Sanctions against North Korea: From the UN Security Council to a Coalition of the Willing?

Eric J. Ballbach

December 2023

GCSP Policy Brief No.12

GCSP
Geneva Centre for Security Policy

Geneva Centre for Security Policy

The Geneva Centre for Security Policy (GCSP) is an international foundation that aims to advance global cooperation, security and peace. The foundation is supported by the Swiss government and governed by 54 member states. The GCSP provides a unique 360° approach to learn about and solve global challenges. The foundation's mission is to educate leaders, facilitate dialogue, advise through in-house research, inspire new ideas and connect experts to develop sustainable solutions to build a more peaceful future.

The GCSP Policy Briefs Series

The GCSP Policy Briefs series addresses current security issues, deduces policy implications and proposes policy recommendations. It aims to directly inform policy- and decision-making of states, international organisations and the private sector.

Under the leadership of Ambassador Thomas Greminger, Director of the GCSP, the series is edited by Professor Nayef Al-Rodhan, Head of the Geopolitics and Global Futures Programme, and Mr Tobias Vestner, Head of the Research and Policy Advice Department, and managed by Ms Christine Garnier Simon, Administration and Coordination Officer, GCSP Geopolitics and Global Futures.

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
E-mail: info@gcsp.ch
www.gcsp.ch

ISBN: 978-2-88947-422-6

About the author

Dr Eric J. Ballbach serves as Korea Foundation Visiting Fellow at the German Institute for International and Security Affairs (Stiftung Wissenschaft und Politik, SWP) in Berlin. He previously served as the director of the Research Unit “North Korea and International Security” at Freie Universität Berlin’s Institute of Korean Studies. His research focuses on North and South Korean foreign and security policies, especially North Korea's participation in international organizations, EU-Korea relations and identity politics on the Korean peninsula. Dr. Ballbach advises the German Parliament and various Ministries on Korea-related issues and he regularly participates in various informal Track 1.5 initiatives involving high-ranking representatives from the DPRK, South Korea and the U.S.

Introduction

Since the breakdown in 2019 of high-level diplomacy with North Korea (officially the Democratic People's Republic of Korea, or DPRK) and as a result of the five-year military modernisation plan that the country announced in January 2021, it has steadily expanded its military capabilities. It has not only conducted an unprecedent number of missile tests and in the process introduced a range of new missile technologies, but recently also introduced a new law that makes significant changes to its nuclear doctrine.[1]

At the same time, the rapidly changing geopolitical context, most vividly exemplified by the intensifying US-China rivalry and Russia's war against Ukraine, not only makes a resolution of the international community's conflict with North Korea over its nuclear weapons and military capabilities even less likely, but strains the central mechanism used by the international community to deal with North Korea during the past years, i.e. the imposition of sanctions through the UN Security Council (UNSC). Despite the unprecedented quantitative and qualitative progress in North Korea's military build-up, the UNSC has imposed no new sanctions on the country since 2017.

This Policy Brief examines why and how the UNSC stopped being the central theatre for imposing sanctions on North Korea and highlights the security challenges that result from this shift. Next, it addresses the most crucial implications of these security challenges. The analysis includes a discussion of the central actors driving new decisions to impose sanctions on North Korea outside the framework of the UNSC, and how these sanctions target one of the country's most crucial sanctions-evasion mechanisms: its cybercrime programme. Based on this analysis, the brief offers policy recommendations that underscore the value of recent coordination initiatives in the field of sanctions and discusses what more needs to be done.

[1] The new law in effect allows pre-emptive nuclear strikes if North Korea detects an imminent attack of any kind, including one using weapons of mass destruction, aimed at its leadership and the command organisation of its nuclear forces. For an English translation of the new law, see KCNA Watch, "DPRK's Law on Policy of Nuclear Forces Promulgated", 9 September 2022, https://kcnawatch.org/newstream/1662721725-307939464/dprk%E2%80%99s-law-on-policy-of-nuclear-forces-promulgated/.

Security challenges

Strained mechanisms for dealing with North Korea

Ever since North Korea's first nuclear weapon test in 2006, sanctions have been one of the central mechanisms that the international community has used in its efforts to deal with the country's nuclear and military ambitions, and in the past few years have become central to these efforts. While numerous countries imposed their own unilateral sanctions on North Korea, the main theatre for the imposition of sanctions since its first nuclear weapon test has been the UNSC, which passed a total of ten resolutions imposing sanctions between 2006 and 2017. As already mentioned, however, the UNSC has imposed no new sanctions on North Korea since 2017 – despite Pyongyang's unprecedented qualitative and quantitative progress in expanding its nuclear weapons and military capabilities in recent years. There are two main reasons for this.

