Canadian Global Affairs Institute
Institut canadien des affaires mondiales

From Intelligence Gathering to Financial Gain: Countering DPRK Cyber Operations

By Dr. Julie Kim

November 2025

POLICY PERSPECTIVE

From Intelligence Gathering to Financial Gain: Countering DPRK Cyber Operations

by Dr. Julie Kim

October 2025

This article is supported by the Korea Foundation

Canadian Global Affairs Institute
Institut canadien des affaires mondiales

Prepared for the Canadian Global Affairs Institute
Suite 2720, 700 – 9th Avenue SW., Calgary, AB T2P 3V4
www.cgai.ca

ISBN:

The Democratic People's Republic of Korea (DPRK, or North Korea) has developed aggressive cyber operations that have evolved into serious global security threats. North Korea's early cyberattacks were primarily politically motivated, focusing on collecting intelligence and gaining insight into how its adversaries operate. Key targets included government officials, academics, journalists, and North Korean defectors. In addition, the DPRK has targeted the defence industry to gain access to sensitive information on weapons development, with particular focus on technologies related to satellites and semiconductors.

The scope of these operations shifted dramatically toward financial gain after the United Nations adopted successive sanctions in response to its nuclear tests. Despite multiple sanctions and international efforts, North Korea continues to fund its weapons of mass destruction and ballistic missile programs through illicit cyber activities. This includes payments remitted by overseas information technology (IT) workers. A significant portion of financial theft is believed to support its nuclear and missile development programs. In fact, a former White House official claimed that about half of North Korea's missile program is funded by cyberattacks and cryptocurrency theft. Thus, DPRK cyber operations are not only a cyber security issue, but also a direct threat to broader military and defence security.

This article examines North Korea's cyber operations, with a particular focus on IT workers and cyber espionage. Over the past decade, North Korea has significantly expanded its cyber capabilities. Its hackers have become increasingly innovative, integrating new technologies, leveraging generative artificial intelligence (AI) to identify targets, and employing social engineering techniques to enhance the effectiveness and efficiency of their attacks. Therefore, despite ongoing international efforts to strengthen cyber security cooperation, substantial challenges remain. To counter DPRK cyber threats, like-minded countries must establish institutional frameworks for intelligence sharing and joint cyber exercises. Domestically, governments, industry, and academia must work together to build robust information-sharing systems that enable rapid and effective responses to emerging threats.

North Korea's Cyber Operations

Information Technology Research & Development

For decades, the North Korean government has emphasized the importance of science and technology development, particularly in information technology. The state invests heavily in fostering young talent through a highly competitive education system, where only the top students are admitted into elite science and technology programs. Students are identified at a young age from elementary or middle schools, such as Kumsong School and Kumsong Number 1 Middle School. Among them, the most outstanding students are selected to study computer science at prestigious universities in Pyongyang, including Kim Il Sung Military University and Kim Chaek University of Technology. They also get opportunities to study and train abroad in China and Russia. Upon graduation, these students typically go on to work in government agencies or IT-related organizations.

Although not officially confirmed, the Reconnaissance General Bureau (RGB) is widely believed to be the primary institution behind North Korea's cyber program. Pyongyang frequently reorganizes the RGB, restructuring and creating new units to better support the regime's objectives. The current size of North Korea's elite cyber force is estimated at about 7,000 hackers. While these elite hackers are primarily engaged in more complex operations, there are also numerous ordinary IT workers who perform mundane IT work while concealing their North Korean identities.

In addition, a significant recent development in North Korea's cyber program was the establishment of a new AI research center. According to several reports, in March 2025, North Korea established "Research Center 227" under the RGB to strengthen its offensive cyber capabilities. The center focuses on developing hacking tools and programs to neutralize security networks, leveraging AI to develop information theft technologies, and building automated systems for data collection and analysis. Shortly afterward, on March

27, North Korean state media announced the launch of a new AI-equipped suicide drone. The integration of AI into both cyber operations and weapons systems is a serious concern for South Korea and the wider international community.

IT Workers

North Korea dispatches thousands of highly skilled IT workers abroad and within the country to support its cyber operations. These workers provide a critical revenue stream that helps fund the regime's economic and security objectives, including its weapons of mass destruction (WMD) and ballistic missile programs. The regime sets annual earnings quotas for overseas workers, and each organization must fund themselves while also meeting their revenue targets. These quotas are believed to be the main driving force behind DPRK IT workers and their diversification and expansion into new cybercrimes. In addition, reports indicate that these workers are subjected to excessive work hours, constant surveillance by security agents, abusive working and living conditions, and little to no freedom of movement.

Outside of North Korea, IT workers are located primarily in China and Russia, with smaller numbers in Southeast Asia and Africa. While posing as non-North Korean nationals, they obtain freelance employment contracts with clients around the world, including in North America, Europe, and Asia. To do so, they submit counterfeit, altered, or falsified documents, such as resumes, identification documents, work visas, diplomas, and bank statements, to deceive employers. Once contracts are secured, they receive payments in cryptocurrency to avoid financial tracking. According to a 2024 UN report, DPRK IT workers generate up to $600 million annually for the regime.

