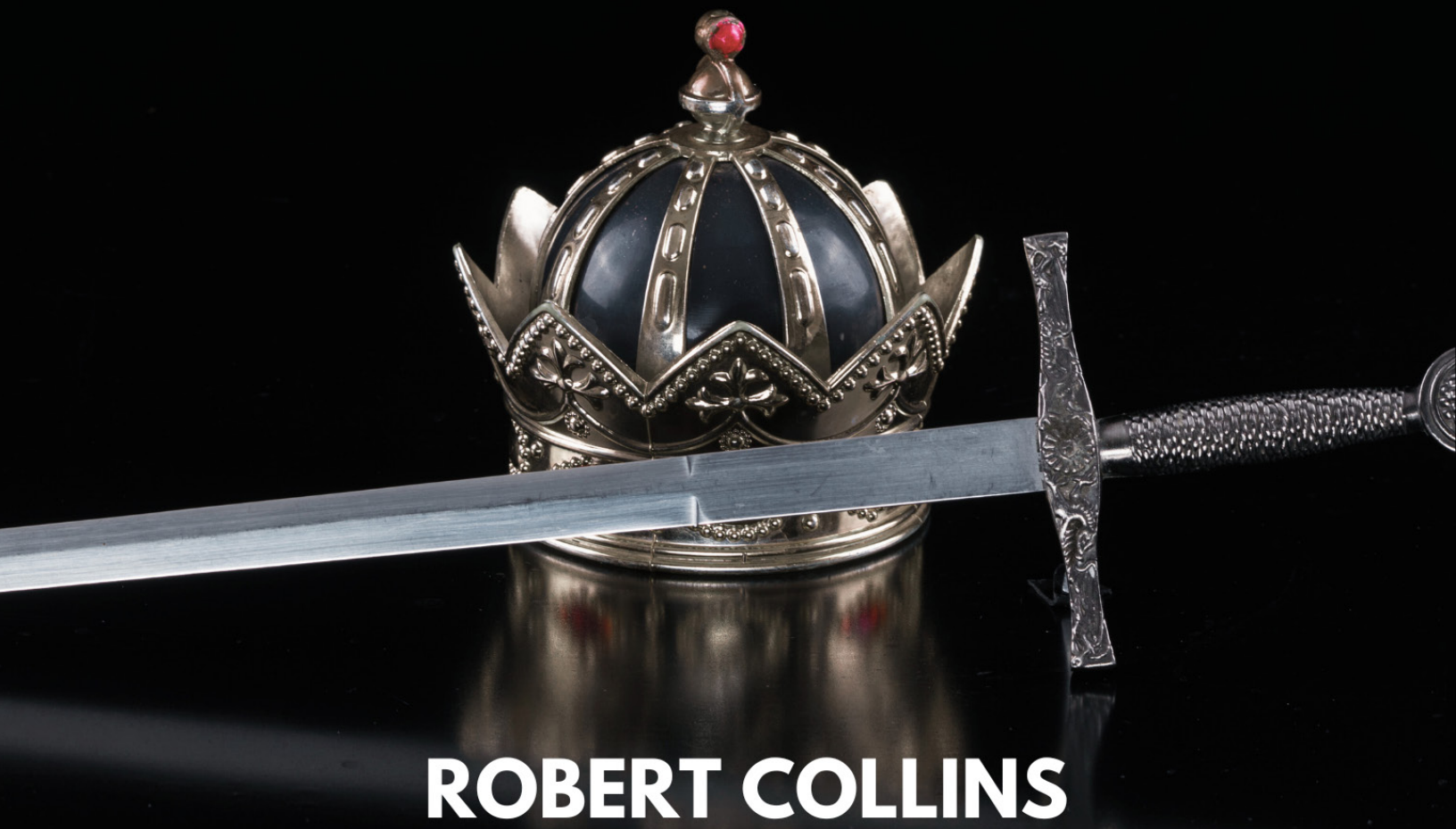
THE RECONNAISSANCE GENERAL BUREAU

The Kim Regime's "Precious Treasured Sword"



ROBERT COLLINS

The Committee for Human Rights in North Korea
북한인권위원회

The Reconnaissance General Bureau

The Kim Regime's "Precious Treasured Sword"

The Committee for Human Rights in North Korea

Robert Collins

"Any catastrophic day begins like any other day."

