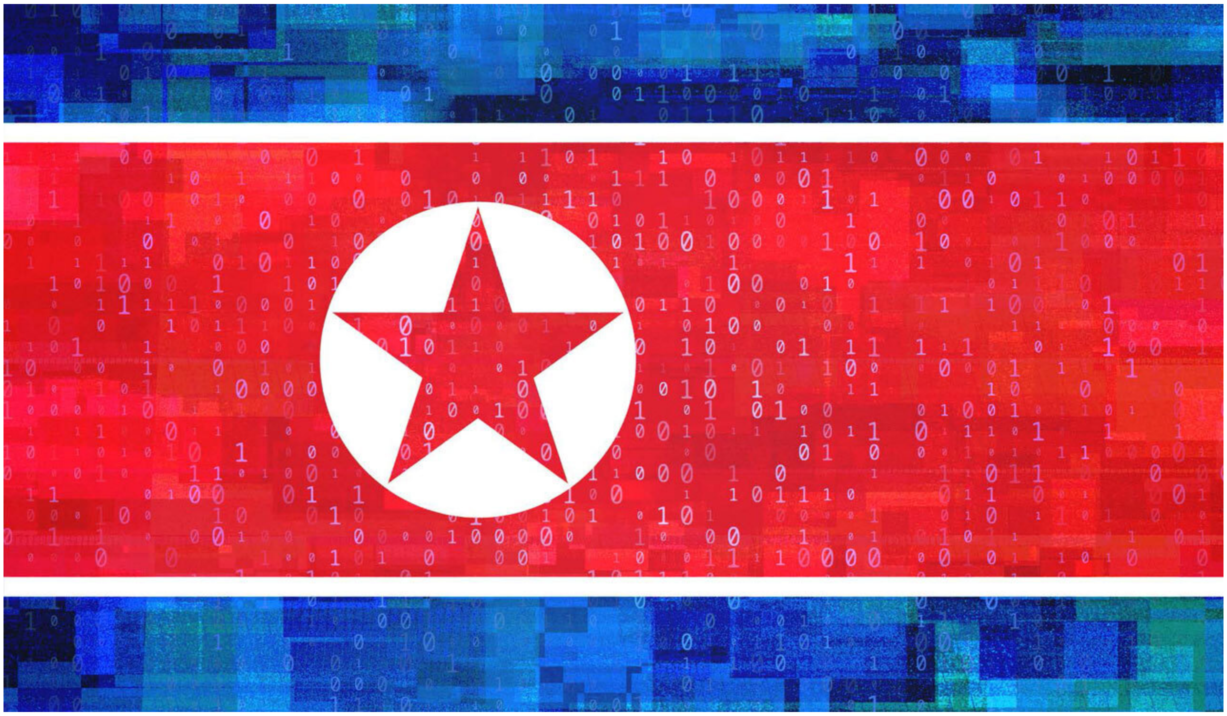
North Korea: Intelligence Assessment 2022

analyst1.com/digital-report/north-korea-2022-intelligence-assessment



Intro

At the end of the Second World War, the United States and Russia segregated Korea into two parts divided at the 38th parallel forming what is known today as North and South Korea. The division has caused political tensions and created an adversarial culture. While the citizens of both nations share a history and heritage, their political and cultural views are very different. Initially, the United States heavily influenced the development of South Korea and its government, whereas the Soviet Union impacted North Korea.

North Korea is under the control of Kim Jong-Un, a son of Kim Jong-Il, who is the direct descendant of Kim Il-Sung, a former Soviet Union military officer. Kim Jong-Un took control after his father died in 2011. However, Kim Jong-Un had a very different upbringing than his father. As a young adult, he spent several years outside North Korea studying Computer Science secretly at the International School of Bern, Switzerland. While attending, Kim lived under a secret identity, posing as a student named “Pak Chol,” and used the cover story he was the son of a driver assigned to escort diplomats stationed at the North Korean Embassy, also located in Bern, Switzerland.

Despite his exposure to the world outside of North Korea, Kim Jong-Un followed in his father’s footsteps and has continued to place military needs over that of the people of North Korea, who mostly live in poverty. Additionally, Kim eliminates anyone he considers a threat to his dictatorship, including his own family. Kim’s father was primarily concerned with building and strengthening his military through equipment and human capital. While Kim Jong-Un appears to consider military power his biggest strength, he has gone about building it differently. Kim realized the power of a cyber-army early into his dictatorship, likely influenced by his academic background, and began developing North Korea’s offensive cyber capabilities. Today, North Korea controls an advanced, sophisticated cyber army.

Purpose

Analyst1 produced this report to:

1. Assess the cyber threat presented by North Korea by combining open-source information, cyber threat data, and our own analysis
2. Detail recent changes and updates to North Korea’s military structure behind cyber attacks.
3. Associate security vendor cover names and malware with each corresponding military and government organization

Executive Findings

North Korea has been under pressure by the United States and the United Nations to denuclearize and terminate its nuclear weapons program. Sanctions against North Korea first began in 1950 when North Korea crossed the 38th parallel and invaded South Korea. Later, additional sanctions were put in place over North Korea's nuclear programs, which further restricted and isolated North Korea from the rest of the world. The economy of North Korea, or lack thereof, is a direct result of the sanctions in place. The economic pressure caused by sanctions intends to compel the North Korean government to cooperate.

Kim Jong-Un has lost faith in the previous leadership directing North Korea's cyber units, such as the RGB and its subordinate bureaus. The regime recently replaced older, more experienced leaders with younger, tech-savvy men. The regime selected these men from North Korea's top technical universities to strengthen its most successful military weapon: cyberwarfare.

Further, through support and alliances with China and Russia, North Korea has increased its military power and expanded its global influence through cyberwarfare. The sanctions and restrictions in place motivate North Korea to continue its attacks against the United States and its allies. As long as North Korea can survive economically, cyberattacks will continue.

> **Note:** This report is based on open-source information. Much of the material detailed in this paper originates from defector interviews, academic, government, and security vendor reporting available in the public domain. However, we found some of these sources contradict one another with the information that exists today. To address this problem, we assessed the information and its source to determine what information is the most accurate and relevant today. For example, we accessed information from a defector with firsthand knowledge to be more accurate than information presented in an academic or scholarly paper.

