

Beyond Lazarus: Organization of DPRK cyber capabilities

By TDR Team, Sae V., Coline C., Clifford

Published: 2026-09-07 · Archived: 2026-09-25 02:01:01 UTC

This article was co-authored by Sekoia's TDR team and Kudelski Security as part of a joint research effort.

Introduction

The **Democratic People's Republic of Korea (DPRK)** has established itself as one of the more prominent state actors in cyberspace. For Pyongyang, cyber operations serve as an instrument of sanctions evasion, a means of projecting reach beyond a diplomatically and economically constrained periphery, and a source of revenue for a structurally weakened economy. These capabilities are the **product of a deliberate strategy**, considerably reinforced under Kim Jong-un, which situates information warfare at the centre of contemporary geopolitical confrontation.

The consequences of that strategy are visible in **the growth of the operator base**, the **successive reorganizations** of the institutions holding offensive cyber mandates, and the **expanding frequency and sophistication** of DPRK operations and revenue-generation activity. As the regime continues to consolidate these capabilities and project them globally, an understanding of the DPRK cyber threat has become a practical necessity for governments and private organizations alike.

This paper seeks to provide the elements required for such an understanding: the function of cyber operations within Pyongyang's wider strategic posture, the organization of offensive capabilities across DPRK institutions, and an overview of threat clusters through which that architecture manifests. The research was conducted in partnership between **Sekoia** and **Kudelski Security**.

Strategic development of cyber capabilities

Origin and structure of the regime

The Democratic People's Republic of Korea (DPRK) was proclaimed on 9 September 1948, a few years after Japan's 1945 surrender ended thirty-five years of colonial rule and left the peninsula divided by Soviet and American occupation zones along the 38th parallel. In the Soviet-administered north, Moscow installed **Kim Il-sung**, a former guerrilla commander who had fought Japanese forces in Manchuria, as chairman of the provisional government. Soviet advisers helped build the **Korean Workers' Party (KWP)** and the nascent security apparatus that would outlast the occupation itself.

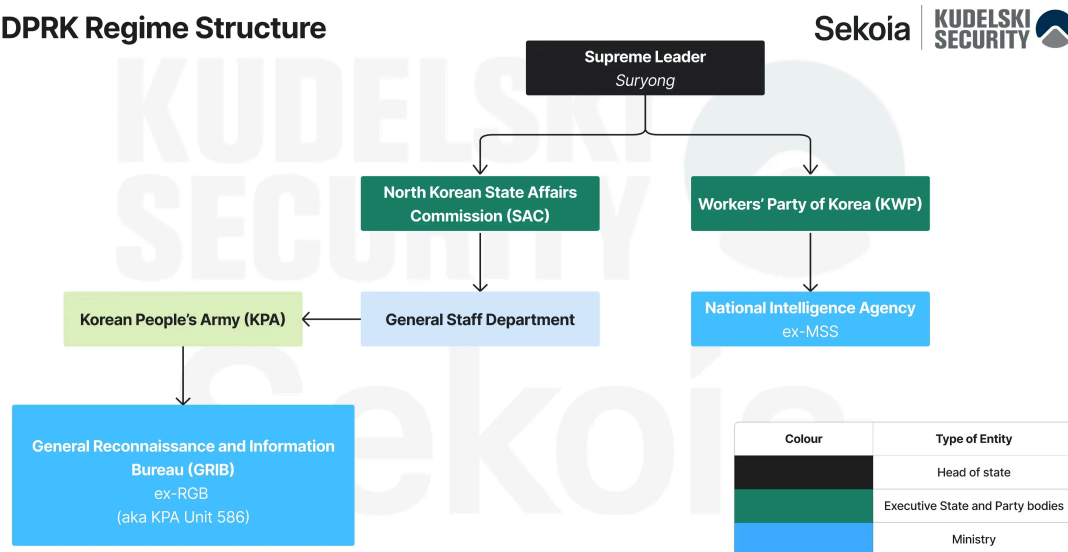
Kim Il-sung consolidated power through the Korean War (1950-1953) and subsequent purges of rival factions. Then, he built a totalitarian, Stalinist-inspired state organized around **juche (self-reliance)** and an increasingly

elaborate cult of personality that was extended, after his death in 1994, to his son Kim Jong-il and, since 2011, to his grandson Kim Jong-un.

Institutionally, the DPRK is a party-state in which the **KWP**, the state bureaucracy (headed by the **State Affairs Commission**, SAC) and the military are formally distinct but functionally fused under the Kim family's personal authority. As chairman of the SAC, supreme commander of the **Korean People's Army (KPA)** and chairman of the KWP's Central Military Commission, Kim Jong-un holds simultaneous command of the party, the cabinet and the armed forces.

Within this structure, intelligence and covert operations, including cyber activity, sit primarily under the **Reconnaissance General Bureau (RGB)**, formed in 2009 by merging several older intelligence organs and reporting directly to Kim rather than through the conventional military chain of command, alongside the General Staff Department of the KPA and the Ministry of State Security.

DPRK Regime Structure



DPRK regime structure

Strategic objectives and their evolution

The regime's overriding objective has remained its own survival against what it portrays as existential threats from Washington and Seoul. From this core goal, three broad and evolving strategic lines can be traced. First, **military-first (Songun policy) deterrence**, which, after the collapse of Soviet and Chinese economic patronage in the 1990s, hardened into a nuclear and missile program **intended to make forced regime change too costly** to attempt. This culminated in nuclear tests from 2006 onward and, more recently, constitutional changes formally vesting command of nuclear forces in the SAC chairman.

Second, Pyongyang has aimed at **asymmetric and covert capability-building**, with the use of electronic warfare, cyber operations, special forces, and proliferation networks, designed to inflict cost on adversaries and generate hard currency while remaining below the threshold of open war. This doctrine has been traced to North Korea's study of the [1991 Gulf War](#) and the [2003 Iraq War](#), and to inspiration drawn from the concept of information warfare developed in China. It was later reinforced by Kim Jong-un's speech at the [3rd Plenary Meeting of the 7th](#)

[KWP Central committee in April 2018](#), when he announced the achievement of the **Byungjin policy's objectives**, which were the development of nuclear capabilities in parallel with the economy. As a new guideline, he stated that the DPRK would focus on socialist economic construction, pivoting from a doctrine of "military-first" to "economy-first". As a result, the number of DPRK cyber operators [doubled that year compared to 2013](#) and lucrative operations targeting cryptocurrency rose as the nascent global crypto market exploded.

Third, [since 2024](#), the DPRK has formally **abandoned the unification goal** that had nominally guided its policy since 1948. Indeed, Kim Jong-un declared inter-Korean relations to be between "two hostile states," and the KWP subsequently dismantled unification-oriented institutions and [revised the constitution](#) in 2026 to define South Korea as foreign territory rather than a temporarily separated part of the same nation. This shift reflects both domestic legitimization needs, with Kim Jong-un increasingly grounding his authority in constitutional and popular-sovereignty language rather than purely dynastic cult of personality claims, and a geopolitical recalculation: deepening alignment with Russia since the invasion of Ukraine, and a long-standing reliance on China, have reduced Pyongyang's incentive to court Seoul or maintain ambiguity for the sake of eventual unification.

