MARCH 2026

Responding to the Evolution and Global Expansion of the DPRK IT Worker Threat

Yena Kim and Donghee Kim

The recent large-scale **indictment** of Democratic People's Republic of Korea (DPRK) information technology (IT) workers by the U.S. Department of Justice clearly demonstrates the escalating sophistication and severity of North Korea's cyber operations. This law enforcement action underscores not merely the detection of illegal activity, but the fact that the DPRK is leveraging cyberspace in a systematic manner to generate revenue for the regime. As of 2024, DPRK IT workers are estimated to generate between **$350 million and $800 million annually**.

As UN sanctions have constricted traditional sources of foreign currency, the DPRK has increasingly relied on overseas IT workers disguised as legitimate employees. What initially appeared to involve ordinary software development or application design has evolved into a coordinated strategy of infiltration, revenue generation, and, in some cases, data theft and financial crime.

This report examines the evolution of DPRK IT workers' operational tactics, the international expansion of their networks, and the limitations of existing responses. It argues that advisory- and sanctions-based measures alone are insufficient and calls for more proactive, government-led coordination and outreach to address this growing threat.

The Evolution of DPRK IT Workers' Operational Tactics

Since around 2017, DPRK IT workers have been creating fraudulent profiles, forged identities, and fake resumes to infiltrate freelance platforms and secure employment abroad. Initially, their work appeared to involve ordinary software development or application design, delaying recognition of the threat and enabling rapid proliferation.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

During the hiring process, when video interviews were requested, accomplices appeared on camera while the DPRK worker redirected the conversation to a phone or chat-based format, citing supposed technical issues. In some cases, they remotely accessed the accomplice's device to perform technical demonstrations during the interview.

Once remote work feasibility was confirmed, DPRK IT units collaborated with U.S.-based conspirators to operate "laptop farms," enabling multiple simultaneous infiltrations. U.S. accomplices received and managed employer-issued laptops, while DPRK operatives remotely controlled them to impersonate numerous employees across several companies.

These workers do not merely conduct software development. They strategically infiltrate defense contractors, government contractors, and critical infrastructure organizations to obtain sensitive internal access. Once inside, they exfiltrate confidential data and intellectual property to DPRK or third-party criminal networks. Some groups install backdoors for follow-on operations or threaten data leaks after termination to extort money. Multiple cases show DPRK IT workers securing developer positions at cryptocurrency companies and directly stealing hundreds of millions of dollars in assets.

More recently, DPRK IT workers have aggressively integrated artificial intelligence (AI) into their disguise and infiltration tactics. They generate fake profile images, automatically produce large volumes of resumes and cover letters using generative AI tools, manipulate social media activity, and use deepfake video and audio during remote interviews.

These AI-enabled methods represent a shift from basic identity fraud to a highly structured and coordinated global infiltration strategy. This trend reinforces the need not only for companies, but also governments, to strengthen both defensive and policy responses, as these operations increasingly constitute a direct national security risk.

The International Expansion of DPRK IT Workers and Accomplices

DPRK IT workers and their accomplice networks have expanded their geographic scope beyond China and Russia—where they had traditionally operated—to new third-country destinations. Since 2020, they have increasingly been deployed to **Equatorial Guinea, Laos, and the United Arab Emirates**, and more recently to **Cambodia, Guinea, Nigeria**, and **Tanzania**, where they conduct remote work for U.S. companies to earn foreign currency. However, in the second half of 2024, as U.S. law enforcement measures intensified, some workers **shifted** operations to Europe, where oversight remains relatively less stringent.

In Europe, IT workers have engaged in coordinated activities across multiple countries—including Germany, Portugal, and the United Kingdom—leveraging numerous personas and AI-generated synthetic profiles to register on local employment platforms and global freelancing websites, and to apply for positions at defense contractors and government-related organizations. One notable case was identified in Serbia, where a DPRK IT worker infiltrated a token corporation and stole approximately **$175,000 worth of cryptocurrency**, subsequently transferring the funds to overseas accounts. This case demonstrates that North Korea is actively exploiting European financial and crypto-asset systems to construct a foreign currency procurement structure.