> Additionally, North Korea frequently updates its organizational structure and the mission of the units within. We believe we have put forth the most accurate information based on the available data; however, due to the nature of any open-source information, caution should be used to make actionable decisions for your organization. When in doubt, always conduct your own research and make your own assessment to ensure accuracy by leveraging public information, such as this report.

Structure & Organization

North Korea holds its military doctrine closely. Due to this, knowledge is sparse, and many information gaps exist regarding the mission and structure of North Korea's government and military compared to most nations today. Further, North Korea frequently updates both leadership and the mission of its directorates. Still, by combining information from many resources, we believe the following information depicts an accurate assessment of North Korea's cyber units and their supporting elements.

The following diagram is a visualization of North Korea's governing elements:

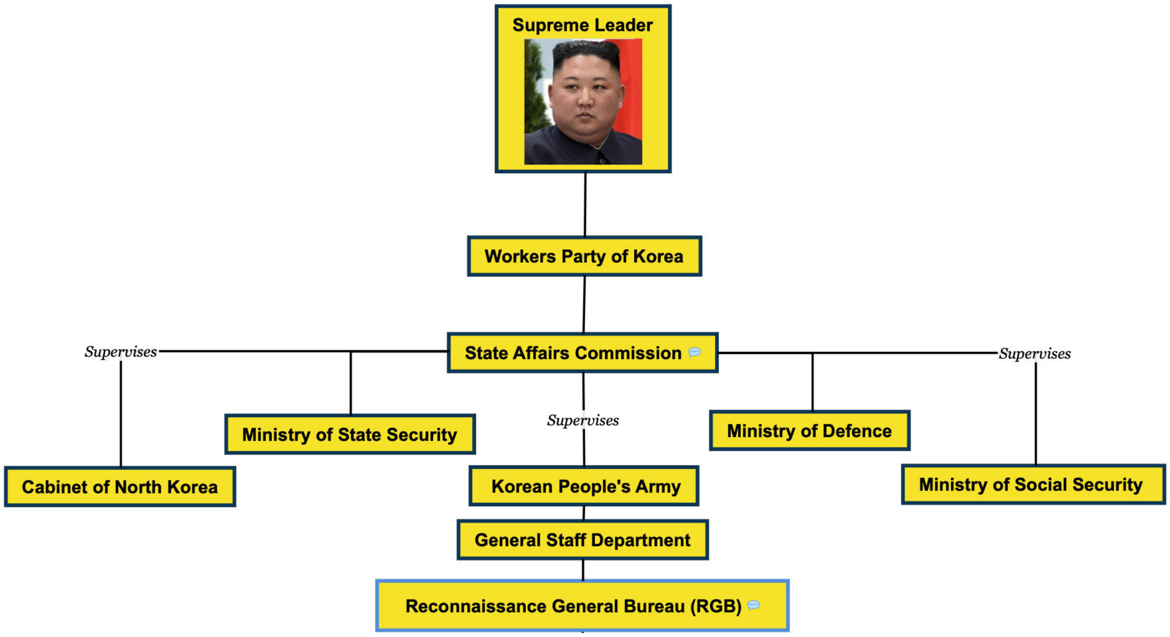


Figure 1: North Korean government structure

Much of the information we used to map out the governing organizations and their role is derived from North Korea's constitution, officially known as the "Socialist Constitution of the Democratic People's Republic of Korea." According to the document, North Korea's government conducts all activities under the leadership of the "**Workers' Party of Korea**" **(KWP)**, led by the Supreme Leader, **Kim Jong-Un**. Under the Workers' Party, the **State Affairs Commission** plays a supervisory role over multiple bureaus, each of which has its own purpose and mission. While not all of these state bodies will have a cyber function, understanding each will provide a greater context in the "big picture" operations of how cyber is used and benefits the rest of North Korea's governing body. Next, we will briefly describe each of these organizations and their purpose.

- **Cabinet of North Korea** (aka "The Cabinet") – The "administrative and executive body of State power and an organ of overall State administration."

- **Ministry of State Security** – The Ministry of State Security (MSS) is responsible for counterintelligence services and reports directly to the supreme leader. The state security body also operates secret police actions/operations and facilitates the administration of concentration camps within North Korea. According to the “Human Rights Council,” North Korea is responsible for human rights violations. The report claims the Ministry of State Security is responsible for conducting violations, including “torture, executions, enforced disappearance and political prison camps.”
- **Ministry of Defence** (aka “Ministry of the People’s Armed Forces”) – Responsible for “allocating material and human resources, administration, and diplomacy with foreign militaries and defense ministries.” It also provides food, medical, and structural management of North Korea’s military facilities.
- **Ministry of Social Security** (aka “People’s Security Department”) – The Ministry of Social Security is the organization tasked to secure and police North Korea’s government facilities, borders, and coastline. However, its most significant role is to monitor its own citizens using “local informers” to spy within village and town social communities across North Korea. When the Ministry identifies citizens or groups conspiring against the regime, it takes action to silence and eradicate the individuals. In some cases, if considered a political threat, the Ministry of Social Security will hand over offenders to the Ministry of State Security, who, as stated earlier, is known to torture and kill North Korean citizens.
- **Korean People’s Army** (KPA) – As the name states, this is the governing body of North Korea’s military. The KPA is broken out into five elements: Ground Force, Naval Force, Air Force, Strategic Rocket Force, and the Special Operations Force. Despite the term “Army” in its name, the KPA is North Korea’s armed forces, which encompass all of its military branches.
- **General Staff Department** – North Korea’s General Staff Department (GSD) oversees all subordinate organizations within the (North) Korean People’s Army (KPA). The GSD provides direction and manages the service branches, including those responsible for cyberwarfare and cyber theft operations. The GSD provides leadership, dictates strategy, and sets the objectives for each subordinate directorate/Bureau/Office. The most notable of these organizations is the Reconnaissance General Bureau (RGB).