Lieutenant General (Retired) Chun In-bum

Committee for Human Rights in North Korea

Printed in the United States of America

Committee for Human Rights in North Korea

1801 F Street NW, Suite 305

Washington, DC 20006

P: (202) 499-7970

www.hrnk.org

ISBN: 978-1-959391-06-7

e-ISBN: 978-1-959391-05-0

Library of Congress Control Number: 9781959391067

Cover Images: Canva

Table of Contents

About The Committee For Human Rights in North Korea

The Committee for Human Rights in North Korea (HRNK) is the leading U.S.-based nonpartisan, non-governmental organization (NGO) in the field of North Korean human rights research and advocacy, tasked to focus international attention on human rights abuses in that country. It is HRNK's mission to persistently remind policymakers, opinion leaders, and the public that more than 20 million North Koreans need our attention.

Since its establishment in October 2001, HRNK has played an important intellectual leadership role in North Korean human rights issues by publishing over 60 major reports (available at https://www.hrnk.org/ publications/hrnk-publications.php). Recent reports have addressed North Korea's system of detention facilities, including its political prison camps, the role of security agencies and key institutions involved in human rights violations, North Korea's practice of dispatching workers overseas, and the connection between security issues and human rights when addressing North Korea. HRNK received UN ECOSOC consultative status in April 2018. It was also the first organization to propose that the human rights situation in North Korea be addressed by the UN Security Council. HRNK was directly and actively involved in all stages of the process, supporting the work of the UN Commission of Inquiry (COI) on North Korean human rights. Its publications have been cited numerous times in the report of the COI, the reports of the UN Special Rapporteur on North Korean human rights, a report by the UN Office of the High Commissioner for Human Rights, two reports of UN Secretary-General António Guterres, and several U.S. Department of State Democratic People's Republic of Korea Human Rights Reports. HRNK has also regularly been invited to provide expert testimony before the U.S. Congress.

About the Author

Robert M. Collins completed 37 years of service as a soldier and U.S. Department of the Army civilian employee. He served 31 years in various assignments with the U.S. military in Korea, including several liaison positions with the Republic of Korea Armed Forces. Mr. Collins' final assignment was as Chief of Strategy, ROK-US Combined Forces Command, serving the four-star American commander as a political analyst for planning on the Korean Peninsula and Northeast Asian security issues. He received the Sam-il Medal (Republic of Korea Order of National Security Medal, Fourth Class) from President Lee Myungbak and the U.S. Army Decoration for Exceptional Civilian Service by the Secretary of the Army. Mr. Collins earned a B.A. in Asian History from the University of Maryland in 1977, and an M.A. in International Politics, focusing on North Korean Politics, from Dankook University in 1988.

Mr. Collins is a Senior Advisor at HRNK, where he conducts interviews with North Korean escapees in South Korea to gather information on the North Korean population and the human rights situation in that country. He is the author of *Marked For Life: Songbun, North Korea's Social Classification System; Pyongyang Republic: North Korea's Capital of Human Rights Denial; From Cradle to Grave: The Path of North Korean Innocents; Denied From the Start: Human Rights at the Local Level in North Korea; North Korea's Organization and Guidance Department: The Control Tower of Human Rights Denial; South Africa's Apartheid and North Korea's Songbun: Parallels in Crimes Against Humanity; Propaganda and Agitation Department: Kim Jong-un Regime's Sword of Indoctrination; and Slaves to the Bomb: The Role and Fate of North Korea's Nuclear Scientists;* and *Coronavirus and North Korean Human Rights: Regime Response and Future Instability Scenarios*, all published by HRNK.

