
**CSAI Foundation**

Cloud Security Alliance AI Safety Initiative

# DPRK's Dual-Track Cyber Doctrine

DeFi Heists and Developer Supply Chains as Parallel Lines of State-Sponsored Finance

Unofficial AI-assisted Research

2026-04-03

## Key Takeaways

- North Korea operates two distinct but converging revenue streams from cyber operations: large direct cryptocurrency heists executed by Reconnaissance General Bureau (RGB) cyber units, and a systematic long-running IT worker infiltration program that extracts steady salary revenue while positioning insiders for future compromise.
- DPRK-linked actors stole an estimated $2.02 billion in cryptocurrency in 2025 — a 51% increase over 2024's $1.34 billion — representing approximately 76% of all crypto-service compromise losses globally by value, with a cumulative lower-bound all-time total exceeding $6.75 billion [1][2].
- The IT worker scheme generated nearly $800 million in calendar year 2024 alone, with individual operatives maintaining up to twelve false identities simultaneously and targeting employers in AI, blockchain, and defense sectors [3][4].
- The February 2025 Bybit hack — the largest single cryptocurrency theft in history at approximately $1.5 billion, as of the document date — was initiated through a supply chain compromise of a Smart Contract wallet provider, illustrating how the two tracks increasingly converge: social engineering of developers enables financial heists at infrastructure scale [5] [6].
- The March 2026 Axios npm compromise attributed to DPRK-nexus threat actor UNC1069 demonstrates that open-source software maintainers are now high-value targets on par with exchange operators, as their trusted credentials provide scalable access to millions of downstream enterprise pipelines [7].
- The Multilateral Sanctions Monitoring Team (MSMT) assessed that cryptocurrency theft may fund up to 50% of North Korea's weapons of mass destruction program, making this a systemic national security risk that extends well beyond the financial sector [8].

---

## Background

Following the 2017 tightening of international sanctions, DPRK-attributed cryptocurrency theft accelerated sharply — a trajectory documented by Chainalysis, the MSMT, and U.S. government assessments as reflecting a strategic shift toward cyber operations as a primary hard-currency

mechanism [1][8]. North Korea's engagement with cryptocurrency theft did not emerge from opportunism alone: it reflects a deliberate pivot toward operations that generate hard currency beyond the reach of the global financial system. The RGB, North Korea's primary foreign intelligence organization, houses multiple subordinate threat clusters — including Lazarus Group, APT38, Andariel, BlueNoroff, and TraderTraitor — that collectively execute both the direct heist and the infiltration tracks [8][13].

The heist track operates through attacks on cryptocurrency exchanges, decentralized finance (DeFi) bridge protocols, and wallet infrastructure. The Axie Infinity Ronin Bridge compromise in March 2022, in which attackers stole approximately $620 million by compromising five of nine validator node private keys, established the template: target the bridging infrastructure or custody layer rather than the blockchain itself [9]. The Bybit hack of February 2025 refined this approach further, attacking the smart contract signing UI layer rather than on-chain contracts — a shift in attack surface documented in technical detail by the FBI and NCC Group [5][6].

The IT worker track operates in parallel and at a different tempo. North Korean nationals, using stolen U.S. personal information, AI-manipulated identity photographs, and facilitators based in third countries, secure remote software engineering positions at Western companies. Wages — typically $3,500 to $10,000 per month per operative, with top performers reportedly earning over $100,000 monthly — are remitted to the regime through cryptocurrency conversion networks [3][10]. The KnowBe4 incident of July 2024, in which a DPRK operative successfully passed video interviews, a background check, and reference verification before deploying infostealer malware on a company-issued workstation, made the scale of this program publicly tangible [11]. As of January 2025, the FBI had identified over 300 U.S. companies as victims of the scheme [10].

The dissolution of the UN Panel of Experts on DPRK sanctions in April 2024 — after Russia vetoed its renewal — eliminated the principal independent multilateral body with a mandate to monitor DPRK sanctions compliance [12]. Eleven nations subsequently formed the Multilateral Sanctions Monitoring Team (MSMT) in October 2024, which has published two substantive reports on DPRK cyber and IT worker activities, most recently in January 2026 [8][12].