The IT workers engage in a wide range of work, including mobile and web-based applications, general IT support, mobile games, graphic animation, and AI-related projects. They rely on remote contract work, disguising their identities and location through arrangements with third-party subcontractors. These subcontractors are non-North Koreans who complete contracts for North Korean IT workers and establish laptop farms with credible IP addresses to make it appear that North Korean workers are operating domestically. The IT workers also use virtual private networks (VPNs), virtual private servers (VPSs), or third-country IP addresses to appear as if they are connecting to the internet from different locations.

With the increase in remote work and the growing use of AI, businesses and security professionals face heightened risks of unintentionally hiring North Korean IT workers. Canada is no exception. In July 2025, the Royal Canadian Mounted Police (RCMP) issued an advisory warning Canadians and Canadian businesses about the risks of hiring North Korean IT workers. Therefore, it is crucial for businesses to implement thorough hiring practices and conduct robust background checks, and for governments to provide guidance and support to mitigate these risks.

Cyber Espionage

DPRK hackers conduct cyber espionage to gather information to fulfil the regime's strategic goals. They primarily target South Korea and the United States, focusing on high-profile individuals in government, the military, and academia. In the past, they have also targeted Russian defence companies to steal military technology. However, it is unclear whether North Korea continues to hack Russia following the signing of the Comprehensive Strategic Partnership (CSP) Treaty in June 2024.

Several known groups conduct cyber espionage, each with different objectives. Kimsuky (also known as APT 43 or Velvet Chollima) focuses on gathering intelligence on geopolitical events, foreign policy, and diplomatic efforts affecting North Korea. They primarily target governments, think tanks, academic institutions, and media. Meanwhile, Andariel (also known as APT 45 or Silent Chollima) primarily seeks to obtain sensitive technical information and intellectual property to advance North Korea's military and nuclear programs. As such, Andariel's main targets include defence, aerospace, nuclear, and engineering sectors.

According to cybersecurity company Recorded Future, the industry most targeted by North Korean cyberattacks is government, followed by cryptocurrency, media, finance, defence, and non-governmental organizations (NGOs). This demonstrates that espionage continues to play a crucial role in North Korea's cyber operations. For example, between March and July 2025, a North Korea-linked hacker group carried out at least 19 spear-phishing attacks against foreign embassies in South Korea. The group impersonated diplomats and officials, luring staff with carefully crafted official letters and event invitations. The operation, which remains active, is believed to be linked to Kimsuky with possible ties to China. A report by cybersecurity firm Trellix found that the hackers' activity closely aligned with Chinese time zone and working hours, pausing during major Chinese national holidays, not North Korean holidays. These patterns indicate that the group may be operating from Chinese territory or leveraging Chinese resources.

In addition to intelligence gathering, DPRK hackers conduct psychological operations to manipulate public opinion. They impersonate foreign media outlets to generate fake news on sensitive topics, such as political tensions and economic inequality, and distribute it across social media platforms to create social discord. Consequently, the persistent and evolving nature of North Korea's cyber operations highlights the importance of international cooperation in countering these threats.

Cyber Operations Abroad and Strategic Partnerships

Although DPRK IT workers conduct cyber operations domestically, due to limited domestic internet infrastructure, their operations within the country are constrained. To overcome these limitations, North Korea leverages third-country networks and IT infrastructure. China and Russia are key destinations for dispatching IT workers.

In addition to hosting IT workers, China and Russia provide various forms of support and sometimes employ them in local companies. In fact, some Chinese front companies helped North Korean IT workers obtain jobs, evade international sanctions, and even provided them with equipment. In addition, Russian companies were sanctioned by the

U.S. Department of the Treasury for signing a 10-year contract with a DPRK company and hiring around 30 IT workers to work in Russia. Southeast Asia has also emerged as a critical region, where DPRK IT workers maintain bases of operation. In Cambodia, authorities even granted citizenship to North Koreans who had violated sanctions.

Furthermore, the CSP Treaty, signed between North Korea and Russia, is expected to influence DPRK cyber operations. The Treaty outlines that the two sides pledged to build long-term relations across military, economic, and political domains. It calls for expanded cooperation and joint research in science and technology, including space, AI, and IT. It also specifies collaboration in information security and the joint development of legal and normative foundations. As a result, collaboration between Pyongyang's and Moscow's cyber capabilities is likely to increase the scale and complexity of North Korea's operations, posing new challenges for global cyber security.

International Cyber Security Cooperation

South Korea's Cyber Security Strategy and International Partnerships

South Korea is the primary target of North Korea's cyber operations. According to South Korea's National Intelligence Service (NIS), North Korea accounted for 80 percent of cyberattack attempts against South Korea's public sector in 2023, amounting to approximately 1.3 million attempts per day. To address these growing threats, South Korea established the National Cyber Crisis Management Center in May 2023. The center is a collaborative effort between the Office of National Security (ONS) and the NIS, bringing together experts from government, public institutions, and the private sector.