Reconnaissance General Bureau

Formerly known as Unit 586, the RGB is North Korea’s premier military intelligence agency located in Pyongyang, North Korea. In 2009, North Korean leadership created the RGB by merging the Operations Bureau, Office 35, and the Reconnaissance bureau into one central entity as part of a massive restructure. The RGB conducts cyberwarfare operations and employs nearly 7,000 trained hackers for espionage and financial theft operations. The RGB structure includes several cyberwarfare units, as shown in Figure 2 below.

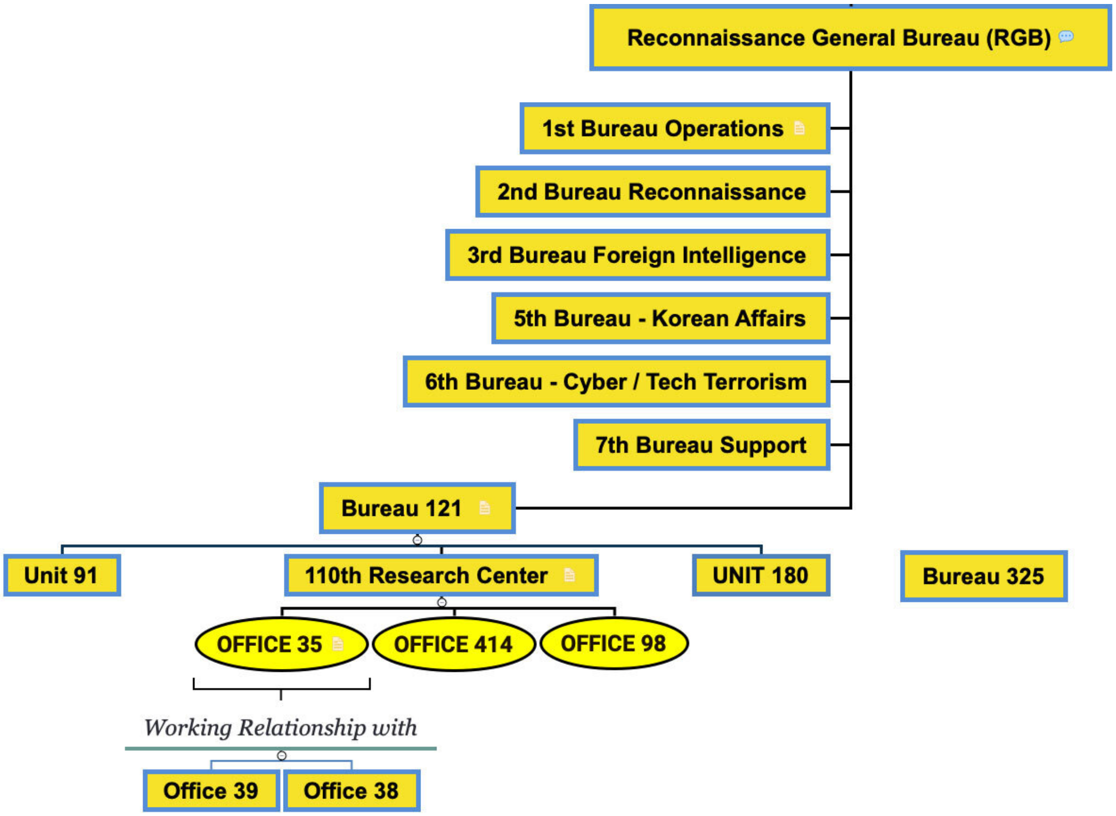

Reconnaissance General Bureau (RGB)
1st Bureau Operations
2nd Bureau Reconnaissance
3rd Bureau Foreign Intelligence
5th Bureau - Korean Affairs
6th Bureau - Cyber / Tech Terrorism
7th Bureau Support
Bureau 121
Unit 91
110th Research Center
UNIT 180
Bureau 325
OFFICE 35
OFFICE 414
OFFICE 98
Working Relationship with
Office 39
Office 38

Figure 2: Reconnaissance General Bureau unit structure

In mid-2020, North Korea appointed new leadership to the RGB as part of a personnel overhaul designed to strengthen "the Workers' Party's chain of command over the RGB." New personnel placed into key RGB leadership roles are younger, more technically skilled men in their "early to mid-30s." Many are "Information Technology experts" who graduated from North Korea's top technical universities, such as "Kim Il-Sung University, Kim Chaek University of Technology, and Mirim University (Command Automation University)." The previous leaders *volunteered* to move into less relevant, obsolete roles, such as managing equipment and supply distribution units. Under new leadership, North Korea hopes to increase its ability to use its cyber assets to steal intelligence and foreign currency.

Time will tell if youth and technology will further empower the RGB. However, the recent personnel shuffle is not due to the RGB's lack of success or technical ability. Next, we will discuss the subordinate units that make up the RGB and their mission.

Unit 121

Unit 121, also known as the **Cyber Warfare Guidance Unit**, is the elite cyber unit of the RGB. Unit 121 oversees several other military units, including Unit 180, Unit 91, Lab 110, and its subordinate organizations. Unit 121 conducts cyberattacks to sabotage, deny service, and steal information from foreign nations. However, around 2015, Unit 121 revised its goals, narrowing its operational scope to focus specifically on hacking campaigns designed to disrupt adversarial nations' critical infrastructure such as gas, power, transportation, aviation, etc., in addition to traditional cyber espionage. Many of its members are selected from the Pyongyang University of Automation and receive privileged treatment such as housing, food, and higher salaries for themselves and their family members.

As strange as it may sound, while its headquarters is located in Pyongyang, North Korea, service members from Unit 121 train and operate out of the basement of a restaurant attached to the Chilbosan Hotel, a hotel in Shenyang, China. The hotel houses North Korean hackers who train and use it to cover for their cyber operations. The hotel is a joint venture between the two nations. In addition to room service, the Chilbosan hotel provides North Korea's Unit 121 with the training they cannot obtain in their own country. This is how Unit 121 service members learn new hacking skills/techniques and conduct cyberwarfare operations.