---

# Security Analysis

## Two Tracks, One Treasury

Chainalysis characterizes the relationship between the two programs as fundamentally complementary rather than independent [13]. The heist track generates large, irregular revenue events. The IT worker track generates smaller, continuous revenue. Both streams are laundered through the same Chinese-language over-the-counter (OTC) broker networks, cross-chain bridge services, and mixing protocols, which serve as the shared financial clearinghouse for the overall program. The MSMT's January 2026 report documented that by September 2025 DPRK had stolen approximately $1.6 billion in cryptocurrency in the first three quarters of the year alone, with proceeds linked to procurement of armored vehicles and portable air-defense missile systems [8].

The IT worker program is not merely a revenue scheme — it is also an access-generation mechanism. Chainalysis has documented cases in which DPRK operatives who gained employment at cryptocurrency and blockchain firms subsequently provided insider access enabling large-scale heists [13]. The convergence of these tracks means that what appears to be a hiring decision is, for some organizations, simultaneously a financial fraud exposure and a future security breach vector.

## The Bybit Compromise as a Synthesis Case Study

The Bybit hack illustrates the maturation of DPRK's combined tradecraft. Attackers attributed by the FBI to TraderTraitor compromised a Safe{Wallet} developer's macOS workstation on or around February 4, 2025, through social engineering — specifically a Docker-packaged project masquerading as a stock investment simulator that delivered a payload connecting to attacker-controlled infrastructure [5][6]. The developer's cloud access credentials were then harvested, and attackers injected malicious JavaScript into the Safe{Wallet} signing interface between February 5 and 17. The injected code was narrowly scoped: it specifically targeted transactions originating from Bybit's cold wallet addresses while displaying a legitimate-looking interface to human signers. On February 21, three Bybit signatories approved a transaction that transferred approximately $1.46 billion in ETH to attacker-controlled addresses.

The attack chain traverses both tracks simultaneously: it used a social engineering technique characteristic of the IT worker and "Contagious Interview" campaigns (developer targeting, fake project delivery) to execute a financial heist characteristic of the exchange compromise track. Within 45 days, 86% of the stolen ETH had been converted to BTC and dispersed through the same OTC laundering network used by prior Lazarus operations [5].

## Developer Supply Chains as an Attack Surface

The "Contagious Interview" campaign (designated CL-STA-240 by Palo Alto Unit 42, and tracked as DeceptiveDevelopment / G1052 by MITRE ATT&CK) represents the sustained industrialization of developer social engineering. Operatives pose as technical recruiters on LinkedIn and other platforms, extending coding challenge invitations that deliver trojanized repositories containing malicious npm packages [14][15]. Socket.dev identified 338 malicious npm packages linked to this campaign with over 50,000 combined downloads, specifically targeting cryptocurrency and blockchain developers [15]. A subsequent wave in October 2025 deployed 197 additional packages with over 31,000 downloads [17].

The March 31, 2026 Axios npm compromise attributed to UNC1069 represents a qualitative escalation: rather than targeting developers as victims who unwittingly install malicious packages, attackers compromised a trusted maintainer account directly to poison a canonical upstream package relied upon by an estimated 100 million weekly download recipients [7]. The technique — harvesting a long-lived npm access token after RAT deployment on the maintainer's machine, then using it to publish backdoored releases containing the WAVESHAPER.V2 implant — bypassed GitHub Actions OIDC-based trusted publishing controls, which had been widely adopted as a supply chain hardening measure. The malicious versions were live for less than three hours, but automated tooling by Socket.dev detected the anomaly within approximately six minutes of publication.

These events, taken together, are consistent with a systematic effort to move up the software supply chain toward positions of greater downstream leverage — though they may also reflect parallel opportunistic campaigns targeting different developer populations by distinct sub-units. Whether the progression reflects a single coordinated escalation doctrine or convergent operations remains an open analytical question.

## Laundering Infrastructure and Resilience

Following large heists, stolen assets are typically staged through a sequence that includes on-chain mixing (Tornado Cash successors, cross-chain bridges), conversion into privacy coins, and ultimately liquidation through Chinese-language OTC networks that guarantee settlement through informal value transfer systems outside the conventional banking sector [13]. The Bybit laundering cycle documented by Chainalysis required approximately 45 days to disperse $1.46 billion. A March 2026 OFAC action targeted six individuals and two entities facilitating IT worker salary repatriation, including a Vietnamese national who converted approximately $2.5 million into cryptocurrency for DPRK workers between 2023 and 2025 [3][16].