Diplomatic efforts in 2018-2019: consequences and eventual failure

A window for diplomacy unexpectedly opened in 2018 and early 2019 following a period that had seen the adoption of the most stringent sanctions yet imposed on North Korea. These toughened sanctions were introduced in 2016 and particularly in 2017 to respond to the country's continued nuclear weapons and missile tests and were aimed at undermining the functional operation of the North Korean state. Instability and tensions on the Korean Peninsula, which had been rising over the 2010s, became particularly acute in late 2017.

The protagonists in the conflict over North Korea's nuclear weapons programme then quickly moved from confrontational behaviour using war rhetoric towards a political détente and opening, culminating in several inter-Korean and US-North Korean summit meetings. Yet in the end the historic meetings between the then-US president, Donald Trump, and North Korean leader Kim Jong Un failed to improve their countries' relations and the security situation, because basically their positions were too far apart. The failed diplomatic efforts led to a breakdown of any substantive dialogue with North Korea. But not least to give diplomacy some room to manoeuvre, for the time being further sanctions were not introduced in the UNSC following the establishment of diplomatic contacts with North Korea.

Changing strategic interests in a confrontational geopolitical context

Despite disagreements among UNSC members (e.g. regarding the logic of sanctions and their respective reach and clout), until 2017 there was overall support for the imposition of sanctions on North Korea through the UNSC – with the United States and China even jointly preparing specific proposals. The unanimous adoption of sanctions in reaction to North Korea's repeated nuclear weapons and missile tests – including the qualitatively stronger sanctions of 2016 and 2017 – reflects the international community's consensus in dealing with North Korea and the shared perception of the threat that these tests

posed. Since 2017, however, Beijing and Moscow have resisted attempts to impose further sanctions on North Korea, arguing that sanctions alone are not the solution and that other measures such as dialogue and engagement are necessary to address the issue.

More importantly, the deepening strategic rivalry between the United States and China, as well as Russia's war against Ukraine, significantly altered the geopolitical context, which in turn had a direct impact on Russia's and China's strategic considerations and priorities in terms of dealing with North Korea. North Korea's strategic value has arguably increased in the context of the emerging power-bloc politics. The North Korean-Russian summit in September 2023, during which the respective heads of states pledge to forge closer ties, is only one of several recent examples. As a consequence, it is expected that the UNSC will no longer be the central space or theatre for sanctions against North Korea, because Moscow and Beijing are highly unlikely to support them, resulting in their being vetoed. In fact, in May 2022 Russia and China for the first time vetoed a US-drafted UNSC resolution to strengthen sanctions on North Korea following its repeated ballistic missile tests in violation of previous UN resolutions.

Policy implications

New actor constellation and new focus in dealing with North Korea

As a result of the UNSC's inability to impose new sanctions, a new actor constellation emerged. Currently an informal "coalition of the willing" is taking the lead to impose coercive measures in the form of sanctions on North Korea. It includes groups of states, such as the G7, as well as individual states, such as the United States, Japan, and South Korea (officially the Republic of Korea, or ROK). Through their actions and the UNSC's inaction, the main theatre for sanctions is being shifted outside the UNSC. Another trend is the shift in the thematic focus of these more recent sanctions. They respond to evolving security threats emanating from North Korea's increased capabilities and efforts in the area of cybercrime.

Central actors driving sanctions outside the UNSC

The G7 group of countries have repeatedly voiced their frustration with the UNSC's inaction. For example, the statement adopted after the G7 foreign ministers meeting in March 2023 refers to the "stark contrast between the frequency of North Korea's repeated blatant violations of UNSC [Resolutions] and the UN Security Council's corresponding inaction because of some members' obstruction".[2] The statement further holds that "North Korea's reckless behaviour demands a swift and unified response by the international community, including further significant measures by the UNSC. We call on all UN Member States to fully and effectively implement all UNSC [Resolutions], and for the UNSC Members to follow through on their commitments".[3] Similarly, in a statement issued after the G7 summit held in Hiroshima in May 2023, the group stated that "It is critical that sanctions be fully and scrupulously implemented by all states and remain in place for as long as North Korea's WMD [weapons of mass destruction] and ballistic missile programs exist".[4]