Cyber operations as an integrated strategic tool

Cyber capability was progressively folded into this strategic architecture. Kim Jong-il began prioritizing "electronic warfare" after observing the decisive role of networked, [information-enabled forces in the Gulf, Kosovo and Iraq wars](#), reportedly describing cyberattacks as "atomic bombs" of the information age.

His successor, Kim Jong-un, who is a [computer-science-trained leader](#), later called cyber operations an "all-purpose sword" alongside nuclear weapons and missiles. Because cyber operations are cheap compared to conventional weapons, deniable, and effective against wealthier and more networked states, such as South Korea and the United States, they became a natural extension of the asymmetric-deterrence line of DPRK.

Consequently, cyber operations have moved from a niche military-modernization experiment (cf. [2009-2011 DDoS attacks](#)) to a load-bearing pillar of DPRK statecraft, simultaneously an **intelligence tool**, a **sanctions-evasion mechanism**, and a **revenue stream** for the nuclear and missile programs that anchor the regime's core survival strategy under Kim Jong-un's influence.

Computer networks exploitation (CNE) and attack (CNA) became a core priority, with [talented children identified in school](#) to integrate elite hacking universities, the emergence of **first DPRK-led destructive cyber operations** (Operation DarkSeoul 2013, Sony Pictures Hack 2014, WannaCry 2017), the **multiplication of intelligence gathering** operations, and the **systematic use of cyber campaigns** for revenue generation.

Indeed, from [roughly 2014 onward](#), cyber operations became an increasingly important **financing mechanism** for the heavily sanctioned DPRK economy, as the regime shifted from pure espionage and sabotage toward bank heists, ransomware, and large-scale cryptocurrency theft (cf. the 2016 Bangladesh Bank \$101 million heist and [the 2025 Bybit \\$1.5 billion theft](#)), reportedly generating [hundreds of millions to over a billion dollars annually](#) to help fund weapons programs.

Institutions with offensive cyber mandates

Mandates and operational roles

As previously mentioned, the North Korean regime relies on institutions such as the **Korea Workers' Party (KWP)** and the **General Reconnaissance and Information Bureau (GRIB)**, formerly known as the **RGB** to facilitate its offensive cyber operations. These operations are considered to be an **integrated strategic tool** or an “all-purpose sword” to achieve the economic and geopolitical objectives of the regime.

General Reconnaissance and Information Bureau (GRIB) 경찰정보총국, ex-RGB 경찰총국

The **GRIB** is **considered** to be the Kim regime's **leading foreign intelligence agency** and **military reconnaissance unit**. However, its [functions](#) are far broader than a traditional military intelligence agency. In addition to intelligence collection and clandestine operations, the GRIB **commands the DPRK's most capable cyber offensive and combat units**. Furthermore, The bureau has used [front companies](#) such as the UN-designated Green Pine Associated Corporation (KPe.010) to conduct illicit arms trade and procurement.

To conduct these varied operations, the GRIB (ex-RGB) is [uniquely placed](#) within the DPRK political and military structure. The agency is hierarchically under the North Korean State Affairs Commission (SAC) and **reports directly** to the KPA Supreme Commander Kim Jong-un. Concurrently, its administrative military designation is **KPA Unit 586**.

Before the RGB was established, Demilitarized Zone (DMZ) infiltration operations were [handled](#) by the KPA Reconnaissance Bureau, a long-standing unit under the KPA General Staff. In 2009, as Kim Jong-un prepared to take power, North Korea restructured this bureau into the RGB, a **large consolidated task force**. The new RGB merged the former Reconnaissance Bureau's large-scale reconnaissance and infiltration functions with the KWP Operations Department and the overseas intelligence operations of KWP Office 35.

Thus, the **RGB** at its inception in 2009 represented **streamlined control and command** of all intelligence operations. Cyber warfare capabilities have also [grown](#) in their effectiveness and importance to the Kim regime more than any other operational functions, thus the reorganization allowed for better control by the Supreme Leader for command as well as political-military oversight.

National Intelligence Agency (NIA) 국가정보국, ex-MSS 국가안전보위성

The National Intelligence Agency (NIA), formerly the Ministry of State Security (MSS) is the regime's [primary](#) counterintelligence, and secret police agency, tasked with **internal security** and protecting the leadership from **domestic and foreign threats**. It reports directly to the State Affairs Commission under Kim Jong-un, ensuring loyalty to the ruling party. Though it is primarily an internal security body, it is also believed to coordinate with military and cyber units to **support regime stability and strategic goals**, including conducting intelligence operations targeting foreign governments, defectors, and dissident groups.

In June 2026, this Ministry was [renamed](#) as the **National Intelligence Agency (NIA)**, or the State Intelligence Agency. Originally, the MSS operated counterintelligence and counterespionage missions, conducting cyber campaigns targeting defectors and DPRK experts. Its renaming was likely as a sign of an expansion of its field of competencies, especially for **foreign missions** and of a new repartition with the **Ministry of Public Security (MPS)**, which will likely assume the role of a **domestic police force**.

Korean Workers' Party (KWP) 조선로동당

Kim Jong-un frequently signals his [priorities](#) for economic and military development in his annual addresses to the KWP plenary meetings. After these addresses, the cyber program's units are observed to **quickly shift** to new mission areas in line with Kim's statements. Thus, the KWP is crucial to sense the **political direction** which mandates cyber offensive activities.

The KWP also retains a [parallel](#) role through bodies like the **Organization and Guidance Department (OGD)**, which controls senior personnel appointments across the party, military, and government and enforces the regime's internal political and censorship controls, giving the party a supervisory hand over the same personnel pipeline that feeds intelligence units. Additionally, [educational programs](#) in DPRK universities focusing on developing skills in science, technology, engineering, and math (STEM), which ultimately produce “**information warriors**” are also set up under the direction of the KWP.

Institutional reorganization

Despite the existence of institutions clearly identified as housing **North Korea's offensive cyber capabilities**, the **frequent reshuffling** of responsibilities makes mapping the hierarchy of political-military entities including units, bureaus and liaison offices difficult.

According to some DPRK-watchers, North Korean intelligence agencies have continuously been [reorganized](#) and/or redesignated, shifting between combined and independent structures over time to align with the regime's **strategic goals**. For instance, in March 2026, the regime **removed references** to [reunification](#) with South Korea from the DPRK constitution, signaling a push for a more hostile policy toward South Korea. The push for the restructuring of the **GRIB** (ex-RGB) and **NIA** (ex-MSS) came soon after, possibly reflecting an effort to realign the intelligence apparatus with the leadership's long-term state-building goals.

Moreover, splitting intelligence missions across multiple agencies creates competition among them for the Supreme Leader's favor. This allows him to keep the agencies watching one another, which strengthens regime security and longevity; a [key goal](#) of the regime being its **survival**, and **response** to global events.

