ORION FORUM

North Korea’s Cryptocurrency Theft and Strategic Logic of Its Cyber Operations

NOVEMBER 4, 2026

Introduction

North Korea-linked state-sponsored malign activities in cyberspace have evolved over two decades, transforming the Advanced Persistent Threat (APT) actors into multi-layered structures. Like China and Russia, North Korea has emerged as one of the most active state actors engaging in cyber operations. On October 29, 2026, North Korea-linked state-sponsored hackers stole $6.3 billion in digital coins from Binance, the world’s largest cryptocurrency exchange, in what appears to be the “biggest crypto heist in history.” The Federal Bureau of Investigation (FBI) attributed the attack to TraderTraitor, an APT actor specializing in hacking and cryptocurrency theft. The Binance heist shows that North Korea-linked APT actors remain motivated to pursue bigger spoils from cryptocurrency theft and can carry out complex operations.

The attack is not an isolated incident. The FBI reported that on or about February 21, 2025, the same APT actor, TraderTraitor, “ targeted blockchain technology and the cryptocurrency industry and was responsible for the theft of approximately $1.5 billion USD in virtual assets” from the Dubai-based cryptocurrency exchange Bybit. Moreover, the United Nations Multilateral Sanctions Monitoring Team (MSMT) estimated that North Korea has stolen “at least $2.8 billion between January 2024 and September 2025.”

Through these and similar activities, North Korea aims to evade United Nations Security Council sanctions and support its WMD program as well as other defense-industrial base projects. The MSMT’s 2025 report highlights that North Korea is “systematically engaged in

violations of United Nations Security Council resolutions". To achieve these objectives, North Korea-linked APT actors engage in two types of operations: IT worker deployment and cyber operations.

IT Worker Schemes and Cyber Operations

It is important to note that North Korea's extensive operations require not only domestic structure at the national level but also an international apparatus that would act as a platform, facilitator, and operational platform. The international component is critical for IT worker schemes and cyber operations.

IT worker schemes involve a network of thousands of skilled IT workers deployed domestically in North Korea or abroad. These workers impersonate nationals of foreign countries and mostly rely on Chinese infrastructure to access its job market and financial institutions, and use its infrastructure as a launch platform to access other countries' job markets. IT worker scheme also relies on foreign facilitators in several countries, such as Japan, the United States, the United Arab Emirates, and Ukraine, to secure employment and remit earnings back to North Korea.

According to the UN MSMT 2025 report, IT worker groups are present in at least 8 countries, including China, Russia, Laos, Cambodia, Equatorial Guinea, Guinea, Nigeria, and Tanzania, with the majority based in China. The same report claims that North Korea heavily relies on the Chinese financial system and China-based facilitators to launder illicit cryptocurrency funds. The schemes aim to evade UN sanctions, generate revenue for North Korea, launder stolen crypto assets, and conduct reconnaissance and information collection to support other cyber operations.

On the cyber operations front, North Korea has built a multi-layered APT platform, with actors engaging in strategic, targeted malicious cyber activities. North Korea-linked cyber operations, by contrast, are more sophisticated and coordinated, ranging from complex phishing and social engineering campaigns to cyberespionage, hacking, credential theft, ransomware, financial fraud (including cryptocurrency theft), and intellectual property theft, such as targeting defense companies. North Korea-linked hackers have increasingly used LinkedIn impersonation

to target security researchers and phishing attacks as common methods.

For North Korea, cyber operations serve as both an asymmetrical national security strategy and a survival kit tool. The strategic locus of these operations has evolved from "politically motivated operations to institutionalized revenue generation, which aimed to evade sanctions since 2014." According to South Korea's intelligence assessment, North Korea has expanded its cyber operations personnel from 6,800 in 2022 to 8,400 by 2024. The Reconnaissance General Bureau oversees cyber operations and coordinates North Korea-linked state-sponsored APT actors. Among others, the Lazarus Group (also known as APT38, Hidden Cobra, BlueNoroff, Guardians of Peace, Whois Team, Labyrinth Chollima) is the most critical APT umbrella structure. Lazarus Group includes several sub-units or sub-cells, which are specialized with distinct missions. For example, TraderTraitor, responsible for the Binance and Bybit cryptocurrency theft, is one such sub-unit and has been active since 2020 under the Lazarus Group umbrella.

Orion Policy Institute's Records of Critical Cyber Attacks (ROCCA) Project's initial findings reveal that the top sectors North Korea's cyber operations have targeted since 2005 include government systems, information technology, financial services, the defense-industrial base, and corporate networks. The top attack types included phishing and social engineering, ransomware, denial-of-service attacks, credential attacks/cyberespionage, and system intrusion/hacking.

Discussion and Conclusion

North Korea's multi-layered cyber operations have become more diversified and internationalized, which requires a different approach than treating them as standard cybersecurity threats. Despite imposing sanctions, law enforcement actions, and public attribution to North Korea's malign activities and cyberattacks, Pyongyang has managed to be more innovative in evading these sanctions.

International sanctions, including UN Security Council resolutions, financial sanctions, and Financial Action Task Force (FATF) blacklisting, fail to achieve their intended result: depriving North Korea of a financial lifeline. Law enforcement response to cryptocurrency theft and

laundering of stolen crypto assets requires more than just law enforcement agencies' efforts. Given the scale and complexity of these illicit operations and law enforcement's limited resources, a public-private partnership is needed to track and dismantle them effectively. Finally, the public announcements have been far from effective.

So, what cyber deterrence strategy could change North Korea's cost-benefit calculation? Deterrence by denial, which includes measures to deny the adversary the ability to achieve its objectives, could help prevent cyberattacks that target global financial systems or US critical infrastructure. However, cost-imposition mechanisms, including strategies and tactics that increase political, financial, or technical costs for the adversary's actions, should become a more dominant feature of the US cyber defense posture to increase deterrence against North Korea-linked APT actors.

Disclaimer: *Orion Policy Institute (OPI) is an independent, non-profit, tax-exempt think tank focusing on a broad range of issues at the local, national, and global levels. OPI does not take institutional policy positions. Accordingly, all views, positions, and conclusions represented herein should be understood to be solely those of the author(s) and do not necessarily reflect the views of OPI.*