Japan is clearly attempting to use its G7 presidency to bring crypto regulation and sanctions to the fore of discussions. For instance, at the latest G7 meeting of central bank governors and finance ministers, an official from the Japanese Ministry of Finance criticised the fact that not enough is being done to stop North Korean crypto hacks, and that, in spite of sanctions, North Korea is

[2] Federal Foreign Office of Germany, "G7 Foreign Ministers' Statement on the Launch of an Intercontinental Ballistic Missile by North Korea", Press Release, 19 March 2023, https://www.auswaertiges-amt.de/en/newsroom/news/g7-north-korea-launch-intercontinental-ballistic-missle/2588604.

[3] Ibid.

[4] The White House, "G7 Leaders' Hiroshima Vision on Nuclear Disarmament", Statement, 19 May 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/19/g7-leaders-hiroshima-vision-on-nuclear-disarmament/.

still "able to continue its missile and other activities".[5] Having adopted one of the strictest crypto regulatory regimes in the world, Tokyo hinted that other nations needed to follow its lead (and perhaps Washington's) to help block North Korean cyber raids.

With the UNSC effectively paralysed, in 2021 groups of states and individual states resumed sanctions activities against North Korea following a year of unprecedented weapons testing activities. As such, a range of – technically unilateral, yet increasingly coordinated – sanctions were imposed in 2022 and 2023, most notably by the United States, South Korea, and Japan. After only annually renewing the existing sanctions regime without adding additional measures between 2019 and 2021, the European Union (EU), through two additional sanctions decisions in April and December 2022, added 16 individuals and eight entities involved in financing North Korea's nuclear programme to its sanctions list.

The latest sanctions decisions reflect an increasing coordination among some of the major actors driving new sanctions against North Korea, mainly the United States, South Korea and Japan, who repeatedly imposed sanctions in unison, most recently in August and September 2023. It has to be noted, however, that all the sanctions adopted since 2022 have been additional designations, and as such no new structural sanctions have been imposed on North Korea since 2017. While this seems rather lacklustre, given that country's dramatic military build-up, the Panel of Experts that assists the UNSC's DPRK Sanctions Committee has repeatedly called for such additional, targeted designations.

Main targets of new sanctions: addressing North Korea's cybercrime activities

North Korea's cyber capabilities are considered to be highly sophisticated and its willingness to engage in cyber attacks for financial gain or political purposes has made it a significant threat in the cyber security landscape. In response, the latest sanctions decisions adopted in 2022 and 2023 have identified and addressed North Korea's cyber activities as one of its two crucial sanctions evasion mechanisms (together with illegal ship-to-ship transfers).[6]

In 2019 UN sanctions monitors reported that North Korea had generated an estimated US$2 billion over several years to fund its weapons of mass destruction programmes using widespread and increasingly sophisticated cyber attacks. South Korea estimated that North Korean-linked hackers stole virtual assets worth US$630 million in 2022, while the crypto analysis firm Chainalysis estimates that North Korea stole approximately US$1bn. "A higher value of cryptocurrency assets was stolen by DPRK actors in 2022 than in any

[5] Annie [sic], "G7 Nations Fail to Stop North Korea's Crypto Hacks: Japan's Warning", Conicu News, May 2023, https://coincu.com/187620-g7-fail-to-stop-north-koreas-crypto-hacks/.

[6] N. Karmini and H.-J. Kim, "US, S. Korea, Japan to Curb Illicit N Korea Cyber Activities", AP News, 13 December 2022, https://apnews.com/article/japan-indonesia-south-korea-north-government-c31a92552bdad882b80d6a771e12ac2d.

previous year",[7] the monitors wrote in their report, which was submitted to the UNSC's DPRK Sanctions Committee.

While many agree on the necessity of addressing North Korea's cyber activities more forcefully, preventing these activities directly via sanctions is extremely difficult. While states have the means to attribute North Korea's cyber activities to specific actors, actually using sanctions to contain or prevent their activities remains a major challenge. This is because these actors operate under different names, quickly regroup once detected, and regularly change their targets and methods, among other things.[8]

While North Korea's cyber activities have not been addressed through UNSC resolutions, they have increasingly been included in unilateral sanctions decisions by individual states. As such, several institutions and individuals linked to North Korean cybercrime activities have since been designated to the respective sanctions lists of the United States, Japan, South Korea and the EU, among others. In 2020, for instance, the EU imposed its first cyber sanctions regime targeting Russian, North Korean and Chinese actors deemed responsible for cyber attacks against EU member states.[9]