Members of the Unit traveled to China in small teams, posing as businessmen using fake names and titles as cover. In the early 2000s, before North Korea had in-country internet access, the hotel provided the regime with servers and network connectivity. Based on this and the continued cooperation with China, the two countries will likely continue to work collectively to target the United States and its allies. It is also worth noting that the relationship between North Korea and the hotel became public knowledge in 2015. Due to this, we do not know if operations at the hotel will continue. If not, it is highly likely that Unit 121 simply changed locations within China. Since the two nations have a strong relationship today, it is unlikely the joint program would cease operation.

Unit 91

Unit 91, also called Office 91, is located in the Mangkyungdae-district of Pyongyang, NK, and "serves as the headquarters for hacking operations." As part of its "headquarters" designator, Unit 91 supplies equipment and mission-essential resources to Lab 110 and its subordinate units. However, procurement is a problem for North Korea since sanctions prevent international trade, including importing and exporting goods. Nevertheless, this has not stopped North Korea from obtaining mission-essential equipment necessary to facilitate its cyber operations through Russia and China.

> Unit 91 serves as the headquarters for hacking operations

For example, Unit 91 illegally conducts business with foreign suppliers to evade sanctions. Since suppliers cannot legally sell their products to North Korea, Unit 91 establishes shell companies in China, Malaysia, and Russia to purchase essential equipment needed to support its cyberwarfare mission. Additionally, Unit 91 conducts black market purchases to supplement their needs further.

In addition to acting as a headquarters element, Unit 91 also plays a significant operational role in supporting the RGB. Specifically, Unit 91 also conducts cyber espionage campaigns intended to steal technologies used to develop nuclear weapons. Previously, the unit conducted cyberattacks against hydro and nuclear power organizations in South Korea.

Lab 110

Lab 110 is also known as the "**110th Research Center**" and the "**Technology Reconnaissance Team**" and is another arm of North Korea's cyberwarfare program. Lab 110 is responsible for sabotage attacks involving destructive wiper malware, denial of service attacks against media and financial institutions across South Korea. Additionally, Lab 110 previously conducted financial attacks against banks globally. One of the most notable attacks was the DarkSeoul campaign, which destroyed thousands of financial systems in 2013 and resulted in outages at the top three television/media companies in South Korea. Lab 110 also conducted several high-profile attacks against the Republic of Korea (ROK) (aka South Korean Army) and stole "confidential defence strategy plans" detailing response and defense to North Korean attacks. Lab 110 infiltrated the ROK Third Army headquarters operational network in a later operation and stole chemical defense/response-related documents.

> Lab 110 is responsible for sabotage attacks involving wiper malware, DDoS attacks.

According to the US government, Lab 110 is also behind financial attacks designed to compromise the SWIFT messaging system. SWIFT facilitates financial transaction messages, such as approval and denial for pending transactions. The attacker would infiltrate institutions and maintain a presence for as long a year to observe and learn the bank's processes and systems related to financial transactions. Then, Lab 110 would use custom malware to compromise the institution's local instance of SWIFT and approve fraudulent transaction requests.

The most notable of these attacks took place against the Bank of Bangladesh in 2016. In that attack, Lab 110 hackers made a spelling error in the fraudulent transaction request, resulting in its discovery. Still, attackers initially made off with $81 million of the bank's money, though it later recovered some of the funds in transit before reaching its final destination.

In addition to these attacks, Lab 110 is also responsible for finding zero-day vulnerabilities and developing malware used in operations by other units within the RGB. While based in Pyongyang, Lab 110 facilitates some of its operations through shell companies located in China and Russia designed to allow its personnel to work outside North Korea to provide cover for their operation.

Understand that, unlike most RGB directorates, Lab 110 appears to have more than one motivation (sabotage, financial gain, espionage, etc.). This is because Lab 110 has three of its own subordinate units: **Office 98**, **Office 414**, and **Office 35**. These units support and execute some of the operations attributed to Lab 110. The attribution is not wrong; however, it can be misleading if the reporting units and their missions are not understood. Luckily, we will discuss these subordinate units next.

Office 414 & Liaison Office 128

Before developing a strong cyberwarfare capability, North Korea obtained most of its intelligence from human sources. At that time, North Korea would send spies to live within the target nation, using false identities to collect or steal information and report back to the regime. Today, the regime relies heavily on cyber espionage to provide its intelligence-gathering capability. As a subordinate directorate to Lab 110, **Office 414**'s role is to provide "information on overseas government agencies, public agencies, and private companies." To accomplish this, Office 414 develops espionage networks and programs to support the RGB mission.

Additionally, Office 414 works directly with another North Korean military organization named the **Liaison Office 128,** which uses hacking resources to compromise foreign intelligence services. It's also worth noting there is an information gap as to the extent Office 414 and Liaison Office 128 play. Historically, in North Korea, Liaison offices focus more on counterintelligence and develop and maintain covert communication with other North Korean units. This, however, does not fit with the information available surrounding the Liaison office. Instead, both Office 414 and Liaison Office 128 appear to have a larger offensive mission within the RGB.

Office 98

Defectors have provided valuable information on the North Korean regime and its military and government structure. For example, much of the information regarding North Korea's cyber programs we know today originates from Professor Kim Heung-Kwang, a former North Korean university professor. This information allows outside nations to better understand North Korea and its operations. Due to this, North Korea created **Office 98**, which is responsible for collecting information, accessing, and monitoring North Korean defectors, including the foreign organizations/agencies that assist them. Office 98 relies on conducting cyber espionage operations similar to other Units under the RGB; however, they are focused specifically on defector-associated targets.

Third Floor Offices

Three Offices/Units share the third floor of the KWP Central Committee Office Complex building in Pyongyang, known as the “Third Floor Offices.” Strangely, at their inception, these units had no official name. Instead, each was referred to by the room number from which it operated (Room 35, 38, and 39). Over time, Third Floor Offices officially adapted their room number as their military unit/office designator. Today, the units do not report to the same directorates within the regime but play a role in funding the regime’s military/government programs and the Kim family itself. For years, the Offices worked together until 2009, when the first of several restructures took place. Next, we discuss each Office and its role.