By analyzing the roles of North Korean entities with cyber offensive functions, certain plausible links can be drawn between their nomenclatures and roles. It must be noted that certain discrepancies will remain and these entities are subject to frequent change.

Nomenclature	Role
Department (부 / -부)	A major, publicly acknowledged pillar of the party bureaucracy
Bureau (국 / -국)	Used at multiple levels to designate executive or operational arms; tends to be an operational command or executive body, often military or security-related, that implements rather than sets policy
Office (실/처)	Smaller, secretive units. North Korea is notorious for giving some of its most sensitive ones anonymous numbers rather than descriptive names

Nomenclature	Role
Unit (부대 or 소조)	A numeric cover designation applied at variable scale, from small operational cells up to entire bureaus
Military units (corps, brigades, etc.)	Conventional troop formations, unrelated to the party apparatus

DPRK-nexus intrusion sets and operational clusters

Organizationally, offensive cyber operators are **largely diluted** into various entities, inside and outside DPRK borders.

Units related to publicly tracked Advanced Persistent Threats (APTs) are intrusion sets sitting mainly within the **GRIB** (ex-RGB), and to a smaller extent, within the **NIA** (ex-MSS). An **intrusion set** is a cluster of malicious cyber activity characterized by its specific victimology, a dedicated arsenal, comprising tools and malware, and key patterns in terms of infrastructure and Tactic, Techniques and Procedures (TTPs).

In addition, DPRK cyber activity is supported by **fake IT workers**, who are North Korean nationals and foreigners recruited to secure technical jobs, channel salaries and information back to the regime, and/or conduct operations from abroad.

In this section, we will present the DPRK-nexus threat actors conducting offensive cyber operations to support Pyongyang strategic objectives, evade sanctions and fund ballistic missiles and nuclear programmes.

An important characteristic of these activity clusters is that **they almost all conduct lucrative operations**. For some of them, it constitutes their main operational objective, while, for others, notably with a focus on cyberespionage, it can be explained by a need to **self-fund** their operations.

DPRK-nexus APTs

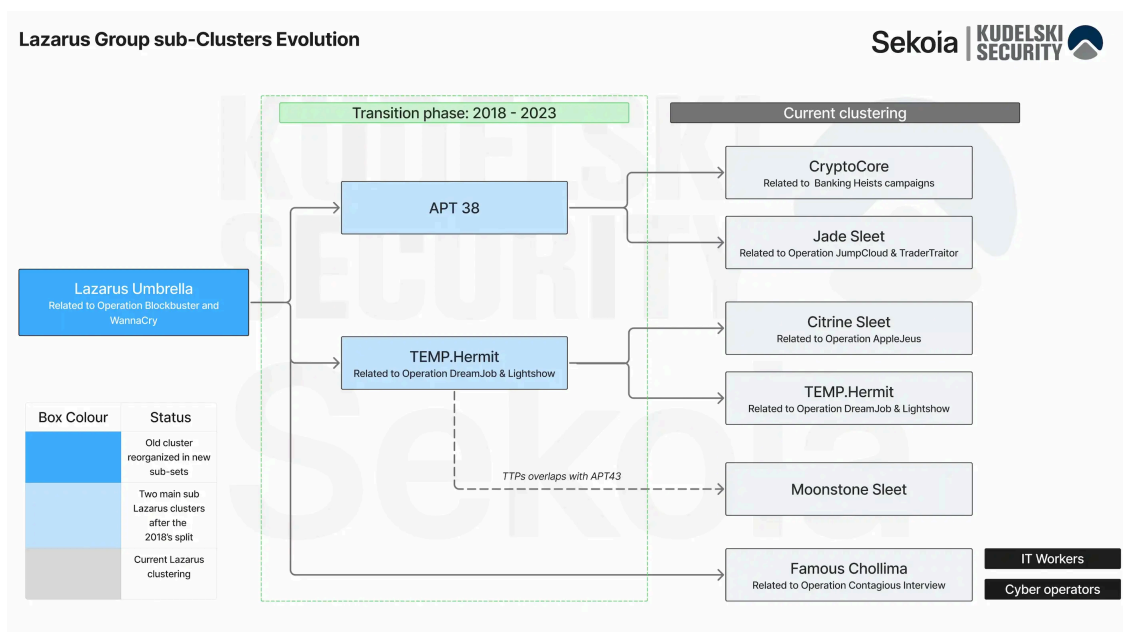
Since the integration of offensive cyber capabilities in DPRK strategy, sophisticated units were implemented, often tracked as **APTs**. These clusters have been mandated to conduct various types of operations, ranging from **financially-motivated campaigns**, to **cyber espionage**, **sabotage** and **influence**.

DPRK-nexus APTs

Espionage	Kimsuky, TEMP.Hermit
Financial Gain	CryptoCore, Jade Sleet, Citrine Sleet
Espionage and Financial Gain	Andariel, Famous Chollima, Moonstone Sleet
Repression	Reaper

DPRK-nexus APTs

As explained previously, these units have been regularly reorganized and renamed, making the understanding of North Korea's cyber ecosystem complex. We categorized DPRK-nexus threat clusters depending on their TTPs and the type of operations they conduct. We notably made our clustering evolved by splitting the **Lazarus umbrella** into six distinct sub-clusters: TEMP.Hermit, Citrine Sleet, CryptoCore, Jade Sleet, Moonstone Sleet, and Famous Chollima. **Famous Chollima** distinguished itself by representing malicious activity related to fake IT workers, which often supports the operational objectives of other cyber warfare units.



Lazarus Group sub-Clusters evolution

Strategic espionage

DPRK-nexus threat clusters **focusing primarily** on intelligence collection sit under the **GRIB** (ex-RGB). Even if their affiliation to the [3rd](#) and/or the [5th Bureau](#) is debated among the CTI community, they are the inheritance of the historical **Lazarus umbrella** and **Kimsuky** cluster.

We identify cyberespionage as the primary objective of the threat clusters mentioned below, as their arsenal and associated campaigns pointed out to intelligence collection capabilities. However, they also happened to conduct cybercrime activity at the margin, likely to self-fund their operations.

Similarly to the Lazarus umbrella, which is now associated with several threat clusters, likely reflecting an internal reorganization following an increase in the number of operators, **Kimsuky** is regarded [by some DPRK experts](#) as a mega-cluster comprising several branches, like **TA406** and **TA408** among others.

