ARI 89/2023
4 October 2023

South Korea-NATO cybersecurity cooperation: learning to work together in the face of common threats

Ramón Pacheco Pardo | Professor in International Relations at King's College London and KF-VUB Korea Chair at the Institute for European Studies of Vrije Universiteit Brussel. Member of the Scientific Council of the Elcano Royal Institute | @rpachecopardo

Theme[1]

This paper analyses the scope for South Korea and NATO cooperation in the area of cybersecurity in the context of their growing ties and the common threats they face.

Summary

South Korea and NATO are taking their relationship to new levels in accordance with the Individually Tailored Partnership Programme agreed in July. Of all the areas in which they are deepening ties, cybersecurity stands out as a priority for both. Seoul and the Transatlantic Alliance have the capabilities and shared interests to develop a wide-ranging partnership in this area.

Analysis

South Korea and NATO are rapidly upgrading bilateral relations within the context of NATO's engagement and partnership with the Asia-Pacific Four or AP4, more recently also labelled the Indo-Pacific Four: Australia, Japan, New Zealand and South Korea (ROK) itself. The growing links between South Korea and NATO were most recently epitomised by the Individually Tailored Partnership Programme agreed by the two partners during the Vilnius NATO Summit held last July. This programme also symbolised another key feature of the relationship between Seoul and the Brussels-based organisation: the two partners are moving from dialogue to practical cooperation. That is, they are shifting from saying to doing. This has implications not only for NATO but also for the EU and NATO's European members.

Indeed, the NATO-South Korea relationship in general and in the area of cybersecurity in particular have evolved dramatically over the past 20 years to reach new heights as of 2023. The two countries launched a regular dialogue and cooperation in 2005, starting within the context of cooperation between the ROK's Armed Forces and NATO troops deployed in Afghanistan. There was thus a very limited focus on cybersecurity, which back then South Korea saw more as a theoretical than a real threat. NATO and South Korea then signed an Individual Partnership and Cooperation Programme in 2012. Even though cybersecurity was included as an area in which to work together, Seoul had only

[1] The author would like to thank Mario Esteban and Raquel Jorge for their comments and suggestions. Any remaining errors are his own.

recently launched its first official cyber crisis countermeasures and cybersecurity was considered secondary to the nuclear and other traditional security threats from North Korea. The Individually Tailored Partnership Programme is therefore arguably the first South Korea-NATO agreement in which cybersecurity takes centre stage at the same level as other areas of cooperation. It is indeed highlighted as an area in which to boost ties.

For context, there are multiple areas of (potential) cooperation between South Korea and NATO. They include cybersecurity itself, non-proliferation of weapons of mass destruction, defence industrial cooperation and new weapon systems development, maritime security, economic security and climate change. This reflects that from NATO's perspective South Korea has become a trusted partner with strong military, economic, technological and diplomatic capabilities, as well as shared values. It also reflects that NATO continues to evolve from a purely military organisation with a defence mandate, to an organisation taking a holistic and forward-looking view of security encompassing both traditional and non-traditional elements. This is the so-called 360-degree approach adopted by NATO in relation to its core functions, as reaffirmed in the 2022 Strategic Concept: deterrence and defence, crisis prevention and management, and cooperative security. Despite its understandable short-term focus on providing assistance to Ukraine in its defensive war against Russian aggression, NATO is taking a long-term approach towards the security of its members and also in maintaining cooperation with its global partners, including the AP4. Depending on the partner and the issue-area, the focus will be on one or another of the three core functions.

Arguably, cybersecurity is in fact one of the areas in which formal relations between Seoul and the North Atlantic organisation are strongest at the time of writing. After all, South Korea became the first Asian country to become a member of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) in May 2022. Based in Estonia, this is NATO's main cybersecurity agency focusing on education, training and cyber exercises for both NATO members themselves and for partners. Thus, it is the agency of most interest for South Korea at this point, when cybersecurity cooperation is strengthening but still at an early stage. South Korea's decision to join shows the importance that the country's policy-makers afford to cooperation in this domain, both with NATO as well as with the EU and European countries. NATO's decision to allow South Korea to become a member indicates Seoul's status as a trusted partner in possession of capabilities and expertise that the organisation finds valuable. At the same time, it should be noted that South Korea only recently started to prioritise cybersecurity to the same extent as other security domains, and thus lags behind the US and many other NATO members.

The focus on cybersecurity makes sense for both parties since it is a global issue in which they both feel vulnerable and under threat. In particular, China-Russia-North Korea potential cooperation in this area as well as each country's own, independent cyberattacks on third parties—including South Korea, NATO and NATO members—is a key reason why this is a global threat. In this respect, cybersecurity epitomises the growing belief among Asian, European, and US policymakers and experts that the Euro-Atlantic and Indo-Pacific theatres have merged to become a single security sphere. It is

thus a priority area in which we can expect South Korea-NATO cooperation to continue to flourish.