Office 35

Office 35, the External Investigations and Intelligence Department, is responsible for intelligence collection and analysis. However, unlike other components of the RGB, Office 35 collects information to produce internal briefings and reports to inform and advise senior leadership within the regime. Its mission focuses primarily on the ROK, United States, Japan, and several nations across Europe. Based on the information provided by a North Korean defector, Office 35 empowers a small but sophisticated and effective hacking group that develops malware and hack tools to acquire information on its targets used to build its intelligence reports. Beyond information gained from hacking campaigns, Office 35 also collects information from human and open-source means to produce its reports.

> Office 35 collects information to produce internal documents to inform and advise senior leadership within the regime

While not as prevalent, Office 35 also conducts operations motivated by financial gain. However, these attacks make up a small percentage of the activity seen by Office 35. We believe this may be a secondary mission for Office 35 to generate profit to support and fund the tools and resources used in their primary mission.

Office 38

The mission of **Office 38 is to manage the Kim family finances**. Office 38 operates holding companies involved in both legitimate and illegitimate business throughout Asia to accomplish this. The holding companies allow the regime to acquire goods banned under current sanctions, such as cars, boats, and entertainment devices (TVs, stereos, tablets, furniture, alcohol, etc.). The funds and goods go directly to the Kim family to furnish homes and provide luxury otherwise absent in North Korea. Some of the funds managed by Office 38 also go to high-ranking North Korean military/government members to show gratitude and award leadership. The gifts and lifestyle provided from funds managed by Office 38 help ensure their loyalty to the Kim family.

Office 39

Established in 1974, **Office 39 is responsible for laundering stolen money** obtained by other offices within the regime. Office 39 works closely with Offices 35 and 38. Much of the funds laundered by Office 39 originate from cyber theft, fraud, and the production and sale of illegal drugs, weapons, counterfeit currency, and other black-market goods. Office 39 also orchestrates the operational structure and movement of money, much of which is secretly laundered and dispersed through various financial resources and organizations globally. For example, Office 39 decides how to covertly move goods into and out of North Korea necessary to launder money, ensuring it evades detection from foreign nations adhering to the restrictions and sanctions in place.

To do this, Office 39 relies on its military vessels or transportation from ally nations such as Russia and China. Additionally, it organizes state-run companies and criminal enterprises to ensure the success of its operation. Finally, Office 39 implements the financial distribution of funds based on budgeting decisions from North Korean leadership once successful laundering takes place. As of 2019, Office 39 managed and laundered around $1 billion per year in stolen funds.

Unit 180

Simply put, **Unit 180 is the primary bureau responsible for stealing money**. The organization conducts cyber operations, targeting foreign financial institutions. North Korea uses the revenue from Unit 180 campaigns to fund North Korean military operations, including nuclear weaponization. Like other RGB components, Unit 180 utilizes graduates from its technical universities to populate its ranks, who often operate outside the North Korean border to circumvent its limited internet resources. For example, in one operation named FASTCash by the US government, Unit 180 compromised ATMs across Asia and Africa to fraudulently steal money from bank ATMs.

Many targeted banks used vulnerable AIX-based servers that Unit 180 exploited to introduce malware that fraudulently approved transactions between the legitimate SWIFT-based payment switch and the ATM. In addition to conducting the cyberattack itself, someone needed to physically access the ATM to acquire the cash funds. Then, North Korea launders the stolen funds through an extensive money mule network once collected. This is just one example of operations conducted by Unit 180 but provides insight into the advanced planning and execution of their attacks.

> **Note:** Because Unit 180 is the primary unit responsible for stealing money, we did not feel Lab 110's attribution to the Bank of Bangladesh attack fit well based on unit missions. However, since the information originated from the United States government, with far more attribution resources than us or any security vendor, we left the attack under Lab 110. It is also possible the SWIFT-based attacks against banks previously fell under Lab 110 and shifted over time to Unit 180. However, without additional evidence to support Lab 110 attributions, we feel both Units should be accessed when evaluating bank attacks geared at compromising SWIFT messaging.

Unlike similar RGB organizations, not all Unit 180 recruits conduct hacking operations. For example, in Dandong, China, Unit 180 sends teams of men to perform legitimate work, such as website and mobile app design, game development, and similar software-based services to generate profit for the regime. Regardless of their function, even legitimate work that financially benefits North Korea is illegal due to sanctions. For this reason, similar to Unit 121, members of Unit 180 must travel to areas of partnering nations, like China, Malaysia, and Russia, covertly.

> **Note:** The relationship between North Korea and Malaysia began to deteriorate in 2017 due to several high-profile incidents resulting in the closing of embassies in both Malaysia and North Korea. Malaysia made attempts to mend the relationship in 2020. However, the effort eventually failed due to a political crisis leading to a change in party leadership within Malaysia. Due to this, it seems unlikely North Korea still uses Malaysia as a cover for its cyber programs.

Unit 204

Unit 204, also known as the “Enemy Secret Department Cyber Psychological Warfare,” is comprised of nearly 100 trained cyber hackers. As their name indicates, this unit conducts “cyber-psychological warfare.” Information on this unit is sparse, but according to previous defector reports, the unit stands up “pro-North websites,” which spread propaganda about South Korea and the United States while reinforcing North Korean views. It is likely the unit also relies on social media to conduct its mission.

Bureau 325

On January 3, 2021, North Korea activated Bureau 325, a new organization within its cyber ranks. The new Bureau has a distinct mission from its peer cyber Units. Bureau 325’s only mission is to steal COVID-19 vaccine research and data. The creation and operation of the unit demonstrate how important COVID research is to the regime. Further, unlike all other cyber units that fall under the RGB, Bureau 325 reports directly to Kim Jong-Un.

> Bureau 325s only mission is to steal Covid-19 vaccine research and data.

Bureau 325’s role in the effort is to use cyber means to infiltrate government, pharmaceutical, and medical organizations to steal vaccine data. Once acquired, the North Korean Ministry of Public Health uses the data to create vaccines and medications. If successful, the measure allows North Korea to bypass the time and capital necessary to develop and test vaccines. Additionally, North Korea would no longer need to rely on China to provide them with vaccines and medications related to COVID.