Such activities have also been detected across Asia. In Japan, multiple incidents have been uncovered involving DPRK IT workers engaged in fraudulent employment and illicit operations. In China, a North Korean worker attempting to **steal** military technology was arrested and detained, illustrating that the activities of these workers are expanding beyond conventional software development into strategically sensitive areas such as defense technology. These incidents indicate that their operations are no longer confined to North America and Europe; instead, they are spreading across Asia and expanding globally in both geographic and industrial dimensions.

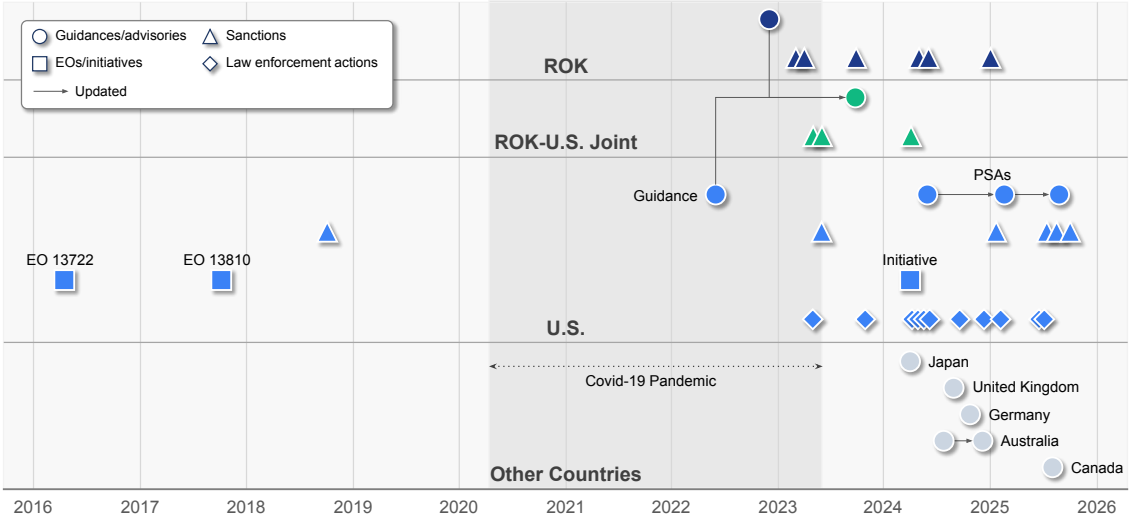
These overseas operations would not be possible without the support of accomplices operating worldwide. **Accomplice networks** in the United States, Japan, Ukraine, and the United Arab Emirates collaborate with DPRK IT workers by managing laptop farms, laundering funds, managing stolen assets, forging identities, and establishing illicit remittance channels. This support network forms the critical infrastructure that enables the covert operations, revenue generation, and sanctions evasion activities of DPRK IT workers.

As North Korea's concealment techniques and operational sophistication continue to advance, and as its networks of workers and accomplices expand globally, it is increasingly clear that the current international cooperation framework alone has limitations in mounting an effective response.

Limitations of International Responses to DPRK IT Activities

The United States is the primary country where DPRK IT workers are most actively operating, and it has responded with the most robust measures, including various sanctions, to curb their employment activities within the country. As a result, by the second half of 2024, DPRK IT workers shifted their operations primarily to Europe, where oversight is relatively less stringent. Figure 1 summarizes guidance and advisories, sanctions, executive orders (EOs) and initiatives, and law enforcement actions issued by the Republic of Korea (ROK), the United States, and other countries, organized by release date. The figure illustrates that DPRK IT workers have long been recognized by the U.S. government as a serious threat, and the United States has actively responded through EOs, initiative, sanctions, and legal actions.

Figure 1: International Responses to DPRK IT Workers



Source: Government advisories, sanctions announcements, and official statements from the Republic of Korea, the United States, Japan, the United Kingdom, Germany, Australia, and Canada.