The United States also pursued similar sanctions and indictments against Russian, North Korean and Chinese actors. In May 2023, for instance, it sanctioned four entities and one individual "involved in obfuscated revenue generation and malicious cyber activities that support the Democratic People's Republic of Korea (DPRK) Government".[10] Earlier, the United States had issued an advisory to companies describing how to recognise malicious ransomware payments, attacks and accompanying sanctions that fall under the US cyber sanctions programme. Similarly, in March 2023 Germany's Federal Office for the Protection of the Constitution and South Korea's National Intelligence

[7] M. Nicholls, "Exclusive: Record-breaking 2022 for North Korea Crypto Theft, UN Report Says", Reuters, 7 February 2023, https://www.reuters.com/technology/record-breaking-2022-north-korea-crypto-theft-un-report-2023-02-06/.

[8] Analyst Sasha Erskine put it as follows: "Cyber sanctions aim to apply conventional facets of sanctions, such as attribution, evidence gathering and asset freezes, to a sphere where gathering such information and accurately designating the actors involved is hampered by easily falsified links and challenges in tracing. The question is therefore whether the use of traditional sanctioning instruments, and sanctions themselves, can be of use in a sphere where weak and blurred connections limit who can be designated and intelligence sensitivities preclude publicising evidence"; S. Erskine, "The EU Tiptoes into Cyber Sanctions Regimes", RUSI Commentary, 12 October 2020, https://www.rusi.org/explore-our-research/publications/commentary/eu-tiptoes-cyber-sanctions-regimes.

[9] Since 2017 the EU has put in place a comprehensive cyber diplomacy toolbox, including an autonomous horizontal cyber sanctions regime adopted in May 2019, to prevent, deter and respond to malicious behaviour in cyberspace. This regime allows the EU to impose sanctions on persons or entities involved in cyber attacks threatening the EU or its member states, or attempted cyber attacks, regardless of the nationality or location of the perpetrator. Sanctions are also possible for cyber attacks against third states or international organisations. See EEAS (European External Action Service), "EU Imposes First Ever Cyber Sanctions to Protect Itself from Cyber-attacks", 30 July 2020, https://www.eeas.europa.eu/eeas/eu-imposes-first-ever-cyber-sanctions-protect-itself-cyber-attacks_en.

[10] US Department of the Treasury, "Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities", Press Release, 23 May 2023, https://home.treasury.gov/news/press-releases/jy1498

Service issued a first-ever Joint Cyber Security Advisory related to North Korean cyber activities.[11]

Following the trilateral meeting among the United States, Japan and South Korea in December 2022, the South Korean Foreign Ministry said in a statement that the three envoys had decided to "double down their efforts to block North Korea's financing of nuclear and missile programs via cyber activities and other means and its attempt to evade sanctions on the North".[12] Realistically, these designations are primarily about using sanctions to successively impede North Korea's cyber activities, limit its options, and influence the structures within which its cyber activities take place.

This strategy can be compared to the earlier development of the broader sanctions regime against North Korea and how knowledge of the various sanctions' implementation processes has improved.[13] This required the generation of a great deal of structural exposure and attention in the first place, and it was only through numerous training programmes and a better understanding of these processes, among other things, that the ability to supervise the implementation of sanctions improved considerably over time. A similar approach is now taken with regard to North Korean cybercrime activities.[14]

[11] German Federal Office for the Protection of the Constitution and ROK National Intelligence Agency, "Sicherheitshinweis zu Cyberaktivitäten und Missbrauch von Googles Browser und App Store-Diensten durch KIMSUKY", Joint Cyber Security Advisory, 20 March 2023, https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2023-03-20-sicherheitshinweis-cyberaktivitaeten.pdf?__blob=publicationFile&v=2.

[12] Karmini and Kim, 2022.

[13] Author background conversation with EEAS official, January 2023.

[14] For example, in November 2022 South Korea and the United States convened a symposium to discuss steps partner governments and private sector stakeholders can take to defend against North Korea's malicious cyber operations, bringing together "Hundreds of participants from over a dozen countries". See US Department of State, "U.S.-ROK Joint Symposium on Countering DPRK Cyber Threats to Cryptocurrency Exchanges", Press Release, 17 November 2022, https://www.state.gov/u-s-rok-joint-symposium-on-countering-dprk-cyber-threats-to-cryptocurrency-exchanges/.