A marked reduction in DPRK theft activity was observed after July 1, 2024, with Chainalysis noting the timing's coincidence with Russian President Putin's June 2024 visit to Pyongyang [2]. This suggests that geopolitical relationships may modulate the tempo of cyber operations, and that future escalation or restraint may be influenced by factors beyond technical capability.

---

# Recommendations

## Immediate Actions

Organizations should begin with their identity verification and software supply chain controls, as these represent the two entry vectors most exploited across the incidents documented in this note. Remote contractor and remote employee identity verification processes warrant immediate audit: verification should include government-issued document checks against authoritative databases, not solely AI or video interview screening. The January 2025 FBI/CISA advisory on DPRK IT workers documents specific red flags including preference for camera-off meetings, laptop forwarding to logistics addresses, inconsistencies between resume and live technical performance, and implausible geographic continuity [10].

Package provenance controls should be enforced wherever feasible. Enabling `npm audit signatures` and configuring package managers to reject unsigned or unsigned-equivalent packages – combined with lockfile enforcement and monitoring for unexpected dependency additions – substantially narrows the window of opportunity for the maintainer account compromise pattern demonstrated by the Axios incident. These controls are most effective when enforced at the CI/CD layer rather than relying solely on developer workstation configuration.

Real-time software composition analysis (SCA) tooling provides the detection surface that point-in-time audits cannot. The six-minute detection window in the Axios compromise, achieved by Socket.dev through continuous behavioral analysis of package registries, demonstrates that automated monitoring can provide actionable early warning before malicious versions propagate through automated update pipelines. Finally, organizations maintaining cryptocurrency custody should review signing workflows specifically for UI-layer independence: the Bybit attack succeeded because the signing interface was compromised, not the on-chain contracts. Multi-party custody workflows must include independent UI verification channels – such as hardware wallet display confirmation of raw transaction parameters – architecturally isolated from browser-based signing interfaces.

## Short-Term Mitigations

A hiring audit covering remote software engineers engaged over the past 24 months provides a structured opportunity to apply FBI indicators of DPRK IT worker activity across an existing population. Relevant indicators include use of facilitator email domains associated with known front companies, Social Security numbers with unusual issuance characteristics, and preference for cryptocurrency compensation. The DOJ DPRK RevGen Domestic Enabler Initiative has published guidance for HR and legal teams on conducting this review [10].

Hardware security keys (FIDO2/passkeys) should be enforced for all npm, PyPI, RubyGems, and similar package registry accounts. The Axios compromise depended specifically on a long-lived classic access token — a credential type that persists indefinitely without the maintainer's awareness once extracted. Modern token formats with short TTLs and hardware-bound authentication remove this specific vulnerability, requiring adversaries to maintain persistent device access rather than relying on one-time credential extraction. Developer workstations should also be segmented from production signing environments: the Safe{Wallet} developer compromise succeeded because cloud credentials with production-scope access were present on a developer workstation. Just-in-time access provisioning for production-scoped credentials, with time-bound and audited issuance, closes this lateral movement path.

## Strategic Considerations

The DPRK dual-track model — sustained salary extraction through IT worker infiltration combined with periodic large-scale heists enabled by supply chain compromise — is best understood as a durable, state-resourced adversary program, not a series of discrete incidents. Organizations should plan their security posture accordingly: threat intelligence sharing within sector ISACs, participation in coordinated disclosure processes with package registries, and engagement with government threat intelligence feeds (CISA AIS, FBI Liaison program) provide meaningful uplift when individual organizations cannot maintain the detection surface required to track a nation-state actor operating across multiple attack vectors simultaneously.

The dissolving boundary between "targeting developers" and "targeting financial infrastructure" warrants a corresponding integration of application security and financial security functions within enterprise risk programs. Custody protocols, smart contract signing workflows, and developer endpoint security should be governed under a unified threat model rather than treated as distinct domains.

---

# CSA Resource Alignment

This research note maps directly to several CSA frameworks and publications.

The MAESTRO (Multi-Agent Ecosystem Security, Threat Research, and Operations) framework's threat model for agentic AI is directly relevant to the Bybit and Axios attack patterns, both of which involved manipulation of trusted execution contexts — smart contract signing UIs and npm package delivery pipelines — that downstream agents (human signers and automated CI/CD pipelines, respectively) relied upon without independent verification. MAESTRO's trust boundary analysis principles apply to any context in which a human or automated agent acts on behalf of a principal based on information delivered through a potentially compromised intermediary.