Acknowledgements

The author would like to thank Lieutenant General (retired) Chun In Bum and Brigadier General Choi Nak Jung for their guidance and perspective on this report. The author wishes to thank Greg Scarlatoiu, President and CEO of the Committee for Human Rights in North Korea (HRNK) for his direction and support; HRNK research interns Myriam Aribaud, Lilli Duberstein, Canion Hempel, Ellie Richard, Sloane Thor, Robert Walker, Gia Yun, and HRNK volunteer advisor Nick Miller for their editing work; and HRNK research intern Joseph Han Sung Lim for his work on the initial typesetting, the cover design, and the overall graphic design. Finally, the author would like to thank Kim Chongsuk Collins for her patience and support during the research and writing of this report.

Foreword

The Reconnaissance General Bureau—The Kim Regime's "Precious Treasured Sword" is the ninth in a series of HRNK reports Robert Collins has authored over the past fourteen years. Collins has mapped and analyzed both the hardware and the software that have propelled the Kim dynasty across three generations, from the regime's institutional building blocks to the plight of the North Korean people suffering from decades under a policy of human rights denial.

Survival remains the regime's fundamental strategic objective. The Kim family regime is not a political cartel. It is a political monopoly, facing no domestic opposition. The only competitor is "the other Korea," the free, democratic, modern, prosperous, economic and cultural powerhouse: South Korea. The North Korean regime understands that its long-term survival can't be guaranteed if South Korea continues to exist and thrive. From its viewpoint, unification under its control is the only way to guarantee its long-term survival.

To achieve that goal, the RGB has been the ultimate instrument of infiltration, subversion, and disruption of South Korea. Collins scrutinizes the RGB's genesis, history, mission, tactics, and chain of control and command. He highlights how RGB operations have violated international human rights law as well as the fundamental human rights of South Koreans and citizens of other countries.

To stay in power, the Kim regime develops nuclear weapons, other weapons of mass destruction, and ballistic missiles. The regime oppresses and exploits North Korean people at home and abroad to procure the funds needed to produce its tools of death and keep its elites happy through access to hard currency and luxury goods. Moreover, it fills its coffers through exporting instability and violence to the terrorist enemies of Israel via Iran and to Russia, for deployment in its unfettered aggression against Ukraine.

Collins thoroughly documents the RGB's critical role in cyber theft pursuant to regime orders. Once operational in three warfighting domains, land, sea and air, the RGB has adapted to the 21st century, aggressively disrupting and exploiting the cyber domain and even exploring involvement in geospatial intelligence and analysis. While subjugation of the entire Korean Peninsula continues to be its fundamental strategic objective, the RGB has become a global threat. Moving forward, Collins' report will serve as an essential, foundational source of information for those investigating the RGB's clandestine operations and their criminal impact on the human rights of South Koreans and others.

Greg Scarlatoiu

President and CEO

February 23 2026

Acronyms

CIA	Central Intelligence Agency (U.S.)
CISA	Cybersecurity and Infrastructure Security Agency (U.S.)
DMZ	Demilitarized Zone
DPRK	Democratic People's Republic of Korea (North Korea)
FBI	Federal Bureau of Investigation (U.S.)
GPB	General Political Bureau
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social, and Cultural Rights
KCC	Korea Computer Center
KPA	Korean People's Army
KWP	Korean Workers' Party
MSS	Ministry of State Security
MPAF	Ministry of People's Armed Forces (now the Ministry of Defense)
MPS	Ministry of Public Security
NDC	National Defense Commission
NIS	National Intelligence Service
NSPA	National Security Planning Agency
OGD	Organization and Guidance Department (KWP)
R&D	Research and Development
RGB	Reconnaissance General Bureau
ROK	Republic of Korea
SKWP	South Korean Workers' Party
UFD	United Front Department (KWP)
UAV	Unmanned Aerial Vehicle
USV	Unmanned Surface Vehicle

Executive Summary

Section 1 provides an overview of North Korea's Reconnaissance General Bureau (RGB), the country's primary foreign intelligence agency. This section outlines the RGB's main objectives as an organization, and explains how its goal of unifying the Korean Peninsula under the Kim regime is linked to human rights violations committed against South Korean citizens.