Cooperation in the area of cybersecurity

Cybersecurity cooperation between South Korea and NATO has been a priority for the liberal Moon Jae-in government (2017-22), which drove the process leading to Seoul joining the CCDCOE, and the conservative Yoon Suk-yeol government (2022-present), which included this domain in its 2023 partnership programme with NATO. This bipartisan consensus in South Korean foreign and security policy, while normal for a country with a decades-old grand strategy, signals that the country's elites recognise the growing importance of cybersecurity as a new domain where hybrid warfare is taking place. From a South Korean perspective, cyber defence is the top priority given the direct threat from North Korea, which regularly launches cyberattacks on South Korean government agencies, private firms and the military. Cyber warfare would come second, in consideration of what South Korea sees as a need to retaliate against Pyongyang and potentially launch pre-emptive cyberattacks to counter the threat that it feels from its neighbour. Other areas such as cyber norms would be secondary, since South Korea generally believes in international norms but also considers that North Korea, China or Russia are unlikely to abide by them in the cybersecurity domain.

Cooperation within the context of NATO does not occur in a vacuum though. A total of 22 NATO members are also EU members, and the EU is also accelerating cybersecurity cooperation with South Korea. This is epitomised by the Digital Partnership Agreement signed by Seoul and Brussels in November 2022, one of only three between the EU and Asian countries together with those agreed with Japan and Singapore. Furthermore, there is also bilateral cooperation between South Korea and specific countries. One particularly interesting case is the Netherlands, arguably the European country that has the strongest bilateral links with South Korea in the cybersecurity domain. As a case in point, South Korea sent a high-level delegation to the Summit on Responsible AI in the Military Domain hosted by the Netherlands in February 2023. Plus, both South Korea and NATO, as well as NATO members, are engaged in cybersecurity cooperation with other partners such as the US, Australia, Canada, the EU, Japan, New Zealand, Singapore and the UK. These connections are creating a network of links in the cybersecurity domain.

One area in which NATO and South Korea are moving from talking to doing is intelligence and information sharing. As an alliance that quickly recognised the importance of the cyber domain in the era of hybrid warfare, NATO has long been harnessing the intelligence and information gathering capabilities of its members to boost the security of each and every one of them as well as the organisation as a whole. South Korea, in contrast, was relatively slow in recognising the importance of cyber warfare in today's security environment. The Lee Myung-bak government released the Comprehensive Countermeasures for National Cyber Crisis in September 2009. Seoul, however, only issued its first National Cybersecurity Strategy (NCS) in April 2019, under the Moon government. The NCS established a clear commitment to international cooperation in the area of cybersecurity for the first time, while also ushering a reform of the Ministry of National Defence (MND) that elevated cybersecurity to the same level as other risks to South Korean security. Seoul thus enhanced its cybersecurity capabilities, including

intelligence and information gathering and sharing. This prioritisation of the cyber domain has continued under the Yoon government.

NATO can therefore share intelligence and information sharing techniques with a South Korea that is still lagging behind the organisation and most of its members, but which is seeking to catch up. In particular, NATO's capabilities in this area targeting countries and regions including China, Russia or Iran and the broader Middle East are of great interest to South Korea. Seoul, meanwhile, has unparalleled intelligence and information on North Korea, one of the most active state users of cyber activities to boost its own security and undermine that of its opponents. For obvious reasons, North Korea is and will continue to be the main target of South Korean cyber activities and counter measures. This is an asset for NATO. Plus, NATO and South Korea should be in a position to provide mutual assistance in case of a cyber crisis, such as cyber-attacks on one or the other by third parties.

Tabletop exercises is another area in which cooperation between NATO and South Korea is poised to grow. South Korea only decisively started to promote international cooperation in the cyber domain following the launch of its NCS in 2019. Both the previous Moon government and the current Yoon government, however, are keen to catch up. This potentially includes tabletop exercises involving the ROK's Armed Forces, government agencies and the private sector. All of them have been mobilised by the Moon and Yoon governments to boost the cybersecurity of South Korea in cooperation with third parties. A case in point is enhanced South Korea-US-Japan trilateral cooperation. Another example is the ties between South Korea and the Netherlands, a country with which with Seoul has engaged in this type of exercises.

South Korea's July 2023 partnership programme with NATO and membership of the CCDCOE have laid the foundations for regular cybersecurity tabletop exercises between the organisation and Seoul. Furthermore, these exercises can include the other AP4 members, since they also have strong links with the CCDCOE –particularly Australia and Japan–. Considering that cyber-attacks often have more than one target located in more than one country, it makes sense for tabletop exercises to involve a range of countries.