The CSA Cloud Controls Matrix (CCM) addresses relevant control domains including Supply Chain Management and Transparency (STA), Identity and Access Management (IAM), and Security Incident Management (SEF). The IT worker scheme and maintainer compromise both illustrate failures in IAM-02 (Identity Verification) and STA-04 (Third-Party Audits), while the Bybit signing interface compromise implicates CCM control IAM-12 (Segregation of Duties) and SEF-01 (Incident Response Planning).

The CSA STAR (Security Trust Assurance and Risk) program's continuous monitoring model is applicable to organizations seeking third-party validated controls that address software supply chain integrity. STAR Level 2 assessments explicitly evaluate supply chain risk management maturity, providing a structured basis for comparing the controls in place at cryptocurrency custodians, DeFi protocol operators, and software vendors.

The CSA Zero Trust Advancement Center's guidance on workload identity and least-privilege access applies directly to the credential harvesting techniques common to both the Bybit and Axios attacks. A Zero Trust posture that enforces just-in-time, hardware-bound credential issuance and continuous session validation would materially reduce the window of opportunity for post-compromise lateral movement of the type documented in the Safe{Wallet} developer compromise.

CSA's AI Organizational Responsibilities guidance addresses AI-assisted identity fraud — specifically deepfake and generative AI use in hiring fraud — as an emerging organizational risk. The KnowBe4 incident and the broader IT worker program demonstrate that AI-enhanced social engineering now operates at sufficient fidelity to defeat conventional identity verification processes that were designed before generative AI was readily accessible to adversaries.

# References


[1] Chainalysis. "North Korea Stole $2.02 Billion in Crypto in 2025, a Record High." Chainalysis Blog, December 2025.

[2] Chainalysis. "Crypto Hacking Stolen Funds 2025." Chainalysis Blog, January 2025.

[3] U.S. Department of the Treasury OFAC. "Treasury Sanctions Facilitators of North Korean IT Worker Schemes." Press Release, March 12, 2026.

[4] Multilateral Sanctions Monitoring Team. "Joint Statement of the Multilateral Sanctions Monitoring Team on the Report Covering DPRK Cyber and IT Worker Activities." U.S. Department of State, October 2025.

[5] FBI / IC3. "North Korea Responsible for $1.5 Billion Bybit Hack." IC3 Public Service Announcement PSA250226, February 26, 2025.

[6] NCC Group. "In-Depth Technical Analysis of the Bybit Hack." NCC Group Research, March 2025.

[7] Google Cloud / Google Threat Intelligence Group. "North Korea Threat Actor Targets Axios npm Package." Google Cloud Blog, April 2026.

[8] Multilateral Sanctions Monitoring Team. "The Democratic People's Republic of Korea's Violations and Evasions of UN Sanctions Through Cyber and Information Technology Worker Activities." U.S. Department of State, January 2026.

[9] FBI / CISA. "FBI Attributes Ronin Hack to Lazarus Group and APT38." As reported by CoinDesk, April 14, 2022.

[10] FBI / CISA / U.S. Department of State. "Guidance on DPRK Information Technology Workers." IC3 PSA250123, January 23, 2025.

[11] KnowBe4. "How a North Korean Fake IT Worker Tried to Infiltrate Us." KnowBe4 Blog, July 2024.

[12] 38 North. "UN Panel of Experts: The Final Act." Stimson Center, April 2024.

[13] Chainalysis. "2026 Crypto Crime Report: Introduction." Chainalysis Blog, January 2026.

[14] Palo Alto Networks Unit 42. "North Korean Threat Actors Lure Tech Job Seekers as Fake Recruiters." Unit 42 Threat Research, October 2024.


 

[15] Socket.dev. "North Korea's 'Contagious Interview' Campaign: 338 Malicious npm Packages." Socket Security Blog, 2025.

[16] Chainalysis. "OFAC Targets North Korean IT Workers Crypto – March 2026." Chainalysis Blog, March 2026.

[17] Socket.dev. "North Korea 'Contagious Interview' npm Attacks – October 2025 Follow-Up." Socket Security Blog, November 2025.