Table 1: International Responses to DPRK IT Workers by Year

Year	Country	Response Type	Date
2016	United States	Executive Order 13722	March 15, 2016
2017	United States	Executive Order 13810	September 20, 2017
2018	United States	Sanctions	September 13, 2018
2022	United States	Guidance	May 16, 2022
2022	ROK	Advisory	December 8, 2022
2023	ROK	Sanctions	February 10, 2023; March 21, 2023; September 1, 2023
2023	ROK–United States Joint	Coordinated sanctions	April 24, 2023; May 23, 2023
2023	ROK–United States Joint	Joint advisory	October 19, 2023
2023	United States	Sanctions	May 23, 2023
2023	United States	Law enforcement actions	April 24, 2023; October 18, 2023
2024	ROK	Sanctions	April 3, 2024; May 24, 2024; December 26, 2024
2024	ROK–United States Joint	Coordinated sanctions	March 28, 2024
2024	United States	Public service announcement	May 16, 2024
2024	United States	Initiative	March 2024
2024	United States	Law enforcement actions	May 15, 2024; May 15, 2024; May 16, 2024; May 16, 2024; August 8, 2024; December 12, 2024
2024	Japan	Advisory	March 26, 2024
2024	Australia	Advisory	August 26, 2024; December 14, 2024
2024	United Kingdom	Advisory	September 12, 2024
2024	Germany	Advisory	October 1, 2024
2025	United States	Public service announcements	January 23, 2025; July 2, 2025
2025	United States	Sanctions	January 16, 2025; July 8, 2025; July 24, 2025; August 27, 2025
2025	United States	Law enforcement actions	January 23, 2025; June 5, 2025; June 30, 2025
2025	Canada	Advisory	July 16, 2025

Source: Government advisories, sanctions announcements, and official statements from the Republic of Korea, the United States, Japan, the United Kingdom, Germany, Australia, and Canada.

Initially, EOs **13722** and **13810** designated DPRK IT workers' overseas deployment and related activities as sanctions targets, prohibiting their provision of software and technical services. However, the **Covid-19 pandemic** (March 2020–May 2023) led to a surge in remote work, enabling DPRK IT workers to work for U.S. companies remotely. Consequently, since 2022, U.S. government and intelligence agencies have issued a total of four documents, including one **guidance** and three **public service announcements** to alert companies to risk indicators and response measures. From 2023 onward, interagency collaboration among the U.S. Departments of Treasury, Justice, and State has intensified, resulting in large-scale sanctions and prosecutions targeting DPRK IT workers and networks.

In March 2024, the United States launched the "**DPRK RevGen: Domestic Enabler Initiative**," prioritizing the identification and shutdown of laptop farms. The initiative disclosed multiple law enforcement actions against accomplices hosting laptop farms, DPRK IT workers involved, domains used for illicit employment, and associated revenues. Particularly, from the second half of 2025, **large-scale joint law enforcement actions and multiple sanctions** targeting DPRK IT workers have been publicly disclosed, reflecting a significant strengthening of U.S. response efforts.

Following the United States, the ROK has been the most active country in responding to DPRK IT worker operations. In December 2022, the ROK issued its first **joint government advisory** calling for enhanced verification of DPRK IT worker identities. Since then, the ROK has independently designated six entities and individuals associated with DPRK IT workers involved in overseas foreign currency-earning activities as sanctions targets. The ROK and the United States have also coordinated in responding to DPRK IT workers. In April 2023, the two countries jointly designated targets for sanctions for the first time, and to date, there have been three instances of joint target designations. Separately, in October 2023, **both countries** issued a joint government advisory updating their respective advisories with the latest trends.

In 2024, countries including **Australia**, **Canada**, **Germany**, **Japan**, and the **United Kingdom** also joined the international effort by issuing advisories on DPRK IT workers' disguised employment. This development reflects a growing recognition that the DPRK's covert employment activities are not merely a foreign currency-earning issue, but also an international security and economic risk. Overall, Figure 1 demonstrates that the principal actors responding to DPRK IT worker operations have expanded from the ROK and the United States to other countries, including those in Europe, highlighting the need for a broader international response framework.