Section 2 explores the historical development of North Korean intelligence prior to the establishment of the RGB. It provides context for the origins of this organization by analyzing earlier agencies that performed counterintelligence work against South Korea in the 20th century. This list includes the Security Bureau, formed under Soviet military leadership, and the National Political Security Department, which combined counterintelligence work with regular policing duties.

Section 3 examines the mission of the RGB and analyzes how each of its six main bureaus contributes to this goal. This section argues that the primary objective of the RGB is to incite an uprising against the South Korean government and unify the Korean Peninsula under the Kim regime. This section also uses diagrams and charts to highlight the RGB's adherence to a strict chain of command that ultimately reports to North Korea's Supreme Leader.

Section 4 reviews the history of the RGB and predecessor organizations in terms of their provocations against South Korea. This section identifies and explores six main kinds of North Korean provocations against South Korea that took place in the 20th and 21st centuries: assassinations, air warfare, naval warfare, abductions, espionage, and DMZ tunnel activity.

Section 5 assesses North Korea's cyber warfare capabilities, which include hacking, information collection, bank/cryptocurrency theft, and ransomware. As the section explores, North Korea poses a sophisticated cybercrime and espionage threat, with organizations like the Lazarus Group stealing money from governments and multinational corporations around the world. Indeed, the section analyzes how North Korea's cyber warfare capabilities threaten global security as North Korea uses money from these operations to fuel its nuclear weapons programs.

Section 6 evaluates the impact of the RGB on the ROK-U.S. military alliance. It concludes that North Korea employs cyberwarfare – exemplified by the work of the Andarial Group — to gain intelligence on South Korean and U.S. military forces, underscoring the threat posed by North Korean cyber operations.

Section 7 discusses the various levels of RGB training and education. The section begins by talking about the level of education required to become a member of the RGB, noting that most hackers begin their training in grade school and later attend top technological universities to refine their skills. The section then shifts to explore the rigorous training and recruitment process within the RGB.

Section 8 reviews the current and past leadership of the RGB. It opens with a summary of North Korea's Supreme Leader, Kim Jong-un, and his relationship with the RGB. The section later explores the roles and influence of other North Korean leaders, including notable military generals like Oh Kuk-ryol, who have shaped the direction and operational priorities of the RGB over time.

Section 9 offers an overview of the international sanctions imposed on the RGB and its affiliated personnel. The section focuses on U.S. sanctions targeting North Korea, with particular attention to executive orders enacted by U.S. presidents in the 21st century. This section also discusses the enforcement actions taken by the U.S. Department of Justice, including the prosecution and indictment of RGB members who were involved in the 2014 Sony Pictures cyberattack.

Section 10 highlights how RGB operations infringe on the fundamental human rights of South Korean citizens and other foreign nationals. This section is divided into various subsections that address North Korean cybercrime, violations of international human rights law, and acts of terrorism. Together, these topics underscore the significant threat of the RGB not only to stability on the Korean Peninsula but global security as well.

Section 11 explains how the RGB has evolved over the years and explores what the future of the organization may look like moving forward.

Section 1: Introduction

North Korea's Reconnaissance General Bureau (RGB) is the Kim regime's leading foreign intelligence agency. However, it is far more than an intelligence agency in the traditional sense. Comparisons with the U.S. Central Intelligence Agency (CIA) or South Korea's National Intelligence Service (NIS) are misleading and incomplete. The RGB is not only a military reconnaissance unit, but also a combat unit, a cyber warfare group, an espionage bureau, a criminal enterprise, a terrorist organization, and a revolutionary entity all organized under a single control and command network that directly reports to North Korea's Supreme Leader, Kim Jong-un. The RGB's component predecessors have been, and continue to be, a direct threat to the independence, lives, and human rights of the South Korean people. Assassination, massacre, abduction, destruction of personal property, sabotage, subterfuge, and cyber theft are just some of the methods the RGB and its predecessors have used to deny South Korean citizens their rights and personal safety. North Korea's intent has been, and continues to be, enabling the Kim family regime to unify the Korean Peninsula under its rule and subjugating South Korea and its citizens to the same crimes against humanity experienced by North Korean citizens. The RGB is integral to this twisted dream.