Towards a stronger South Korea-NATO cybersecurity cooperation

Institutionalised regular expert exchanges and track-1.5 meetings are one more area of NATO-South Korea cooperation in cybersecurity that should be strengthened. The US and the EU are boosting this type of link with South Korea, with Seoul showing its interest in holding regular meetings at the director-general level. Other countries such as the UK are also starting to formalise their links with South Korea in the digital and cyber domains, leading to similar exchanges. Germany and Poland, as well as the EU, are among the other actors that have expressed an interest in this type of meetings. In the case of the EU, its Digital Partnership Agreement with South Korea and the regular bilateral dialogue on cyber and digital matters have already laid the foundations to take such a step. NATO should also embrace this format with South Korea, which, even though it may have less obvious practical implications than intelligence and information sharing or tabletop exercises, is a sign of political commitment to cybersecurity cooperation. Plus, NATO

members, including those hailing from Europe, could combine their own bilateral exchanges to those taking place at the NATO level.

Institutionalising regular exchanges and meetings would also help to bring in NATO member officials and European, North American and South Korean private sector and non-governmental organisation experts on an ad hoc basis and as necessary. This is the approach being pursued by the US and the EU. Given its military nature, NATO could lead in institutionalised and regular engagement with South Korea's MND beyond the links that the ministry has already established with Seoul's ally –the US–. This would be a further boon to NATO-South Korea cooperation, since most dialogues involving South Korea are led by the Ministry of Foreign Affairs or some other specialised ministry, rather than the MND.

Third-party digital and cyber capacity building is another area in which NATO and South Korea should be moving into more concrete action. Even though South Korea is relatively new to prioritising cybersecurity to the same extent as other security domains, as explained above, its high rate of digitalisation and its burgeoning security ties with countries in regions such as South-East Asia and South Asia means that there is strong demand for its involvement in capacity building. Certainly, NATO's involvement in this type of activities outside its own members and strongest partners could prove controversial. But partnering with South Korea, as well as other AP4 countries, could be a way to overcome scepticism over the organisation's reach beyond Europe. This seems to be the EU's approach, with Brussels' digital partnership agreements with Japan, Singapore and South Korea itself including a capacity-building component. Plus, the Camp David joint-statement issued by South Korea, the US and Japan also includes a commitment to cyber-capacity building. Even though the specific types of capacity building activities are yet to be announced, this commitment, if put into action, would help South Korea to also engage in capacity building together with its core ally and increasingly close neighbour.

In this respect, cyber resilience is a concern across different parts of the world. Governments and societies worldwide have shown their concern about the potential for the cyber space to be weaponised, resulting in unwelcome interference in domestic affairs. European countries such as Finland, Germany, the Netherlands and Sweden, for instance, emphasise cyber resilience as part of their security strategies. NATO could benefit from partnering with South Korea as it seeks to support the cyber resilience of third parties, including its partners in Asia such as India and Mongolia. South Korea, for its part, is keen to become more involved in the training, education and joint exercises with third parties willing to learn from its experience and to share their own.

The NATO-South Korea partnership programme signed during the Vilnius Summit emphasises emerging technologies as an area to be prioritised by the two partners. Arguably, South Korea's advanced capabilities in sectors such as 5G/6G, AI, semiconductors and quantum computing is one of the key reasons why NATO is keen to boost bilateral ties. In particular, new technologies are arguably the main area of competition between the US and China, and European countries such as Germany, the Netherlands and the UK are among those that have been dragged into it and thus have a particular interest in this issue. From this follows that it is one of the main areas in which

NATO sees China as a competitor, given Washington's leading role in the North Atlantic organisation. Many if not all of these technologies are of dual use, and therefore have a strong military angle. In this respect, NATO's newly launched Defence Innovation Accelerator for the North Atlantic (DIANA) and NATO Innovation Fund (NIF) could serve as tools to develop new technologies with partners –including Seoul–.

South Korea faces the direct threat of North Korea and is regularly ranked as one of the most innovative countries in the world. This explains its vast investment in new technologies, both military and civilian. In fact, this is a reason why South Korea is often cited as a potential partner in the second pillar of AUKUS, which focuses on the research and development of new military technologies and weapons systems. Considering that South Korea has experience in developing new military capabilities with partners, such as a jet fighter with Indonesia, and has announced plans to seek to develop new weapon projects with NATO member Poland, there is clear potential for the North Atlantic organisation to quickly scale up cooperation with Seoul in this area.

