FOR EUROPEAN STUDIES
KF VUB KOREA CHAIR
Policy | brief

South Korea's Cybersecurity and International Cooperation

Issue 2019/08 • July 2019

by Rasmus Eriksson

Prompted by the exposed vulnerability of its highly connected society after North Korea's cyberattacks in recent years, South Korea has set out to improve its cybersecurity infrastructure. Whilst important steps have been taken to outline a national cybersecurity strategy, a further risk assessment shows that a considerable threat remains and that South Korea stands to benefit from integrating cybersecurity into its international security cooperation agenda. Improving intelligence sharing and organization should be prioritized considering the country's omission from the Convention on Cyber Crime, and the common international incentive of curbing North Korean offensive cyber capabilities makes such policy highly feasible.

Over the past decade, North Korea has proven itself to be one of the world's foremost threats in the realm of cyberwarfare; a surge of cyberattacks of increasing potency since the 7.7 DDos attack in 2009 has demonstrated the range of disruptive techniques which Pyongyang is capable of wherein South Korea is often the target. Attacks have been characterized by (but not limited to) hacking and obtaining sensitive government information, sabotaging the operation of banks, coordinating campaigns of misinformation alongside military exercises, and hacking of South Korean cryptocurrency exchanges. In a security context, North Korea's offensive cyber capabilities compensate for its inferior conventional military strength which in turn contributes to South Korea's asymmetric relationship with its neighbor. The response from Seoul in recent years is emblematic of the fact that any form of retaliation would either lack potential cyber targets or would appear disproportionate if military forces were mobilized. Instead, an approach of improving South Korea's own cybersecurity has been the chosen, and arguably appropriate course of action for the Korean Peninsula's overall security. Due to this, South Korea has decided to prioritize enhancement of their own cybersecurity as the appropriate course of action for the Peninsula's overall stability and security.

The government's establishment of the Cyber Command in 2010, its sponsorship of cybersecurity related departments in universities and its increased funding for cybersecurity defense measures are indicative of necessary steps being taken in this direction. However, problems remain in other areas such as information sharing and organizational processes. Despite not being subject to any larger reported cyberattacks in 2018, except for an October incursion by unnamed hackers where data was stolen from the Defense Acquisition Program Administration, the growing network dependency makes the country consequently more vulnerable to cyberattacks. The scope of societal areas susceptible to cyberattack due to widespread incorporation of the Internet of Things (from hospitals and military bases to democratic processes) makes the potential damage of a coordinated attack devastating in real security terms as well as financial costs. Seoul, however, is not alone in dealing with this security concern. Given how cybersecurity threats can easily transcend national boundaries, it would make little sense for one country or company to combat such threats on their own.

The Bilateral Cyber Consultations held between the US and South Korea in the wake of the WannaCry ransomware cyber-attacks of 2017 is a sign of Seoul taking the international scope of this issue seriously. Recognizing that multiple states outside of the Korean Peninsula share a similar interest in deterring North Korea from employing its offensive cyber capabilities is a step in the right direction, as well as ensuring that such disruptive cyberattack attempts fail in the future. However, the Trump administration has displayed intentions of downgrading the priority of cybersecurity issues by removing the cybersecurity coordinator from the White House. Additionally, American rhetoric surrounding security guarantees in Asia also casts doubt on its promises. Skeptics suggest that Seoul ought to look for cooperative measures with the EU, in addition to US-ROK cyber relations, to realize their full security potential.

Strengthening cooperation with the EU and its member states would provide South Korea with a contemporary parallel to its own high degree of interconnectedness and a relationship where common threats emanating from Russia and North Korea serve to unite defense policy priorities. Seoul should consider ratifying the Budapest Convention on Cybercrime as a first measure of incorporating cybersecurity into their ongoing dialogue with the EU. It should also consider joining the NATO-accredited Cooperative Cyber Defence Centre of Excellence in Tallinn. Aside from promoting a rule-based international order in cyberspace, improving Seoul's cyber diplomacy and relations means; learning and sharing respective approaches on securing Internet of Things devices, promoting information exchange in order to limit malicious cyber activity, and working together with the EU in capacity building efforts. International cooperation on cybersecurity and operationalizing these measures is not an easy task. However, a few measures which may facilitate this cooperation are following the model of UK-Japan cyber-focused bilateral dialogues and utilizing the framework of the EU-ROK relationship in other areas of trade (especially joint 5G development measures) and security. The Japanese government's recent announcement that it is planning to develop a counter-attack computer virus intended for defensive purposes (with North Korea most likely in mind) demonstrates the regional opportunities for planning on the basis of collective goals as well as the necessity for communication so as to avoid a cyber arms race between potential allies.

Improving cybersecurity cooperation with the EU would also not exclude the option of China as a regional security partner. Traditionally, Beijing has been conceived as a cyber 'aggressor' in the sense that its offensive capabilities have been used for cyber espionage in many countries including South Korea. However, China's future espionage motivations may be thwarted in catering to their current priorities of establishing a stronger cybersecurity infrastructure and an interest in stabilizing and policing cyberspace - which in part requires international cooperation. Thus, despite past grievances, the potential of China-ROK cyber relations may be promising. And most importantly, a true deterrence system will require a true multilateral process for the adoption of international cyber space norms and for legal enforcement. A potential feature of any future brokered peace deals could conceivably include a penalty mechanism monitored by both the EU and China.

The need for upholding momentum in cybersecurity developments is of utmost importance for South Korea's future resilience against digital threats and forms an incentive for Seoul to secure an important role in international cyber cooperation.

ABOUT THE AUTHOR

Rasmus Eriksson is a KF-VUB Korea Chair Events and Research Intern and student in Politics and International Studies at the University of Warwick. He is the winner of the 2018 KF-VUB Korea Chair Pan-European Korean Peninsula Security Writing Contest.

in Rasmus Eriksson

The present publication has been conducted by IES-VUB in full independence.

All KF-VUB Korea Chair publications can be found on www.korea-chair.eu.

The KF-VUB Korea Chair (www.korea-chair.eu) at the Institute for European Studies (www.ies.be) is the primary contact point in Europe on policy issues related to the Korean Peninsula and plays a strategic role in furthering Europe-Korea relations.

As a joint initiative between the Korea Foundation and Vrije Universiteit Brussel (VUB), the Chair acts as an independent platform in Brussels and across Europe to advance academically rigorous and informed discussions on policy questions that are of relevance to Europe and the Republic of Korea. It conducts policy research and discussions on a wide range of areas, with special focus on the security of the Korean Peninsula, Europe-Korea relations and South Korea's foreign policy.

The Chair holder is Dr. Ramon Pacheco Pardo who is also Reader in International Relations at King's College London.

The KF-VUB Chair
at the Institute for European Studies
is a joint initiative between the
Korea Foundation (KF) and
Vrije Universiteit Brussel (VUB)
www.korea-chair.eu

Institute for European Studies
Pleinlaan 5
B-1050 Brussels
T: +32 2 614 80 01
E: info@ies.be
www.ies.be