Figure 1 also highlights certain challenges. According to U.S. indictments, DPRK IT workers have been active since at least **2017**. Their initial activities were disguised as legitimate employment, which delayed recognition of the associated risks by both the international community and private companies. The figure shows that substantial international responses only began in earnest around 2024.

During the Covid-19 pandemic, as remote work culture expanded, DPRK IT workers found it increasingly easy to participate in overseas corporate projects by posing as third-country workers. During this period, they are also believed to have rapidly enhanced both their technical capabilities and their identity-masking and money-laundering techniques. At the same time, international sanctions enforcement and broader multilateral responses remained largely stagnant, creating a widening gap between North Korea's evolving methods and the international community's ability to counter them.

As a result, advisory and sanctions-based responses have inherent limitations. DPRK IT workers are state-sponsored and systematically managed, allowing them to continuously develop innovative techniques and methods. In practice, new identity-masking and technical methods have repeatedly emerged immediately following sanctions. While the United States has combined executive orders, sanctions, prosecutions, and law enforcement actions, these measures alone have had limited effectiveness, as North Korea consistently develops new evasion methods to circumvent sanctions.

Consequently, advisory- and sanctions-based responses alone remain insufficient to fundamentally disrupt DPRK IT worker operations. While detection and response at the company level are important, the burden of identifying and mitigating these threats has largely been placed on individual companies, many of which lack the resources, visibility, or expertise to do so effectively. Moreover, the transnational and adaptive nature of DPRK IT worker networks limits the effectiveness of isolated, reactive measures.

These limitations underscore the need for a more proactive and coordinated approach led by governments. In particular, systematic outreach to domestic companies, structured engagement with international partners, and sustained public-private collaboration are essential to closing existing response gaps. Without stronger government-led efforts to disseminate risk awareness, share intelligence, and align international countermeasures, existing responses will continue to lag behind the evolving tactics of DPRK IT workers.

Government-led Outreach and Coordination to Counter DPRK IT Worker Threats

DPRK IT worker operations are expected to persist through 2026 and continue expanding geographically as enforcement pressure intensifies in the United States. These operations are likely to leverage increasingly sophisticated techniques, including multimodal generative AI—including voice, text, and video deepfakes—to sustain disguised employment. At the same time, cryptocurrency-related companies and other digitally native sectors will remain **high-value targets** due to their remote work structures and the potential for rapid financial gain.

International sanctions and law enforcement actions have imposed tangible costs on these networks, but they have not fundamentally disrupted DPRK IT worker operations. The adaptive, state-sponsored nature of these activities enables rapid evolution in response to enforcement measures. Reliance on reactive, company-level detection alone places an unsustainable burden on individual companies and creates persistent gaps between emerging threats and effective countermeasures. Addressing these limitations requires a shift toward proactive, government-led outreach and coordination.

LESSONS FROM THE PRIVATE SECTOR: IMPLICATIONS FOR GOVERNMENT ACTION

Companies face significant structural constraints when disclosing DPRK IT worker incidents. When a company inadvertently hires a DPRK IT worker, the resulting risks extend beyond technical compromise to reputational damage, customer attrition, legal exposure, and contractual liabilities. These factors strongly discourage voluntary disclosure, even when early reporting would benefit the broader ecosystem.

Nevertheless, in 2024, one cybersecurity company publicly **disclosed** an attempted internal intrusion linked to DPRK IT worker activity. The company documented the full recruitment process—including job postings, interview procedures, and identity verification steps—and immediately shared all relevant

data with U.S. cybersecurity firm Mandiant and the FBI to support early-stage investigations. The company also publicly release lessons learned and response measures through its website.

Following the incident, the company **conducted** organization-wide employee training, implemented fingerprint-based identity verification, and restricted corporate laptop delivery to verified UPS shipments requiring photo identification. In addition, the company published a comprehensive **white paper** detailing insider-threat risks and preventive controls, and it continued to release updates on DPRK IT worker activity trends.

According to the company's CEO, the decision to disclose was intended to raise awareness of the widespread nature of DPRK IT worker infiltration attempts and to warn other organizations of comparable risks. By transparently sharing its experience, the company contributed to elevating industry-wide security standards while reinforcing customer trust.