Further, Kim Jong-Un’s sister, Kim Yo-Jong, oversees the regime’s non-cyber efforts from North Korea’s medical science and health-related organizations and updates the “supreme leader.” According to Daily NK, a news/media outlet focused on North Korea, “the (North Korean) Central Committee recently ordered the Ministry of Public Health and Ministry of Foreign Affairs to focus all their abilities on securing vaccines, even if that means putting aside other activities.”

Time will tell if Bureau 325 is successful. We also don’t know if Bureau 325 relies on tools, malware, and experienced personnel from existing units to accomplish its mission or if it develops and uses standalone cyber espionage resources. Based on the priority and oversight of Bureau 325, we believe top hackers and resources will transfer from other Bureaus/Units within the RGB to bring it up to speed and make it operationally effective as quickly as possible.

Foreign Support

China

China and North Korea have a long-standing relationship. Despite sanctions, China provides North Korea with many resources, such as energy, fuel, food, and consumer goods. More importantly, China supplies North Korea with one of the two fiber optic lines that the regime relies on to connect to the global internet, in addition to technology hardware and other cyber resources. China also provides North Korea's state-run telecommunication company with the IP address range it depends on to traverse the internet.

As described earlier, China also provides North Korea's cyber units within the RGB with training, technology, infrastructure, and cover for their cyber espionage and financial theft operations. A relationship with China is vital to North Korea. China shares a border with North Korea and is one of the regime's few allies willing to trade and enable North Korea's cyberwarfare program. Further, Huawei, a China-based technology and telecommunications company widely accused of enabling surveillance for the Chinese government, helped North Korea develop its first commercial wireless communications network. Later, China assisted the regime in developing its own cell phone called the "Kimtongmu," though other media outlets claim China secretly manufactured the phones for North Korea. The development of a wireless communications network in conjunction with North Korean-branded cell phones helps the regime stay relevant in today's evolving tech world. By controlling both the country's network and cell phones, North Korea can also control which citizens can obtain access to them.

Russia

Russia provides North Korea with its second point of internet access. The access eliminates the risk of having a single point of failure and dependency on China. The resource is significant since China could completely control the regime's access to the rest of the digital world without it. Russia also provides North Korea with military technology and weapons such as unmanned aerial vehicles (UAVs) and various missile-related technologies. For example, North Korea relies on Russia's satellite navigation system to launch and control the orbit of ballistic missiles. Without it, the regime would have to rely on US GPS technology and networks, allowing the US government to hinder or even sabotage the regime's program.

Further, Russia and North Korea have discussed jointly building a gas pipeline through North Korea. Russia could leverage the pipeline to generate billions in profit by supplying gas to South Korea. Additionally, in 2015, Russia and the regime discussed building an electrical grid through North Korea. While North Korea would share profit from both endeavors, it is doubtful South Korea would ever welcome the resources due to its long-standing conflict with the north. This is likely why neither effort came to fruition.

Technologies

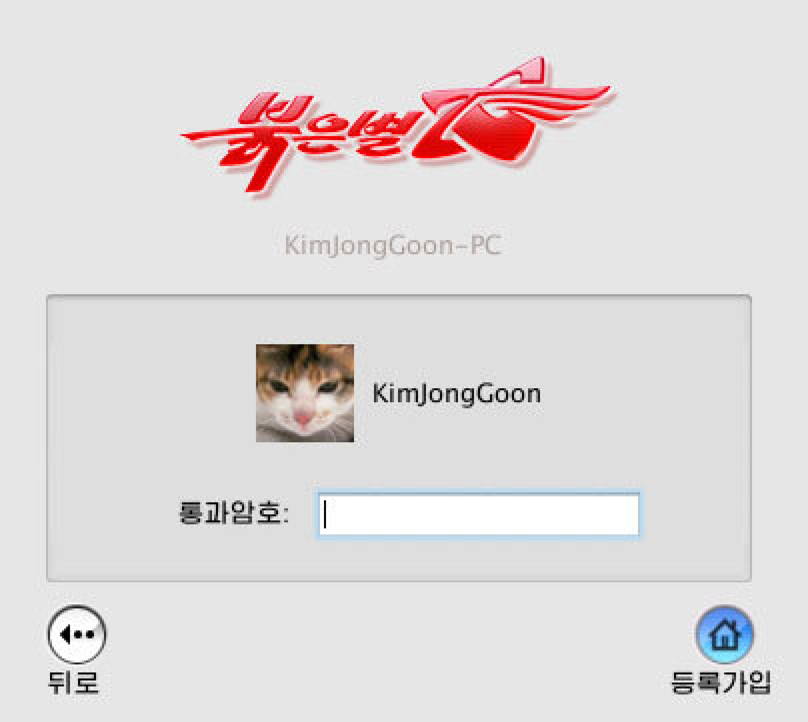
In addition to North Korean cell phones, the regime also has its own operating system used by the government and military, called Red Star OS.

Operating System

Red Star OS (aka Pulgunbyol) is the operating system created by the North Korean technology research center, the Korea Computer Center (KCC). The KCC created version 1 in 2008 and incrementally updated it through version 4, which they began using in January 2019. Red Star OS is based on Linux, though the first versions visually mimicked Windows XP, and later versions looked similar to Apple's OSX operating system.

The KCC also created a custom browser to traverse the internet called **Naenara**, built on open-source Firefox code. The browser comes configured to use "**Sam heug,**" North Korea's search engine developed using Chromium open-source code. By using their own intranet, operating system, and search engine, North Korea adds several layers of security between their data and the rest of the world. This provides additional safeguards to help keep out foreign intelligence agencies; however, it also limits North Korea's access to resources the global internet provides.