Prior to 2021, the preamble to the Korean Workers' Party (KWP) charter stated, "The immediate purpose of the KWP is to build a powerful and prosperous socialist country in the northern half of the Korean Peninsula and to carry out the tasks of national liberation and democratic revolution across the country in order to fully achieve independence. This is the final goal of the Party."[1] Under this guidance, the RGB conducts operations of political warfare, foreign intelligence, propaganda, subversion, kidnapping, special operations, sabotage and assassinations to carry out the Kim regime's political-military strategy. The RGB is North Korea's main anti-South Korea operations and terrorism organization.[2]

The RGB operates in a unique place within the North Korean political and military structure. The official name of the RGB is the Reconnaissance General Bureau of the Korean People's Army (KPA). Its administrative military designation is KPA Unit 586. At the same time, the RGB is an agency directly under the North Korean State Affairs Commission (SAC) and it reports directly to the KPA Supreme Commander – Kim Jong-un. It is so important that the its reports are referred to as "No. 1 reporting unit" reports.[3]

---

1 National Commitee on North Korea, Bylaws of the Korean Workers Party", National Committee on North Korea, May 9, 2016.

2 Kwang-jin Kim, "North Korea's Terror Organizations and Their Possible Provocation (북한의 대남테러 조직 및 테러전망)," Korean Studies Information Service, 76, https://www.inss.re.kr/activity/bbs/academic_view.do?nttId=405324&bbsId=academic&page=10&searchCnd=0&searchWrd=.

3 Ibid, 78.

Prior to the establishment of the RGB, the KPA Reconnaissance Bureau, which was responsible for infiltrating the Demilitarized Zone (DMZ), was a long-standing organization subordinate to the KPA General Staff. In 2009, while Kim Jong-un was preparing to take office, North Korea restructured the KPA Reconnaissance Bureau and, to create a huge task force, designated the RGB. The new unit, as founded, included large-scale reconnaissance and infiltration operations by the former KPA Reconnaissance Bureau and the KWP Operations Department, as well as overseas intelligence operations conducted by the KWP Office 35. The RGB also oversees developing cyber warfare capabilities, which have grown in their effectiveness and importance to the Kim regime more than any other operational functions.[4]

The RGB was reorganized for better control by the Supreme Leader, both for command and political-military oversight. These aspects serve to shape national security for the North Korean party-state.

The RGB has focused on the unification of the Korean Peninsula under Kim regime rule and has therefore intentionally violated the human rights of South Korean citizens through abductions, assassinations, military provocations, monetary theft, and direct kinetic action as well as other threats. The RGB has carried out several vicious operations, such as the assassination of Kim Jong-un's brother, Kim Jong-nam, at Kuala Lumpur International Airport in Malaysia, and the DMZ mine blasting incident in 2015. In particular, the RGB has repeatedly carried out major hacking operations targeting South Korean banks, government agencies, and even the computers of the Blue House, the current South Korean presidential residence.[5]

On June 18th, 2015, Kim Jong-un posed for a photograph with RGB personnel during the first-ever RGB conference. Kim Il-sung and Kim Jong-il never posed for such a photograph with North Korean intelligence. Kim Jong-un described North Korea's reconnaissance and intelligence workers as "the Party's precious treasure" at the first Congress of KPA Reconnaissance Workers in 2015, demonstrating his trust and confidence in his premier foreign intelligence agency. In his address to RGB personnel, Kim Jong-un stated: "Our trusted reconnaissance workers and fighters – the Party has charged you with carrying out the most difficult and dangerous reconnaissance and intelligence front, even while fighting while you are young and missing family life. You are destroying the enemy while the whole world looks up to our state which is the strong unification of Paektusan country."[6]

---

4 Kwang-jin Kim, "North Korea's Terror Organizations and Their Possible Provocation (북한의 대남테러 조직 및 테러전망)," Korean Studies Information Service, 76, https://www.inss.re.kr/activity/bbs/academic_view.do?nttId=405324&bbsId=academic&page=10&searchCnd=0&searchWrd=.