Espionage-Oriented Threat Clusters				Sekoia KUDELSKI SECURITY 
Intrusion Set	Active since	Sectors Targeted	Geographies Targeted	Related Campaigns
Kimsuky	2013	Defense, Government, Research, Media, Energy, Finance	South Korea, US, Japan, Europe	Korea Hydro and Nuclear Power Breach (2014), Babyshark (2018-2020), KAERI breach (2021), SHARPEXT (2021-2023), DMARC abuse (2023-2025), MoonPeak (2024), HttpSpy (2026)
TEMP.Hermit	2019	Defense, Aerospace, Government contractors, Media, Technology, Cryptocurrency, Nuclear sector	Global	Operation DreamJob (2019-2026), Operation In(ter)ception (2019-2020), TeamCity CVE exploitation (2023), Trojanized CyberLink installer (2023)

Espionage-oriented threat clusters

Historically, DPRK-nexus threat clusters associated with cyberespionage campaigns also conducted **sabotage** operations leveraging wipers. Well-known cases are the **Operation Dark Seoul** (2013), and the **Operation Blockbuster** (Sony Picture Hack) (2014) attributed to **Lazarus**. **Kimsuky** was also observed using wiper components during the **Korea Hydro and Nuclear Power breach** in 2014. However, no investigations pointed out the use of wipers in recent campaigns, likely due to refocus on stealthy espionage operations. The most recent case was **APT38**, now considered as splitted between **CryptoCore** and **Jade Sleet**, which was a financially-motivated threat cluster, which leveraged disk-wipe techniques ([KillDisk](#)) as an anti-forensics measure in 2017.

Dual-mandate: Espionage and revenue generation

Characteristic of Pyongyang's strategy, a set of DPRK-nexus threat clusters conduct **both financially-motivated campaigns and cyberespionage**, likely to support the development and the [funding](#) of the nuclear and ballistic missiles programs.

Of note, **Andariel** is particular as it used custom ransomware (Maui and H0lyGh0st) for financial theft, as well as ransomware-as-a-service (RaaS) developed by an operator of the Russian cybercrime ecosystem. It was notably [observed](#) collaborating with **Play** in 2024. Another DPRK cluster, **Moonstone Sleet**, acted similarly by deploying its custom malware **FakePenny** in 2024, but also the **Qilin** RaaS in 2025. It is interesting to note that the two clusters integrated RaaS in their campaigns within two months of each other.

Lucrative and Espionage-Oriented Threat Clusters

Intrusion Set	Active since	Sectors Targeted	Geographies Targeted	Related Campaigns
Andariel	2014	Defense, Finance, Gambling, Healthcare, Aerospace, Nuclear sector, Manufacturing, Education	South Korea, the US, Japan, Europe	Campaign Rifle (2015-2017), Operation Bookcodes (2019-2020), Maui ransomware (2021-2022), HolyGhost ransomware (2021-2022), and SHATTEREDGLASS ransomware deployment (2021), TeamCity CVE exploitation (2023), Cyberespionage against Defense and aerospace (2022-2024), Play ransomware collaboration (2024), RID hijacking (2024-2025), South Korea financial sector (2026)...
Famous Chollima	2018	Cryptocurrency industry, Web3, Decentralized Finance	Global	Contagious Interview/DEV#POPPER/Deceptive Development (2022-2026)
Moonstone Sleet	2023	Technology, Education, Defense	Global	DeTankWar game operation (2024), FakePenny ransomware deployment (2024), Malicious npm packages (2024), Qilin RaaS deployment (2025)

Lucrative and espionage-oriented threat clusters

Revenue generation

In a **transition phase** during which the Lazarus umbrella likely reorganized internally, the group was divided into sub-clusters, likely specializing their activity between financial gain and espionage. This evolution happened between **2018 and 2023**, in the context of an expansion of the cryptocurrency market globally.

As a result, the sub-cluster **APT38** was identified and associated with financially-motivated operations likely conducted by the **110th Research Institute** under the GRIB (ex-RGB). It focused on the targeting of the cryptocurrency industry, Web3 and blockchain technologies.

Currently, APT38 has likely splitted in two sub-clusters that we associate with **CryptoCore** and **Jade Sleet** as a result of our research. These two clusters are characterized by focusing exclusively on financially-motivated campaigns, likely to generate revenue for the regime.

Lucrative-Oriented Threat Clusters

Intrusion Set	Active since	Sectors Targeted	Geographies Targeted	Related Campaigns
Citrine Sleet	2018	Financial institutions, then Web3	Asia, then Global	Operation AppleJeus (2018-2021), Impersonation of a crypto exchange representative (2022), 3CX Supply chain attack (2022-2023), FudModule (2024), PondRAT PyPi campaign (2024)
Cryptocore	2018	Financial institutions, then Web3	Global	Dangerous Password (2018-2023), SnatchCrypto campaign (2020-2022)
Jade Sleet	2020	Blockchain technology, Cryptocurrency Exchange, Gambling, Web3	Global	Operation TraderTraitor (2020-2022), Ronin Network/Axie Infinity Breach (2022), JumpCloud compromise (2023), Bybit theft (2025), Exchanges and Web3 intrusions (2025-2026)

Lucrative-oriented threat clusters

Surveillance and internal repression

In line with the **NIA** (ex-MSS) mandate, the related threat cluster **Reaper** focuses on DPRK defectors, South Korean DPRK-focus activists and NGOs, acting as a secret police with cyber means. [This new ministry name](#) implemented in 2026 likely confirmed the wide range of sectors, mainly in South Korea, targeted by Reaper for espionage. Indeed, it is likely as a sign of an expansion of MSS competencies and of a new repartition with the **Ministry of Public Security (MPS)**, which will likely assume the role of a police force focused on internal affairs.

Reaper also likely increased in 2024, with the dismantlement of the **United Front Department**. According to [analysts](#), cyber operators from the United Front Department were transferred notably to the GRIB (ex-RGB) and to the NIA (ex-MSS).

Repression-Oriented Threat				Sekoia KUDELSKI SECURITY 
Intrusion Set	Active since	Sectors Targeted	Geographies Targeted	Related Campaigns
Reaper	2012	Defectors, Activists, NGOs, Government, Education, Energy, Finance, Media	South Korea, North Korea	Operation Daybreak (2016), ROKRAT campaign (2017-2026), Operation Golden Time (2017-2018), InkySquid campaign (2021), Internet Explorer CVE exploitation (2022), Operation Code on Toast (2024), KoSpy operation (2022-2025), PubNub compromise (2025), BirdCall breach (2025-2026)...