Analyst1 obtained a copy of Red Star OS to explore while conducting research for this report. The Figures below display the Red Star OS login page, desktop, and the Naenara browser:

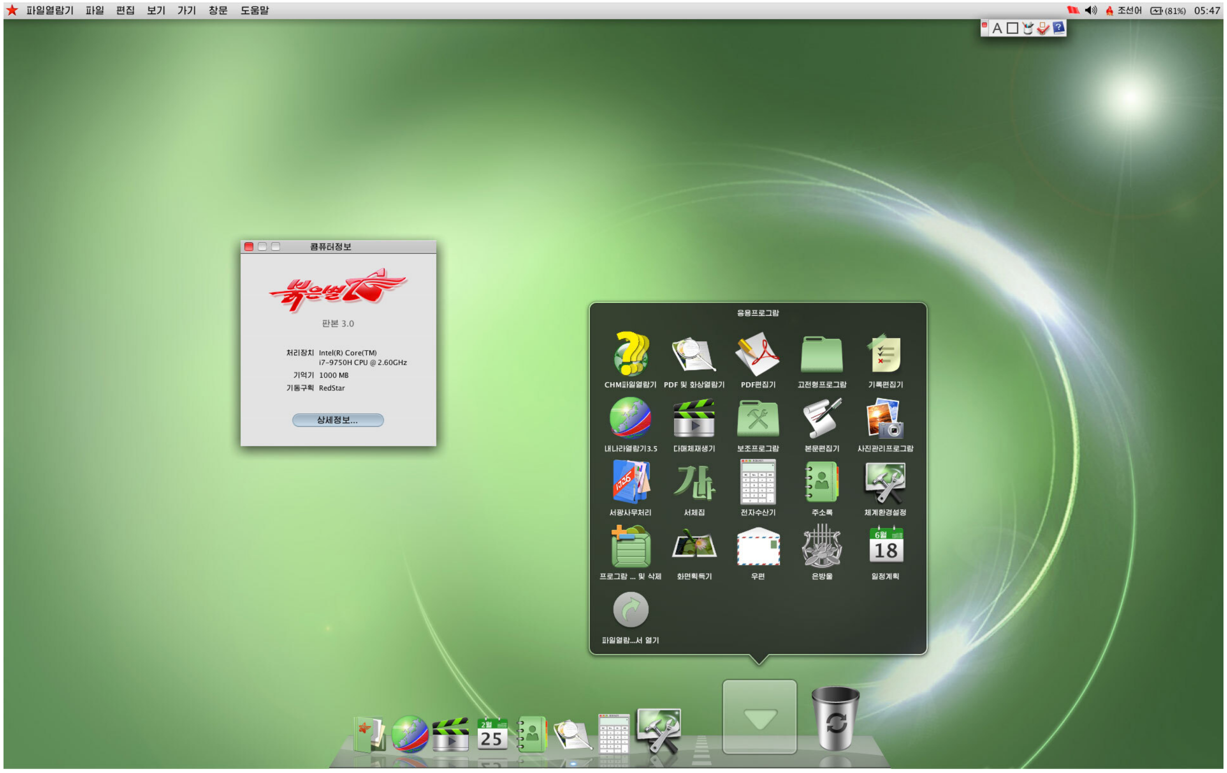


KimJongGoon-PC

KimJongGoon

통과암호:

Figure 3: Red Star OS login screen

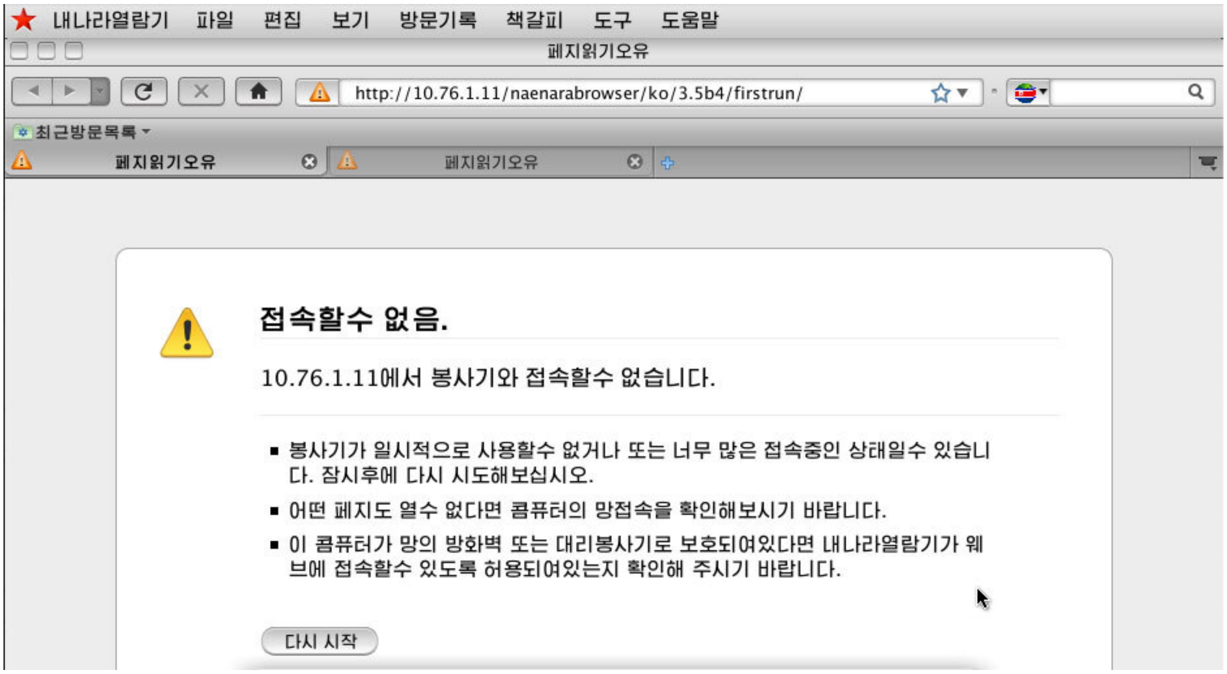


콤퓨터정보

판본 3.0

처리장치 Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz
기억기 1000 MB
기동구획 RedStar

Figure 4: Red Star OS desktop



접속할수 없음.

10.76.1.11에서 봉사기와 접속할수 없습니다.