5 Hyun-ki Lee, "북한 정찰총국의 실체" [Status of North Korea's Reconnaissance General Bureau], RFA, February 25, 2021. https://www.rfa.org/korean/weekly_program/c548cc2cc77c-bc15c0acc758-c8fcac04c9c4b2e8-1/weeklydiagnosis-02252021090845.html.

6 Seong-rim Ji, "北, 대남공작・사이버전 강화 예고..정찰일꾼대회" [North Korea foretells strengthening of cyber operations and cyber warfare…Reconnaissance Workers Demand], Yonhap TV, June 18, 2015. https://v.daum.net/v/20150618151731851?f=o.

Kim Jong-un has also labeled the RGB hackers as a "treasured sword."[7] The terms "treasure" and "sword" are Kim Jong-un's way of shaping political-military strategy by expressing his favoritism to competing bureaus – an effective but flawed tactic. Kim Jong-un has also proclaimed his leading intelligence agency as the "brave RGB…warriors…for the construction of a strong and prosperous nation."[8]

This report will describe the threat the RGB poses not only to the existence of the South Korean nation-state, but also to the South Korean populace. Many South Korean citizens may think North Korean actions have no impact on them personally. However, the North's policies do impact support for the South Korean government, including the personal and financial security of both the government and people, as well as ideological efforts to undermine the South Korean government and democracy on the domestic and international level.

7 Ed Caesar, "The Incredible Rise of North Korea's Hacking Army," The New Yorker, April 19, 2021. https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army.
8 Ibid.

Section 2: Historical Background of North Korean Intelligence Prior to the RGB

Since the end of the Japanese occupation period (August 15th, 1945), North Korean intelligence has predominantly focused on South Korea, both before and after its official founding as a state. The organization, institutional responsibility, and mission sets of the North Korean intelligence apparatus have changed from Kim Il-sung to Kim Jong-il, and eventually Kim Jong-un. However, its primary focus has always been on South Korea.

North Korean intelligence agencies have continuously been reorganized and/or redesignated from combined to independent structures and vice versa. The division of intelligence missions and tasks among several intelligence agencies has created competition between them for the Supreme Leader's favor. This division allows the Supreme Leader to ensure the agencies monitor one another, improving regime longevity and security.[9] The exact function and organization of North Korean political-military elements is difficult to assess due to frequent reorganization and redesignation. Furthermore, with advances in technology, specified functions have changed over the last five decades, offering North Korea further opportunities to exploit South Korean political, military, and technical vulnerabilities. We will address these changes in this chapter.

North Korea's first intelligence agency was the Security Bureau (보안국), which was established upon the founding of North Korea's Provisional People's Committee on February 8th, 1946, under the leadership of the Soviet Union's 25th Army (commanded by Colonel General Ivan Chistyakov). At that time, the Security Bureau mandate included border security, internal state security, inspections, firefighting, and security escorts. Under the Security Bureau, an intelligence branch was established. This branch conducted standard intelligence missions against South Korea, constituting North Korea's original predecessor of the RGB. At first, the Security Bureau was commanded by Choi Yong-geon, who served with Kim Il-sung as an anti-Japanese partisan before and during World War II.

When the North Korean Provisional People's Committee, led by Kim Il-sung, established the Ten Administrative Bureaus (행정10국) in February 1946, the Security Bureau was given a subordinate Political Security Department (정치보위부), commanded by Kim Pa. This organization's function paralleled the Ministry of State Security (MSS) and the RGB of today. On May 11th, 1946, the North Korean Provisional People's Committee established the Security Independent Brigade (보안독립여단), commanded by Choi Hyon, another anti-Japanese partisan.[10] A year later, on February 27th, 1947, the Security Bureau was redesignated the Internal Affairs Bureau (내무국), under the command of Pak Il-u.

9 Dong-yol Yoo, "북한 정보기구의 변천과 현황 (North Korean Intelligence Organizations Change and Status), 178. https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002354345.