Repression-oriented threats

IT worker operations

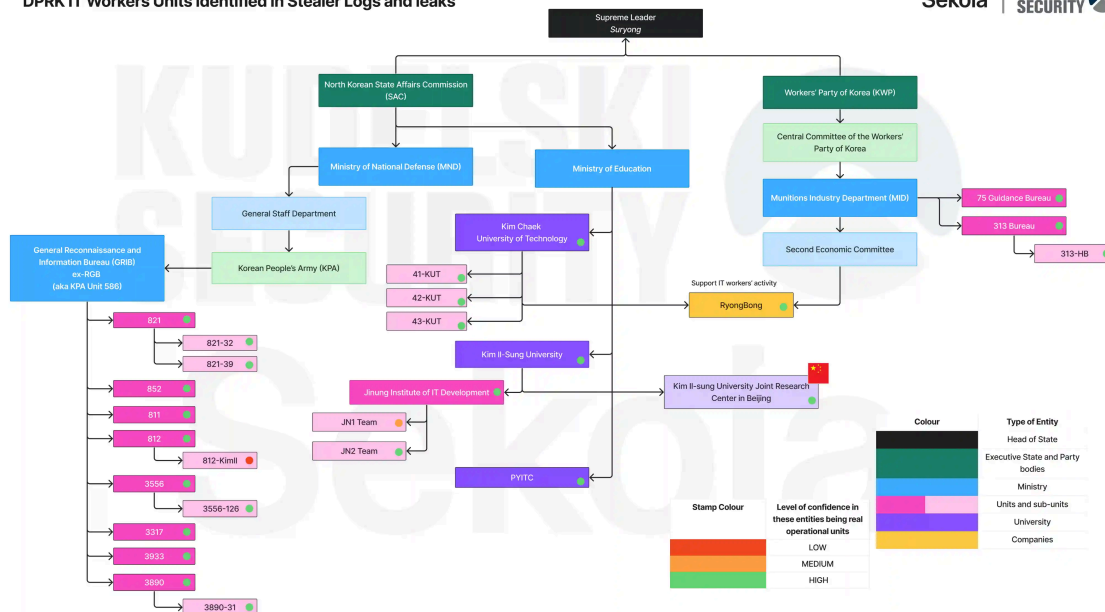
Beyond the operations of APTs intrusion sets, the DPRK's offensive cyber capabilities are complemented by the activities of **IT workers**. They are skilled individuals, predominantly DPRK nationals and in some cases supported by foreign facilitators recruited online, tasked with **generating revenue** for the regime in order to circumvent international sanctions and finance the country's ballistic missile and nuclear programmes.

The IT-worker programme **adapts an established practice** rather than inaugurating a new one: the dispatch of North Korean labor abroad to earn foreign currency dates to the 1960s and 1970s, beginning with logging in the Soviet Far East before broadening into construction, textiles and restaurant services across Russia, China, the Gulf and Africa. The shift into the IT sector is documented publicly from at least 2018, when the [US Treasury designated](#) Yanbian Silverstar and Volasys Silverstar as IT-worker front companies, and was set out systematically in the [2022 joint advisory](#) of the US Departments of State and the Treasury and the FBI.

Their number is [estimated in the thousands](#), operating both within and beyond the DPRK's borders and systematically obfuscating their location and identity in order to **secure contracts in the IT sector**. Such employment serves as leverage in two respects: it enables the **remittance of salaries** to the regime, and it affords privileged access from which to **conduct operations** for financial gain or espionage.

Cross-referencing [open-source reporting](#) with [stealer logs](#) surfaced the profiles of IT workers themselves, indicating that they draw on the same infrastructure as the operators conducting intrusions. **Infiltration appears in part opportunistic rather than target-driven**. In the cases observed, workers queried internal corporate documentation while nominally engaged as employees, and reproduced the same behavior within client organizations where they can be deployed as remote consultants. This placement model allows them to extend **their reach** beyond the entity that contracted them.

DPRK IT Workers Units Identified in Stealer Logs and leaks



DPRK IT workers units identified in stealer logs and leaks

The workers are organized into units embedded across a **heterogeneous range of host entities**: DPRK military and state institutions, state-owned enterprises, front companies, legitimate businesses abroad, and [universities](#). Although the units from which they operate are not concentrated within a limited set of characteristic organizations, it can nonetheless be monitored through their **means of communication**, which are considerably more constrained. Three channels can be distinguished:

- Chat platforms, mainly **Slack** and **IP Messenger** (IPmsg);
- Machines designated **PC-call**;
- A proxy operated by **Ryonbong** and marked as "RB".

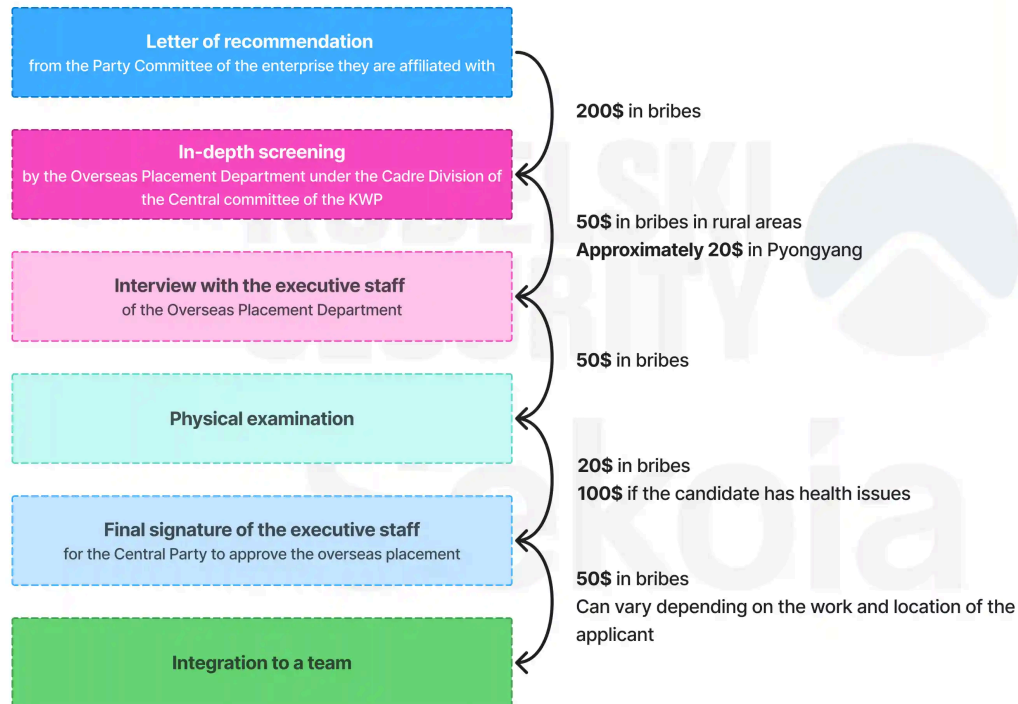
An interesting inflection point in these communications can be situated around October 2022. Internal exchanges, previously conducted in Korean and in a markedly formal register, thereafter **shifted to English**, a change assessed to follow a directive, and consistent with aligning working practices to international norms while reducing the distinctiveness of the workers' online presence.

Internal policy on internet access likewise appears **considerably more permissive** than for the ordinary DPRK citizen: identified users adopt working pseudonyms drawn from Western, South Korean and Japanese popular culture (G-Dragon, Superman, James Bond, Harry Potter, Olaf, Kisame). The practice presupposes a degree of cultural exposure, and a latitude in displaying it, unavailable to the general population.

Recruitment into IT workers roles follows a **formalized selection process**, notably documented by the [Korea Institute for National Unification](#), which indicates that access to the function is far from open to the general population. Candidates must first satisfy vetting on political and social background, both their own (*songbun*) and that of their family (*todae*), before they can be considered for overseas deployment. Individuals with relatives resident abroad are excluded from selection outright, and a substantial proportion of those eventually dispatched have prior employment in Pyongyang or other major cities. At the final stage, candidates seeking a particular

destination are expected to pay for it, the scale of the bribe varying with the nature of the mission to which they are assigned.