Policy recommendations: improved coordination and practical cooperation

While information sharing among "like-minded" partners exists, steps to ensure the more comprehensive coordination of new sanctions decisions are only in their initial stages. For example, in 2022 the United States and South Korea established the Working Group on the DPRK's Cyber Threat to regularly coordinate activities and exchange information "about the DPRK's malicious cyber activities, including cryptocurrency heists and related money-laundering, and the fraudulent activities of DPRK information technology (IT) workers stationed abroad".[15] Moreover, a number of cyber dialogues between South Korea and the EU have been established that regularly address North Korea's cyber activities, while some EU member states (such as the Netherlands) maintain their own cyber dialogues with Seoul. South Korea's admission to the NATO Cooperative Cyber Defence Centre of Excellence as the first Asian country in 2022 is also to be seen in this context.

While progress has certainly been made, there are still significant gaps in efforts to ensure detailed and rapid information sharing among the states coordinating their responses to the security threat emanating from North Korean cyber activities. There is also a need to move cooperation on this matter from dialogue to practical cooperation. This could include improved intelligence sharing and joint tabletop exercises involving government officials, experts and representatives from various industries, which mimic real cybersecurity incidents to improve resilience against North Korea's cyber activities. In parallel, and in addition to improving government-to-government collaboration, bringing in academics and industry experts into a wider coordination process will be important. North Korea's cyber-espionage operations specifically targeting international experts highlight the central role non-governmental actors play in both implementing national cyber resilience and evaluating national cybersecurity and geopolitical strategies.[16]

[15] US Department of State, "The 3rd U.S.-ROK Working Group Meeting on the DPRK Cyber Threat", Press Release, 9 March 2023, https://www.state.gov/the-3rd-u-s-rok-working-group-meeting-on-the-dprk-cyber-threat/.

[16] A. Fixler and S. Furukawa, "U.S.-South Korean Cyber Cooperation Can Combat North Korean Threats", FDD Policy Brief, 26 June 2023, https://www.fdd.org/analysis/2023/06/26/us-south-korean-cyber-cooperation-can-combat-north-korean-threats/.

Moreover, in the case of the EU, internal administrative hurdles need to be removed, which impede efficient and effective cooperation among members of the international community seeking to coordinate their sanctions activities vis-à-vis North Korea and prevent rapid responses to evolving security threats, as illustrated in the area of cybercrime. In the current system, in addition to structural provisions (such as appeal deadlines), unilateral sanctions (since they are not UNSC resolutions) must be introduced by one or more EU member states before they can then be discussed and ultimately implemented in Brussels. Greater efforts need therefore to be made to simplify and streamline these processes.

Conclusion: UNSC's inaction and new responses to evolving security threats

While the UNSC's sanctions regime against North Korea is still in place and subsequently created institutions, such as the Panel of Experts, continue to implement its mandate, new UNSC resolutions are highly unlikely for the time being, given the opposition of permanent members Russia and China. The intensifying rivalry between the United States and China, as well as Russia's war against Ukraine, has changed the geopolitical context, which, in turn, has a direct impact on Russia's and China's strategic considerations and priorities in terms of the issue of North Korea. As a consequence, it is highly unlikely that Moscow and Beijing will support new UNSC sanctions on North Korea for the time being.

The stark contrast between North Korea's rapidly increasing military capabilities, on the one hand, and the UNSC's inaction since 2017, on the other hand, has shifted the central theatre for sanctions against North Korea away from the Security Council. UNSC resolutions are essential, though, because they impose international legal obligations on member states. They reflect a political consensus reached in this representative forum, which is mandated by UN member states to maintain international peace and security. However, these resolutions are not the only approach. While the UNSC's reach is unmatched, a broader coalition of the willing can achieve significant progress.

Against this background, a targeted coalition outside the UNSC is essential to raise awareness of and directly address North Korea's central sanctions-evasion mechanisms such as its cybercrime activities. As such, the UNSC's inaction has already changed the way in which sanctions are currently imposed, leading to a process that now takes place outside the UNSC. However, if sanctions remain at the heart of the international community's strategy to deal with the increasing military and nuclear weapons threat from North Korea, much stronger coordination among the states driving this process is required.

People make peace and security possible

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
E-mail: info@gcsp.ch
www.gcsp.ch

ISBN: 978-2-88947-422-6

GCSP
Geneva Centre for Security Policy