10 Ibid, 158.

The National Security Agency (민족보위성) was created on February 7th, 1948 and assumed the duties of national defense under Kim Chaek. Once the North Korean state was officially founded on September 9th, 1948, the Internal Affairs Bureau became the Ministry of Internal Affairs (내무성). The Ministry of Internal Affairs continued conducting police and intelligence functions while the National Security Agency continued military intelligence functions.[11] The KPA Reconnaissance Bureau (militarily referred to as the 589th Army unit) was also established during this period.[12]

In March 1951, the Political Security Department, along with other intelligence elements, was reorganized into the Ministry of Social Safety (not to be confused with today's Ministry of Social Security). The Ministry of Social Safety's mission during the Korean War was mainly internal security to ensure the population remained loyal to the Kim regime. At this time, the Ministry of Social Safety consisted of a headquarters with eleven bureaus that had branches at every province, county, and city level as well as other lower regional levels as required.[13] The Ministry of Social Safety carried out standard counterintelligence, police, firefighting, citizen registration, prison functions, port control, and air defense missions. It even established the first North Korean government prison bureau in the state's history. The Ministry of Social Safety was subordinated to the Ministry of Internal Affairs in October 1952, as the areas of responsibility were too vast for the organization to control alone. Pang Hak-se led this combined organization.[14]

Intelligence activities targeting South Korea have historically been led by the KWP with its subordinate elements – the United Front Department (UFD), the External Liaison Department, Operations Department, and Office 35. In 1961, the Kim regime integrated anti-South Korean and foreign intelligence agencies by establishing the KWP Liaison Bureau (연락국), commanded by Major General Cho In-cheol. The subsequent commanders included Pak In-cheol and Im Hae.[15] The integrated agencies included the KPA Reconnaissance Bureau, the Ministry of Internal Affairs Counterintelligence Branch (반탐처), and the KWP Liaison Department (연락부).[16]

---

11 Dong-yol Yoo, "북한 정보기구의 변천과 현황 (North Korean Intelligence Organizations Change and Status), 158. https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002354345.

12 Joseph S. Bermudez, Jr., North Korean Special Forces, Naval Institute Press, Annapolis, Maryland 1998; 29, 60.

13 Dong-yol Yoo, "북한 정보기구의 변천과 현황 (North Korean Intelligence Organizations Change and Status), 158. https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002354345.

14 Ibid, 159.

15 Joseph S. Bermudez, Jr., North Korean Special Forces, 64-5.

16 Il-Gi Kim and Ho-hong Kim, "김정은 시대 북한의 정보기구" [North Korean Intelligence Organizations in the Kim Jong-un Era], inss.re.kr, December 31, 2020, 10. https://inss.re.kr/publication/bbs/rr_view.do?nttId=409818.

In 1956, the Ministry of Internal Affairs underwent a major reorganization. Under Bang Hak-se, there were five deputies, nine bureaus, and seven branches. The 1st Bureau (Social Safety Bureau) was responsible for anti-South Korea missions that reflect those of today's RGB. On October 23rd, 1962, police functions were once again transferred to the re-established Ministry of Public Security (MPS). In 1968, the KPA established the Political Safety Bureau (정치안전국). On December 27th, 1972, the North Korean Constitution was rewritten and the MPS was redesignated the Social Safety Department (사회안전부), placed under the North Korean Cabinet. In May 1973, counterintelligence functions were separated from police functions, which were retained by the Social Safety Department. The newly established National Political Security Department (국가정치보위부) assumed counterintelligence duties.[17]

North Korea established the KWP Investigations Department in the early 1960s. In the 1980s, the KWP Investigations Department was divided into two branches: the KWP Overseas Intelligence Investigation Department and the KWP Operations Department. General Oh Gukryol, arguably one of the most competent military leaders in KPA history, commanded the Operations Department during the period of 1989-2009 and ran infiltration agent operations during that time. The Operations Department was later incorporated into the RGB in 2009.[18]

In the mid-1960s, the Anti-South Korea Affairs General Bureau led intelligence operations against the South. In the late 1960s through the early 1970s it was led by the KWP Secretary for South Korean Affairs. Under Kim Il-sung and Kim Jong-il, North Korean intelligence agency leaders experienced both trust and harsh criticism from the Supreme Leader.[19] These organizations remained the centers of intelligence gathering in various iterations until 2009 when North Korea restructured the KPA Reconnaissance Bureau to formally create the RGB.