- 봉사기가 일시적으로 사용할수 없거나 또는 너무 많은 접속중인 상태일수 있습니다. 잠시후에 다시 시도해보십시오.
- 어떤 페지도 열수 없다면 콤퓨터의 망접속을 확인해보시기 바랍니다.
- 이 콤퓨터가 망의 방화벽 또는 대리봉사기로 보호되여있다면 내나라열람기가 웨브에 접속할수 있도록 허용되여있는지 확인해 주시기 바랍니다.

Figure 5: Naenara web browser configured to use 10.76.1.11, which is the address used to host North Korea’s search engine

Internet

Internet access is limited in North Korea and only available for official government/military business and a select demographic of high-level leadership officials. Due to limited internet access, North Korea created its own intranet, known as “Kwangmyong,” which, with a few exceptions, is disconnected from the global internet. North Korea’s intranet allows the regime to use private state-controlled websites and resources available within the country itself. This may sound limited, which it is, but using an intranet network allows the regime to share resources and control the content available within North Korea. The Kwangmyong intranet also makes it difficult for foreign adversaries to access or disrupt its connectivity since it does not rely on outside internet access.

Beyond the Kwangmyong intranet, North Korea utilizes three other IP address ranges to allow their infrastructure to access the global internet. Table 1 shows each range and its details.

Source	Range	Note	Registration/WHOIS record

Kwangmyong (intranet)	10.0.0.0/8	Private address range used across the regime’s intranet	N/A – Non-routable IP address range reserved for private networks
“.kp” assigned infrastructure	175.45.176.0/22	Used mainly for publicly accessible North Korean websites	inetnum: 175.45.176.0 - 175.45.179.255 netname: STAR-KP irt: IRT-STAR-KP address: Ryugyong-dong Potong-gang District e-mail: postmaster@star-co.net.kp abuse-mailbox: postmaster@star-co.net.kp admin-c: SJVC1-AP tech-c: SJVC1-AP auth: # Filtered mnt-by: MAINT-STAR-KP last-modified: 2014-12-02T01:23:29Z source: APNIC
Russia	77.94.35.0/24	North Korea uses this address range more than any other allocated range since 2017	inetnum: 77.94.35.0 - 77.94.35.255 netname: SATGATE-LEBANON person: Alexander N Mashchenko address: M. Pocobuto g. 23, address: Liepiskes, Vilnius address: LT phone: +370 (5) 2101250 e-mail: tekill@satgate.net

China	210.52.109.0/24	Address range primarily used before switching to the Russian-associated range	inetnum: 210.52.109.0 - 210.52.109.255 netname: KPTC country: CN person: TECH GROUP CNC nic-hdl: TC254-AP address: 9/F, Building A, Corporate Square, No. 35 Financial Street, address: Xicheng District, Beijing 100032, P.R.China country: CN

Table 1: North Korean network and internet information

Shell Companies

We mentioned North Korea uses shell companies to mask operations used to facilitate its cyberwarfare capabilities. Below, you will find the names of the shell companies identified while conducting research for this report. North Korea used the following organizations to conduct illegal business in an effort to circumvent sanctions in place against the regime:

- Chosun Expo Joint Venture
- May 18th Trading Company
- Maebong General Trading Corporation
- Unha General Trading Corporation
- Samcholri General Trading Corporation
- Unpyol General Trading Corporation
- Kumnung General Trading Corporations
- Celas Trade Pro
- Yang Ban Corporation
- Mingzheng International Trading Ltd.

Group Mappings

Security vendors use cover names to attribute TTPs, malware, and attack campaigns with specific threat actors. At the start of this project, one of our initial goals was to identify the cyber units within North Korea and map each vendor’s name to a specific office or bureau.

Doing so would be helpful since *most* vendors either do not map actual North Korean organizations to attack groups or attribute all activity to North Korea. At best, we see vendors attribute to the RGB or Unit 121. While not incorrect, the RGB and Unit 121 are umbrella organizations with several subordinate units supporting their mission, making specific attribution less accurate. In another example, security vendors mapped *all* North Korean activity to the Lazarus group for many years. Fortunately, this is evolving, and security vendors like FireEye, CrowdStrike, and several others have begun mapping to "Lazarus subgroups." Still, we are far from a one-to-one mapping for North Korea's military cyberattack groups.

Due to this, as we attempted to identify each cyber unit/office/bureau and its role within the North Korean regime, a lot of the attributed activity included attack attributes spread across multiple subordinate groups within the RGB and Unit 121. For that reason, we are not mapping out the groups to vendor names as it would cause more confusion than clarity.

Conclusion

Due to many years of strict sanctions, North Korea is one of the poorest countries in the world. While much of the population is starving, its government created one of the most successful and dangerous cyber armies that exist today. The regime mastered turning something out of nothing and continues to defeat sanctions and come closer to becoming a global nuclear power. This is a massive accomplishment for a country with two physical connections to the internet. Further, prior to 2014, many of us in the cybersecurity community incorrectly assessed the accurate threat level North Korea presented.

While the US defense community has tracked and defended against North Korea heavily since at least 2009, it took the decimation of Sony Pictures Entertainment in 2014 to get the attention of corporate America. However, if the Sony attacks were not enough, the 2017 WannaCry attacks certainly put the regime on the radar of most organizations globally. Today, outside of Sony and WannaCry, North Korea is most known for conducting financial attacks.

Analyst1 assesses that North Korea will continue to conduct financial attacks and focus its resources heavily on cryptocurrency theft. While North Korea has an elaborate portfolio of SWIFT-based bank and ATM attacks, recent attack campaigns show the regime's growing interest in cryptocurrency. Further, cryptocurrency is more difficult to track and easier to launder, making it more attractive to steal than traditional currency. The regime will continue to use the stolen proceeds to supplement the economic loss due to sanctions and fund its nuclear weapons program.

Last, while we believe financial attacks are the primary motivator of North Korea, **espionage efforts**, especially toward health and COVID-related targets, **will not only continue but likely increase**. Today, North Korea does not have the resources or know-how to research or develop advanced medication on its own. For this reason, it is highly likely that COVID research will continue to be a major priority for the regime. North Korea will continue to dedicate resources and money to cyber operations designed to steal COVID-related research and data.