IT Workers Recruitment Process



Source: Korea Institute for National Unification

IT workers' recruitment process

Stealer logs indicate that selection is followed by a **structured onboarding phase**. The material recovered covers the workers' assigned objectives, prescribed means of communication, the platforms to be used in conducting fraudulent activity, and a body of development-related reference questions. The presence of such material suggests that workers enter the programme with little or no direct exposure to the outside world, and that the requisite operational and cultural knowledge is supplied at induction rather than presupposed.

DPRK Fake IT Worker Onboarding

General Questions:

How many freelancer sites are there, and what are they?

Freelancer, upwork, workana, Fiverr, Toptal, Guru,

What are common rules while using upwork and freelancer?

All clients and freelancers mustn't use other communication tools.
In other words all transactions should be performed only in their site.

What countries do the best clients come from? List 5 countries at least

USA, Australia, New Zealand, Swiss, Canada, Belgium

How many communication platforms are there, and what are they? List 3 platform names at least

Skype, Telegram, Discord, Slack, WhatsApp

Explain about github working flow what you experienced so far

And then there are branches. Remote branch and local branch.
All devs works in local branch.
After working they add their updated contents to remote branches.
So project manager can manage all processes of developing.

What is typescript and the benefits of using them.

TypeScript is a language that is inherited from Javascript. In typescript all variables have their data types.
Benefits: In developing tracking debug is easy.

Explain feelings after you access the internet.

I am very stressful and I think this is my biggest challenge in my life.

What is deposit/withdraw/pending in all platforms generally regarding payment?

Comment [1]: Song: have you ever heard about PPH?

Comment [2]: Another freelancer account: Guru

Comment [3]: Song: not only communication platforms, but also other external payment platforms not allowed.

Comment [4]: Australia is 3rd ranked country

Comment [5]: 1. Create repository
2. Clone repository
3. Create branch
4. Working and commit changes
5. Push latest updates(commits) to Github (local to original branch)
6. Create Pull Request to other branch
7. Review branch
8. Approve to merge Pull Request.

Comment [6]: Better productivity as well

Comment [7]: Hahaha, don't get stress. But more and more trying.

DPRK Fake IT worker onboarding

The primary function of DPRK IT workers is the **generation of revenue** for the regime, directed towards circumventing international sanctions and financing its ballistic missile and nuclear programmes. The restrictions on DPRK labor abroad were introduced incrementally by the United Nations **through 2017: [decision UNSCR 2371](#)** capped worker numbers at existing levels; **[the decision UNSCR 2375](#)** barred the issuance of new work authorisations ; and **[the decision UNSCR 2397](#)** required the repatriation of all DPRK nationals earning income in member states' territories by 22 December 2019.

The cumulative effect was to remove any lawful basis for employing DPRK labor abroad. However, as **each obligation is linked to nationality**, concealing this fact at the time of recruitment places the transaction outside the scope of the ban, at least from the employer's perspective. The IT workers model therefore relies on the **use of a false identity** during recruitment, and on the **laundering of the resulting profits**. Documented conversion methods [include](#):

- Converting stolen assets **via centralized exchanges or OTC trades**, using proxy accounts run by local facilitators to bypass Know Your Customer (KYC) checks;
- Exploiting **decentralized exchanges** with weak ID verification to swap stolen assets for other cryptocurrencies, followed by cashing out to fiat;
- Conducting crypto-to-cash trades on **peer-to-peer (P2P) platforms**, splitting large amounts into smaller, staggered transactions to avoid detection.

Alongside APT groups, DPRK **IT workers** are also [found](#) to be engaging in cryptocurrency thefts. Some documented instances include [OnyxDAO](#) (\$3.8 million), [Munchables](#) (\$62.5 million) and Exclusible Penthouse

(\$827,000). It is interesting to note that in one of the theft operations in (Munchables 2024), funds stolen by probable IT workers were ultimately returned **due to operational challenges** faced in the laundering process.

Enabling ecosystem: Indirect and supporting entities

As a heavily sanctioned country, the DPRK has constructed a complex network of intermediaries, whether **educational, entrepreneurial, or criminal**, to [enable](#) its cyber offensive operations. These intermediaries fall into two broad categories.

The first is educational institutions, which serve a **dual purpose**. They train the DPRK's cyber operatives, and, in the later stages of education, they function as **operational nodes** for offensive activity, particularly when located in allied countries such as China or Russia.

The second is a web of third-country relays and enterprises. These help the DPRK overcome domestic technical constraints related to infrastructure and networks, enable plausible deniability, and serve as financial relays to circumvent sanctions.

Educational institutions

North Korean educational institutions

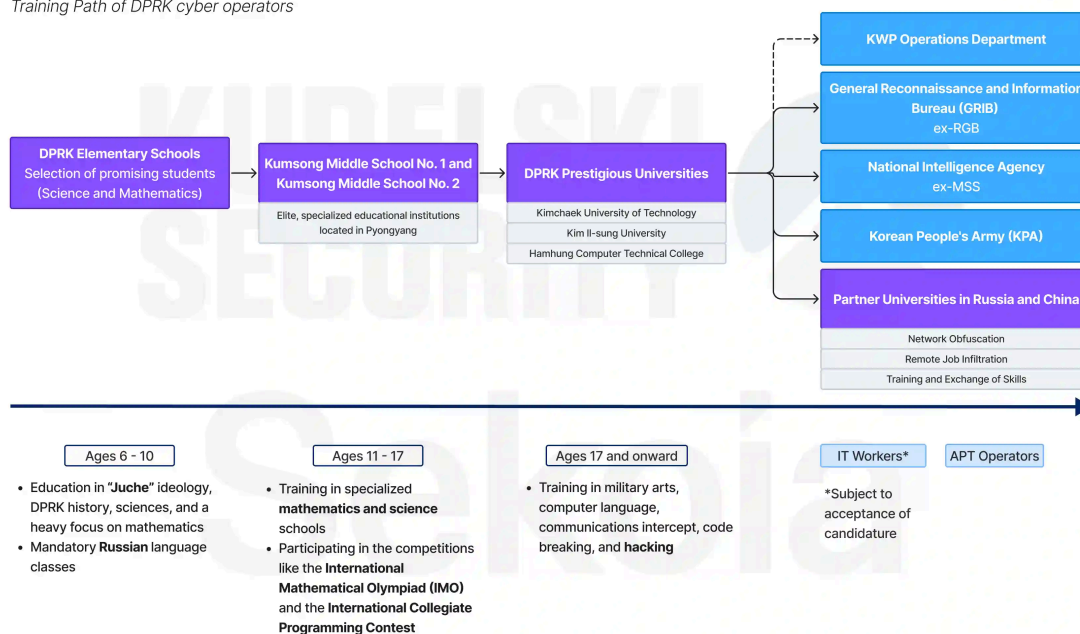
North Korean Institutes are the first stepping stone in the training of cyber operators, starting as early as primary school. The brightest students, aged 11 to 17, are [funneled](#) through elite, specialized educational institutions like **Kumsong Middle Schools** located in the capital, before advancing to **Kim Il-sung University and Kim Chaek University of Technology** to begin their training as “cyber warriors”. Other colleges like **Hamhung** and **Moranbong** focus on cyber engineering, giving students roughly [ten years](#) of training by graduation.