Since the establishment of the National Cyber Security Center (NCSC) in 2004, the ROK government has also worked closely with intelligence and security agencies of key allies, as well as international cyber security organizations. In particular, South Korea has deepened its ties with NATO. Since 2021, South Korea has participated in NATO's annual cyber defence exercise Locked Shields. In May 2022, it became the first Asian country to join the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). In addition, in July 2023, South Korea and NATO signed an enhanced partnership, the Individually Tailored Partnership Programme (ITPP), which includes cooperation in cyber defence and emerging technologies.

Moreover, in April 2023, South Korea and the U.S. announced the ROK-U.S. Strategic Cybersecurity Cooperation Framework, expanding the scope of their mutual defence treaty into cyberspace. The agreement includes intelligence sharing as well as cooperation in technology and policy. In November 2023, South Korea, the U.S., and Japan launched a high-level trilateral cyber dialogue to strengthen collaboration in countering DPRK's malicious cyber activities. These initiatives highlight Seoul's growing role in advancing international cyber security cooperation.

Canada's Expanding Cyber Security Partnerships in the Indo-Pacific

Canada has identified cyber security cooperation as a key component of its Indo-Pacific Strategy (IPS). As part of the IPS, Canada announced the *Cybersecurity and Digital Technology Diplomacy* project, which allocates $47.4 million over five years (2022-2027) to enhance cyber security capacity in partner countries and increase regional engagement through the deployment of cyber attachés.

Moreover, the newly established Canadian Armed Forces Cyber Command (CAFCYBERCOM) plays a central role in advancing Canada's cyber operations and strengthening partnerships with Indo-Pacific allies. In May 2025, Canada and South Korea participated as a team in Exercise LOCKED SHIELDS, the world's largest cyber defence exercise organized by NATO CCDCOE. In August 2025, under Operation HORIZON, Canada and Japan worked together in MASAKARI 25, a bilateral cyber defence activity designed to deepen operational cooperation in the Indo-Pacific. In addition, in September 2025, CAFCYBERCOM participated in Cyber Summit Korea 2025 in Seoul and contributed to the Allied Power Exercise (APEX) 2025, which combined field technology and policy simulation training.

Although North Korea's cyber operations do not pose the same level of threat to Canada as those from China and Russia, DPRK cybercrime activities present a persistent threat to Canadian individuals and organizations across a wide range of industries. Therefore, Canada's continued cyber security cooperation with its Indo-Pacific allies will not only benefit all parties involved, but also reinforce collective resilience against shared threats.

Looking Ahead

As of 2025, a significant share of foreign and security policy issues now revolve around developments in cyberspace. The resilience of cyberspace is also critical to economic security, supply chain resilience, and technological development. Moreover, the rapid evolution of emerging technologies and AI is expected to make the cyber security environment increasingly complex. Therefore, cyber security must be regarded as a core pillar of national security.

Despite ongoing efforts to strengthen cyber security cooperation, many challenges remain. The global nature of cyber operations means that countries need to establish institutional frameworks for sharing intelligence, conducting joint exercises, and coordinating responses. In addition, it is important to establish information-sharing systems between governments and the private sector to ensure timely exchange of information and responses to cyber threats.

A particular challenge in countering North Korea's cyber operations is the lack of an accountability framework. There is a need for a multilateral cooperation framework to reinforce accountability among countries like China and Russia – both major cyber aggressors – and countries in Southeast Asia, where North Korean IT workers are primarily based. Additionally, expanding cyber capacity-building programs in Southeast Asian countries will be crucial to prevent North Korea's illegal use of their networks. This challenge is further complicated by the CSP Treaty signed between North Korea and Russia, which includes provisions for cooperation in science, technology, AI, and information security. Such collaboration is likely to enhance Pyongyang's cyber capabilities and elevate the scale and complexity of its operations, heightening risks for the international community.

Against this backdrop, Canada and South Korea have had a particularly vibrant year of cyber security cooperation in 2025. The two countries participated jointly in Exercise LOCKED SHIELDS and collaborated in the multinational cyber defence exercise APEX during Cyber Summit Korea 2025. These initiatives mark an important step toward deepening the bilateral cyber partnership and expanding it into a broader multilateral framework with other Indo-Pacific allies.

About the Author

Dr. Julie (Jung-eun) Kim is a Post-Doctoral Fellow leading the Korea Program at the Canadian Global Affairs Institute (CGAI) and a Country Expert on North Korea for the Bertelsmann Transformation Index (BTI). She received a PhD in Political Science from Heidelberg University as a German Academic Exchange Service (DAAD) scholar. Her dissertation explores the social control system and autocratic regime stability in North Korea. She has a Master of Arts in North Korean Studies and a Bachelor of Arts in German Language and Literature from Ewha Womans University.

Julie has previously worked as a Research Intern at the Stockholm International Peace Research Institute (SIPRI) and a Global Asia Fellow at the East Asia Foundation. She has published various articles and a book chapter, including in the *Journal of East Asian Studies*, *BTI Country Report – North Korea*, and *Global Asia*. Her research interests include authoritarian regimes, geopolitics with a regional focus on the Korean Peninsula, and Canada-Korea defence cooperation.

You can connect with Dr. Kim at jkim@cgai.ca

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.