However, such best practices remain fragmented across jurisdictions and sectors, making comprehensive access difficult for most companies—particularly small- and medium-sized enterprises. This fragmentation highlights the limitations of relying solely on voluntary private sector disclosure. Accordingly, governments should assume a more active role in collecting, standardizing, and disseminating these lessons through sustained outreach efforts.

CENTRALIZED INFORMATION SHARING AND INSTITUTIONAL VERIFICATION FRAMEWORKS

Governments already possess extensive intelligence related to DPRK cyber operations and IT worker networks, yet this information often fails to reach companies in a usable and timely manner. To close this gap, the ROK government should centrally aggregate and disseminate both best practices and DPRK IT worker–specific indicators—including email addresses, recurring account naming patterns, profile photos, commonly cited education and career information, and IP addresses associated with laptop farms.

Rather than creating new mechanisms, existing government–private sector information-sharing platforms focused on DPRK cyber threats should be expanded to incorporate these indicators. Centralization would significantly lower access barriers, enabling companies of all sizes to integrate this information directly into recruitment screening, identity verification, and internal security training processes.

In parallel, the ROK should consider establishing an institutional employment-eligibility and identity verification framework analogous to the U.S. I-9 and E-Verify systems. In the United States, these mechanisms have been used not only to confirm work authorization, but also to flag identity inconsistencies and third-country impersonation patterns relevant to DPRK IT worker investigations. A comparable system in the ROK would provide companies with an additional safeguard when pre-employment screening fails.

REPORTING, INCENTIVES, AND ENFORCEMENT MECHANISMS

Timely reporting remains critical to preventing escalation and secondary harm once DPRK IT worker activity is detected. However, incentives alone are unlikely to overcome companies' reluctance to disclose incidents. A dual-track framework combining legal protections and meaningful penalties is therefore required to make reporting the rational choice rather than concealment.

The government should provide whistleblower protections and limited liability safeguards for companies that report suspicious activity promptly. At the same time, penalties—including increased

fines—should be strengthened for companies that knowingly or negligently employ DPRK IT workers or fail to report suspicious indicators within a defined time frame. Enforcement should also extend to operational enablers, such as laptop farm operators and intermediaries who facilitate overseas employment and financial flows, as these actors are essential to sustaining DPRK IT worker networks.

INTERNATIONAL OUTREACH AND THE ROK'S STRATEGIC LEADERSHIP

Although remote work is less prevalent in the ROK than in many Western economies, the country faces unparalleled national security exposure due to its geographic proximity to North Korea. This position confers both heightened risk and a unique responsibility to lead international awareness and coordination efforts.

Recent reporting indicates that DPRK IT worker activity has increased across Europe, where remote work adoption remains high and threat awareness comparatively low. The ROK should proactively engage European partners to emphasize that weak awareness in remote work environments can escalate into broader national and economic security risks. Similar outreach is warranted in Southeast Asia, Africa, and other regions where awareness remains limited.

In parallel, bilateral cooperation between the ROK and the United States—as well as trilateral coordination with Japan—should continue through regular advisories, working-level exchanges, and joint statements. Given the increasingly blurred line between DPRK IT workers and overtly malicious cyber actors, a new joint advisory emphasizing the growing use of direct exfiltration and intrusion tactics would reinforce shared threat perception and strengthen collective deterrence.

Ultimately, countering DPRK IT worker operations requires more than cooperation—it requires leadership. By centralizing information, institutionalizing verification mechanisms, incentivizing reporting, and proactively engaging international partners, the ROK can move from a reactive participant to a global agenda-setter in addressing this evolving threat. ■

Yena Kim *is a senior researcher on the Cybersecurity Policy Research Team at the National Security Research Institute in the Republic of Korea.* ***Donghee Kim*** *is a senior researcher and manager of the Cybersecurity Policy Research Team at the National Security Research Institute in the Republic of Korea.*

TThis report is made possible through support from the National Security Research Institute (NSR) of Korea. CSIS and NSR conducted scholarly research on U.S.-ROK cyber resilience. The analysis presented here was independently authored by researchers at NSR.