In exchange, families get [perks](#) like Pyongyang relocation and extra rations. At university, top performers are chosen for advanced hacking training, then [commissioned](#) into the KPA's **GRIB** (ex-RGB) or placed in IT units under the **Munitions Industry Department (MID)** or **Ministry of National Defense (MND)**. This process can be observed in the following talent pipeline.

DPRK Talent Pipeline

Training Path of DPRK cyber operators

Sekoia KUDELSKI SECURITY



DPRK talent pipeline

Beyond this internal talent recruitment process, the DPRK also relies on exchanges with foreign universities to train its operators. These exchanges also serve as **operational channels** thanks to the close ties between the DPRK and the host country. This is particularly evident in the cases of China and Russia.

Academic exchanges between North Korea and the PRC

North Korea and China have historically maintained close-relations, owing to a [shared](#) history of communist movements. Today, China remains one of North Korea's closest allies despite a [tumultuous](#) relationship. Thus, it is not surprising that formal training and access to resources for DPRK cyber talent is also provided through a **network of universities** in China.

During our investigation, we found mentions of several Chinese universities in stealer logs of DPRK IT workers, including **Shanghai University of Electric Power**, **Chongqing University** and **Beijing Institute of Technology**. The complete list of universities can be found in Annex 1. According to official diplomatic [communications](#), "DPRK students at institutions such as Jilin University and Yanbian University gain insights from China's reform and opening-up, and advancements in science and technology, which they bring back to their country".

However, these universities are known to host DPRK-nexus malicious actors, for instance in [joint research](#) centre facilities, and offer them operational stability.

North Korea has also replicated this strategic model in Russia to expand its operational footprint, especially as Beijing increasingly seeks to [distance itself](#) from North Korea to avoid Western sanctions.

Academic exchanges between North Korea and Russia

Alongside the [strengthening](#) of long-existing ties between Russia and North Korea, educational exchanges between these two countries also **expanded quickly** since the former's 2022 invasion of Ukraine. This is highlighted by mandatory Russian language schooling in the DPRK, increased university scholarships, and high-level academic [delegation](#) visits.

Indeed, Russian is now a [compulsory subject](#) in DPRK schools from the 4th grade onward. According to Alexander Kozlov, co-chair of the **intergovernmental commission of the Russian Federation and North Korea**, 96 North Korean citizens were accepted to Russian universities. Furthermore, Russia [granted](#) over 36,000 entry visas to North Koreans in 2025 (a fourfold increase from 2024) among which over 98% were for education. These [closer ties](#) with Moscow are likely used to uplift Kim Jong un's domestic image as a strong leader.

We observe that a key difference between the DPRK's exchanges with Russia and China lies in **visa transparency**: As of August 2026, Russia has [publicly disclosed](#) detailed data on visas issued to North Korean nationals, while China has not. This asymmetry might reflect, in part, China's **tactical ambiguity**, which aims to [avoid](#) being drawn into the conflict the DPRK faces with the West.

Finally, it is crucial to note that while these exchanges likely include some training and knowledge-sharing with partners who have well-developed cyber offensive ecosystems, such as China and Russia, their [primary aim](#) is to **gain access to third-country networks** in order to conduct cyber offensive operations.

Front companies and money laundering hubs

North Korea often obscures its **operational origins** by leveraging [overseas intermediaries](#), particularly **physical relay networks** as channels for conducting cyber operations and **criminal enterprises** for laundering illicit funds.

Firstly, this allows the regime to **compensate for its limited domestic internet infrastructure** (2 325 IPS and 1 ASN [in the DPRK](#), compared to 344 902 269 IPs and 6 656 ASNs [in China](#)) by rerouting attacks through [relay networks](#) in allied countries like China and Russia. Secondly, it allows for a web of state-sponsored, private and criminal actors to **cooperate** and **generate revenue** for the regime while evading sanctions.

Physical relay networks

Physical relay networks have not only served as a financial and infrastructural [channel](#), but also as a **physical base** for DPRK cyber operations. In this context, physical relay network refers to overseas hubs, such as offices, hotels, or front companies staffed or frequented by DPRK operatives, that provide a base outside North Korea for conducting operations and generating revenue.

These operational networks are notably located in China, Russia, Southeast Asia, and certain African countries. Among them, China stands out, given its status as a historical partner of Pyongyang. These intermediaries can be both **fronts** or **legitimate businesses** with operators working for North Korea abroad. For instance, a [member](#) of the Lazarus Group was associated with **Chosun Expo**, which is a North Korean **front company** based in China. Additionally, operatives from Bureau 121, allegedly responsible for the 2014 Sony hack, were speculated to be [working](#) from **Chilbosan Hotel in Shenyang, China** during the operation. These methods were likely used to enable North Korea to plausibly deny its cyber operations.

Yet another example is **Chinyong Information Technology Cooperation Company (Chinyong)**, a sanctioned North Korean enterprise subordinated to the Ministry of People's Armed Forces (KPe.054), active since at least 2016. The enterprise is [involved](#) in the **employment of DPRK IT workers** overseas and the generation of **illicit revenue** abroad. Chinyong's teams are primarily known to [operate](#) out of China, Laos, and Russia, where they engage in "traditional" freelance IT work, as well as in cryptocurrency theft using their insider access to blockchain projects.

In the African continent, DPRK [front companies](#) such as **Junggongchon Trading Corporation** are known to deploy IT worker teams in countries like **Tanzania**. According to the [Chollima group](#), DPRK operatives are also likely deployed in **Guinea** and **Nigeria** through similar fronts.

At times, this physical infrastructure extends into the target countries themselves. In the United States, there were documented cases of "[laptop farms](#)", which are third-party proxies used by DPRK IT workers to receive company-issued laptops, allowing them to appear as though they are working from within the US while operating from abroad.

Of note, physical relay networks are not only used by rank-and-file IT workers who are deployed abroad, but also by **APT operators**. For instance, Kudelski Security [observed](#) that fake IT workers and offensive teams often share the same VPN exit nodes. It is thus plausible that these operators either conduct cyber operations alongside their ostensible day-to-day work or, in the case of front companies, do so on a **full-time basis**, coordinating with counterparts based inside the DPRK.

Criminal enterprises

The DPRK has [historically](#) exploited **underground criminal systems** to support state-building activities. Until the late 2010s, the most lucrative state-sponsored criminal operations included the smuggling of cigarettes and the creation of counterfeit money. Following the DPRK's pivot toward cyber operations as a source of illicit revenue, DPRK-nexus intrusion sets have applied a similar playbook to launder the proceeds of their operations.

These actors launder funds through criminal networks notably across Southeast Asia by [actively exploiting](#) the region's vulnerable and weakly-regulated financial environment linked to local illicit actors. In particular, casinos and cryptocurrency exchanges with **high-volume cash conversion channels** in **Myanmar, Thailand, Laos, and Cambodia** have served as key operational nodes for **money laundering**.