Another area in which NATO and South Korea can boost ties is critical digital infrastructure resilience. This includes command and control centres, data centres, transmission cables and other organisations and equipment essential to the well-functioning of the digital and cyber domains. In the case of NATO, this is an issue that the organisation has long been aware of. It is fair to say that in the case of South Korea the concern is more recent. However, regular cyber-attacks from North Korea, especially, as well as by China and, to an extent, Russia, have served to awaken South Korean attention to this issue. As with NATO members, South Korean government officials and private sector stakeholders alike fear that a cyber-attack could paralyse certain sectors of the country's government, economy or military. The EU-NATO Task Force to strengthen critical infrastructure resilience could serve as an example to drive South Korea-NATO cooperation in this area, as well as with third parties, including capacity building.

Since this is a shared concern for NATO and South Korea, it should be possible to incorporate critical digital infrastructure resilience into some of the activities outlined above, including intelligence and information sharing, tabletop exercises and institutionalised and regular exchanges and meetings. After all, the digital infrastructure cannot be disentangled from cybersecurity. And since cyber-attacks often have more than one target, as mentioned above, enhancing South Korea's cyber resilience is of interest to NATO even from the perspective of its own security and vice versa.

More broadly, cybersecurity is closely linked to issues such as foreign information manipulation and interference (FIMI), industrial espionage and economic security. In other words, it has implications that go beyond NATO's military focus but that are closely related to the well-functioning of its members' politics and economics. It is the same for South Korea. In particular, democracies are considered to be more vulnerable to this type of activities given their more open political systems, societies and, often, economies. Therefore, NATO and Seoul have an interest in cybersecurity cooperation that goes beyond the area of security and defence. Examples include industrial cybersecurity, crucial for an industry-heavy economy such as South Korea, and export controls and FDI

screening at a time when industrial strategy is making a comeback and the protection of domestic industries has again become an acceptable goal.

Take the case of FIMI. South Korea has only very recently started to systematically consider the potential negative consequences of countries such as China and North Korea seeking to spread fake news and misinformation. This has become an even bigger threat given the potential for Artificial Intelligence (AI) to generate realistic fake images relatively easily. Thus, South Korea is now engaged in discussions about FIMI with the US and the EU, as well as with European countries including Germany and the UK. There is a clear potential for NATO to include this topic in its engagement with South Korea. Industrial espionage and economic security, meanwhile, are of concern to NATO given its ever-expanding understanding of security and also to high-tech and globally-integrated South Korea. Therefore, it makes sense to include them in NATO-South Korea cooperation in the area of cybersecurity.

Less likely in the short term but of potential interest in the future could be South Korea-NATO cooperation in cybersecurity confidence-building measures (CBMs) with countries such as China and Russia, along with other partners. Certainly, CBMs with any of the two as of 2023 seems unlikely –especially with a Russia that persists in its aggression against Ukraine. But NATO members have been seeking to develop universal cyber rules since the turn of the 21st century, including via the Budapest Convention on Cybercrime signed in 2001. And agreeing to global rules would certainly reduce cybersecurity risks for NATO, its members, South Korea and their partners. Thus, this is a long-term goal that should not be totally abandoned.

Conclusions

South Korea and NATO are in the process of moving their partnership from words to deeds. In South Korea there is palpable excitement at the prospects of deeper ties with the North Atlantic organisation, regardless of whether progress is speedy or slow and publicly advertised or kept more private. NATO, meanwhile, has had a strong China focus for some years now, and is aware that there is a need for cooperation with South Korea and the other AP4 countries to address the concerns that the organisation has. This dates back to the London Summit of 2019, which mentioned China for the first time, followed by internal discussions since then, and reinforced by the inclusion of China in the 2022 Strategic Concept, as well as in the 2023 statement from the Vilnius Summit. For some NATO members, above all the US but also Canada, Lithuania, Norway and the UK, this focus on China has been reinforced by their diplomatic and economic tensions with Beijing. Since the interest in cooperation with the other is mutual and both partners agree that dialogue should transform into action, we should expect cooperation to continue to move forwards.

Cybersecurity is an area in which links between the two partners are already relatively strong and yet, crucially, much more could be done building upon existing structures. These include the Individually Tailored Partnership Programme agreed in July 2023 and Seoul's membership of the CCDCOE since May 2022. NATO and South Korea have a solid basis on which to build an enduring partnership in the area of cybersecurity, with a strong working level component that will ensure a continuation even following changes

in leadership. In fact, cybersecurity cooperation between South Korea and NATO took a substantial move ahead under Moon that has continued under Yoon.

Strong ties between South Korea and NATO in the area of cybersecurity would be hugely beneficial for the overall links between the two. It would help political and military leaders in both the Asian country and the North Atlantic organisation show that their partnership is not merely rhetorical but actually has practical benefits. After all, South Korea-NATO relations ultimately have to benefit the peoples in both. Cybersecurity will help to show what some of these benefits are.