SANCTIONS SOS

QUICK-READ ANALYSIS

The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities

MSMT Report, October 2025

(for the full MSMT report, click here)

What is reported & why it matters

- **Systematic sanctions evasion:** North Korea/DPRK is systematically engaged in violating UN sanctions through its overseas IT labor exports and cyber operations.

- **Full-spectrum cyber programme:** DPRK's cyber force is now a full-spectrum, national programme rivalling China and Russia. It is explicitly used to circumvent UN sanctions and generate funds for North Korea's illicit WMD and missile programmes.

- **Global reach:** These capabilities make DPRK a sophisticated threat, with attacks and thefts targeting companies worldwide. UN Member States are obligated to crack down on these activities under multiple UNSCRs (e.g. 1718, 2375, 2397).

Record-high crypto thefts & laundering

- **Heists of scale:** In 2024, DPRK-linked cyber groups stole at least $1.19 billion in cryptocurrency. From Jan to Sep 2025, that figure became $1.65 billion. This spike was driven by a single $1.4 billion hack of crypto exchange Bybit in Feb 2025.

- **Global laundering networks**: Stolen crypto is funnelled through a variety of crypto exchanges and services in UN-member jurisdictions. DPRK uses networks of its nationals and foreign facilitators (in China, Russia, Cambodia, UAE, etc) to convert digital loot into fiat currency, fuelling its nuclear and missile programmes.

DPRK IT workers abroad

- **Widespread deployments:** DPRK has sent IT worker delegations to at least 8 countries (incl China, Russia, Laos, Cambodia and several in Africa) in 2024–2025.

- **Scale of workers:** China hosts the majority of IT workers (roughly 1,000-1,500). Notably, reports indicate a plan to send 40,000 North Korean labourers (including many IT specialists) to Russia.

- **UN sanctions violations:** These overseas labour schemes violate UNSCRs 2375 and 2397, which ban any work authorisations for DPRK nationals and required repatriation of all DPRK workers by 2019.

- **Use of middlemen:** DPRK IT networks rely on facilitators in countries like Japan, Ukraine, the UAE, and the US to secure employment contracts and channel remittances back to Pyongyang. This complex web hides the flow of illicit funds and labour from enforcement.

Ties to UN-designated entities

- **State-run apparatus:** Nearly all DPRK cybercrime and illicit IT worker revenue serves UN-sanctioned state entities. Those directing the work include the Korean Workers' Party, Reconnaissance General Bureau, Ministry of National Defence, Ministry of Atomic Energy & Industry, Munitions Industry Department, Office 39, and the Second Academy of Natural Sciences.

- **Front companies:** These sanctioned organisations deploy cyber units and IT workers under the cover of front companies overseas. The front companies hide activities while funnelling stolen assets and skills back to DPRK's WMD/missile programmes.

How it works: inside the DPRK playbook

- **Advanced persistent threats:** DPRK uses specialised hacking teams (APTs) that use social engineering, malware and ransomware. They steal sensitive IP and funds, often targeting defence firms and critical infrastructure to support WMD development.

- **Layered laundering**: Illicit funds flow through layers of shell companies, crypto exchanges, mixers and on-ramps. F.e., at least 15 Chinese banks were identified as channels for laundering DPRK cybercrime and IT work proceeds. DPRK actors also use over-the-counter dealers in China to convert large crypto sums into cash.

- **Evasion by trade**: Even sanctioned state traders exploit crypto. The DPRK's arms trading arm (KOMID) has used stablecoins for purchasing military equipment and raw materials (like copper), deliberately evading UN embargoes on arms and related commodities.

Strategic impact on sanctions enforcement

- **Sanctions under siege**: DPRK's cyber/IT evasion scheme directly funds its WMD programmes, undermining the impact of UN sanctions. Its cyber programme is explicitly described as reshaping the region to Pyongyang's advantage and insulating North Korea from UN measures.

- **Real-world damage:** These operations have destroyed computer systems, stolen billions, and even endangered lives. Reported DPRK-linked attacks have disabled hospitals and utilities, causing financial losses and health/safety risks.

- **Weak points exposed:** The large scale (~$3B+ stolen crypto) and global reach highlight gaps in enforcement. As the MSMT report warns, illicit DPRK funds often slip through traditional banking and compliance nets, strengthening Pyongyang's illicit finance stream.

What the international community must do

- **Fill the oversight gap:** With the UN 1718 sanctions panel now disbanded, countries must proactively raise awareness of DPRK sanctions evasion. This includes educating private sector and government agencies on DPRK cyber and labor schemesthat fund illegal weapons programs.

- **Chase the money:** States should strengthen capabilities to trace cryptocurrency flows and legally freeze or seize DPRK-controlled crypto assets. Law enforcement must collaborate internationally to disrupt DPRK crypto laundering networks.

- **Enforce labour bans:** Governments must identify and repatriate DPRK nationals working abroad in IT or other sectors. Companies and recruiters should be scrutinised for ties to North Korea.

- **Harden financial systems:** Follow FATF's call-to-action on the DPRK by terminating direct/indirect correspondent banking ties, applying counter-measures against DPRK parties, and enforcing strict due diligence in crypto and banking services. Engage crypto exchanges and mixers to improve KYC and cooperate on DPRK alerts.

What's next

- **Escalating capability**: MSMT notes a large expansion of DPRK's cyber forces over the past two years, a new APT clusters and more personnel than ever are active. North Korea is investing heavily in cyber tech and overseas labor to evade sanctions and pursue its strategic goals.

- **Enforcement void risk**: With no dedicated UN 1718 panel to monitor DPRK, the responsibility is on individual states and industry to adapt. The next 6/12 months will test whether organisations pay attention to these warnings. Expect DPRK to innovate further in crypto use and exploit any new avenues for labour export.

- **Stay ahead**: The key takeaway is urgency. DPRK's asymmetric sanctions-breaking toolkit is growing. The international community and private sector must act now to strengthen controls. Foresight, coordination, and strong sanctions compliance are crucial to outpace DPRK's next moves.

How Sanctions SOS can help

Sanctions Investigations & Combatting Evasion Training - 18 November, London:

Want to sharpen your own abilities to investigate potential DPRK sanctions evasion within your organisation?

This expert training, delivered in our unique immersive style, will help you identify practical tools to investigate cases, leverage OSINT, recognise key sanctions evasion typologies, and understand enforcement action taken by regulators.

4 spots left: secure your place here, or scan the QR code.

Prefer to leave the hard work to us?

Sanctions SOS provides comprehensive sanctions consultancy services: compliance framework design/review, deep-dive investigation support,and red-flag detection.

Let us know how we can help you today:
enquiries@sanctionssos.com

SANCTIONS SOS