Cambodia, in particular, has emerged as a laundering hub due to its less regulated financial and gambling sectors, with an estimated **\$37.6 million** in North Korea-linked cryptocurrency laundered between 2021 and 2025 through the Cambodia-based **Huione Group**, whose [executives](#) have shown indications of direct ties to North Korean actors. Huione's infrastructure, including technical tools that facilitate scams and **stablecoins** that cannot be frozen, has allowed North Korea to bypass regulations, convert illicit proceeds into ostensibly legitimate assets, and **sustain revenue generation** from its cyber operations.

Conclusion

The DPRK's offensive cyber apparatus is not an adjunct to the regime's strategy but a constituent part of it. Most states maintain cyber capabilities for intelligence collection and military contingency, Pyongyang has additionally

constituted them as a source of state revenue, notably to fund its nuclear and ballistic missile programmes, and that model has proven durable under sustained international pressure. The intrusion sets examined in this paper and the IT worker programme operating alongside them both serve this dual purpose.

Several conclusions can be drawn. First, the institutional map is **unstable**. Mandates are redistributed between bureaus, organs are periodically reorganized, and certain entities operate transversally rather than within the hierarchy. Ryonbong is a great example: its formal position within the defense-industrial structure does not necessarily translate its operational responsibility in IT workers' campaigns.

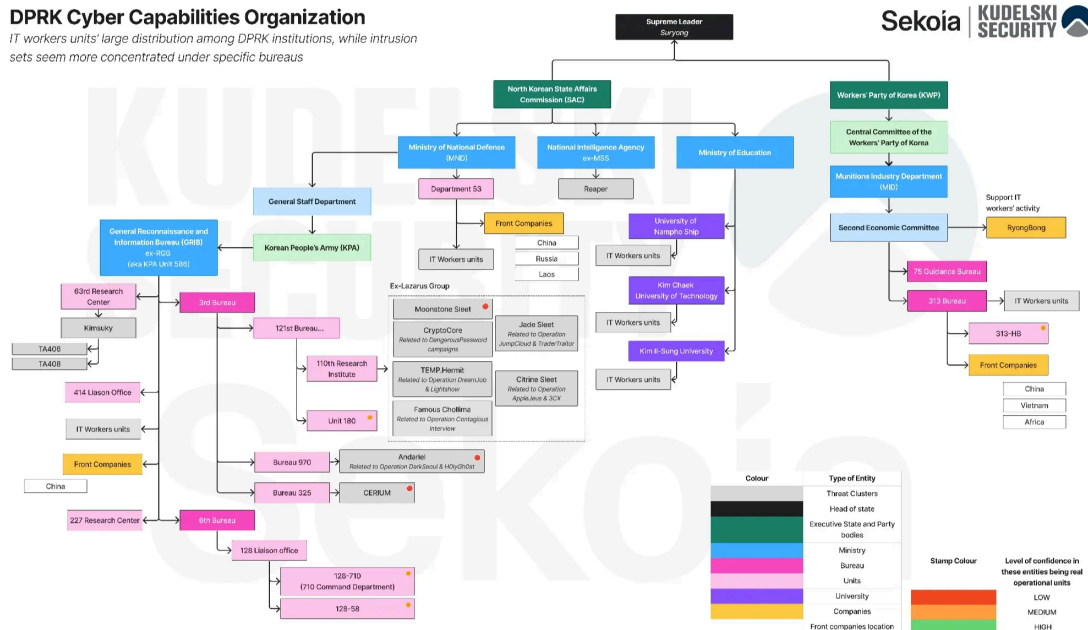
Second, the IT worker programme fits awkwardly within conventional threat intelligence frameworks. It works like a **criminal enterprise**: the units are dispersed across a heterogeneous range of host entities, with the end goal of making profit. They use cyber means, but also fake identities, fraud schemes and lures to channel foreign currencies to the regime.

Third, the distinction between espionage and revenue generation is less firm than it appears. Access acquired for financial purposes has been turned to collection, and the same infrastructure appears to serve both. On the other hand, intelligence units self-fund their operations, conducting lucrative campaigns at the margin.

Aliases proliferate, clusters are divided and consolidated differently across vendors. However, what endures is the understanding of how the DPRK operates. Indeed, the history of these clusters and following their successive reconfigurations, alongside their characteristic tradecraft and motivations can help defenders to better monitor and anticipate the threat posed by Pyongyang operators. This paper is intended to support that approach.

DPRK Cyber Capabilities Organization

IT workers units' large distribution among DPRK institutions, while intrusion sets seem more concentrated under specific bureaus



DPRK Cyber Capabilities Organization

Annexes

Annex 1 - North Korean university acronyms found on stealer logs and leaks

North Korean university's acronym or nickname	Meaning and affiliation	Confidence level of the meaning
HUCE	Hamhung Chemical Industry University <i>Contain a Fake IT worker cell</i>	HIGH
PUCR	Pyongyang University of computer science <i>Contain a Fake IT worker cell</i>	LOW
PUCS	Pyongyang University of computer science Information Exchange Company. <i>Contain a Fake IT worker cell</i>	HIGH
UOS	University of Science <i>Contain a Fake IT worker cell</i>	MEDIUM
Trans Univ	<i>Pyongyang University of Transport - Contain a Fake IT worker cell</i>	MEDIUM
KUT	Kim Chaek University of Technology <i>Contain a Fake IT worker cell</i>	HIGH
PUG	<i>Unknown - Likely contain an attack infrastructure</i>	<i>Unknown</i>
HUT	Huichon University of Telecommunications <i>Contain a Fake IT worker cell</i>	LOW
PAU	Pyongyang University of Automation <i>Contain a Fake IT worker cell</i>	MEDIUM
Univ JN	Jinung Institute of IT Development - Kim Il Sung university <i>Contain a Fake IT worker cell</i>	HIGH
Print University	Pyongyang University of Printing Engineering <i>Contain a Fake IT worker cell</i>	MEDIUM
Nampho Ship	University of Nampo ship <i>Contain a Fake IT worker cell</i>	HIGH
PYITC	Pyongyang Information Technology Center	MEDIUM

Annex 2 - Overlap between fake IT workers and DPRK offensive campaigns

Annex 2. Overlap between fake IT workers and DPRK offensive campaigns

IP exit node used by DPRK fake IT workers	Campaign and cluster source	Source
23[.]237[.]102[.]130 37[.]120[.]154[.]98 38[.]75[.]137[.]97 45[.]86[.]208[.]162 50[.]7[.]159[.]34 91[.]239[.]130[.]102 103[.]214[.]44[.]138 167[.]88[.]61[.]117 185[.]135[.]76[.]89 188[.]43[.]33[.]252 211[.]21[.]16[.]181	Contagious Interview (Recorded Future)	Recorded Future
45[.]86[.]208[.]162 70[.]32[.]3[.]15	Contagious Interview (SentinelOne)	SentinelOne
66[.]118[.]255[.]35	Bybit attack (Silent Push)	Silent Push

Source: <https://www.sekoia.com/blog/beyond-lazarus-organization-of-dprk-cyber-capabilities>