17 Dong-yol Yoo, "북한 정보기구의 변천과 현황 (North Korean Intelligence Organizations Change and Status), 160. https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002354345. Reportedly, the UFD has been disbanded and redesignated Bureau 10, with many of its functions shifted to North Korea's Ministry of Foreign Affairs.

18 Il-Gi Kim and Ho-hong Kim, "김정은 시대 북한의 정보기구" [North Korean Intelligence Organizations in the Kim Jong-un Era], inss.re.kr, December 31, 2020, 63, 64. https://inss.re.kr/publication/bbs/rr_view.do?nttId=409818.

19 Ibid, 89.

Section 3: RGB Mission and Organization

The mission of the RGB is to support the communization of South Korea and the unification of the Korean Peninsula under the Kim regime. It carries out specific tasks targeting South Korea such as intelligence collection, agent infiltration, psychological warfare, terrorism, sabotage, assassination, abduction, inter-Korean military dialogue, reconnaissance, manufactured social confusion, unmanned aerial vehicle operations, and cyber warfare.

The Kim regime has historically engaged in illegal transactions like counterfeiting, blackmail, dealing pharmaceuticals, arms exports, and human trafficking to gain funding for its regime objectives and military programs (instead of the welfare of the North Korean people). Besides supporting these efforts, other specific RGB tasks include creating conflicts within South Korea, managing public relations, directing socio-political dialogue in support of the North, and supporting pro-North Korea efforts in South Korea. All operations are geared towards creating an ideal environment for unification of the Korean Peninsula under the Kim regime.[20]

In February 2009, the Kim regime established the RGB by integrating three agencies: the Reconnaissance Bureau under the Ministry of People's Armed Forces (MPAF, now the Ministry of Defense), the KWP's Operations Department, and the KWP Office 35 (which oversaw operations against South Korea and overseas operations as well as North Korea's disparate cyber capabilities). The RGB was created so the North Korean Supreme Leader would have streamlined control and command of all intelligence operations.[21]

Although the RGB is organized under the KPA General Staff, it reports directly to Kim Jong-un as the Supreme Commander of the KPA and the Chairman of the SAC.[22] The chart below depicts the initial control chain under Kim Jong-Il, which has remained virtually the same though some organizations have been renamed since.[23]

To update the titles on this chart to the present, Kim Jong-un replaces Kim Jong-il ("Kim Chong-il"), the SAC replaces the National Defense Commission (NDC), and the Ministry of Social Safety.

---

20 Kwang-jin Kim, North Korea's Terror Organizations and Their Possible Provocation (북한의 대남테러 조직 및 테러전망) 76. https://kiss.kstudy.com/DetailOa/Ar?key=50168279, Kim Il-Gi and Kim Ho-hong, "김정은 시대 북한의 정보기구" [North Korean Intelligence Organizations in the Kim Jong-un Era], inss.re.kr, December 31, 2020, 10. https://inss.re.kr/publication/bbs/rr_view.do?nttId=409818.

21 Laura Bicker, "Drugs, arms, and terror: A high-profile defector on Kim's North Korea", BBC, October 10, 2021. https://www.bbc.com/news/world-asia-58838834.

22 Ibid. The Administrative Department was disbanded in 2013 and all of its functions and responsibilities were assumed by the Organization and Guidance Department, thus vastly increasing the power and influence of the Organization and Guidance Department.

23 Joseph S. Bermudez, Jr., "Special Report: A New Emphasis on Operations Against South Korea?," 38 North, June 11, 2010. https://www.38north.org/wp-content/uploads/2010/06/38north_SR_Bermudez2.pdf, note that the National Defense Commission is now the State Affairs Commission, the Ministry of People's Armed Forces is now designated the Ministry of Defense, the State Security Department is now the Ministry of State Security and Organization and Guidance refers to the KWP Organization and Guidance Department.

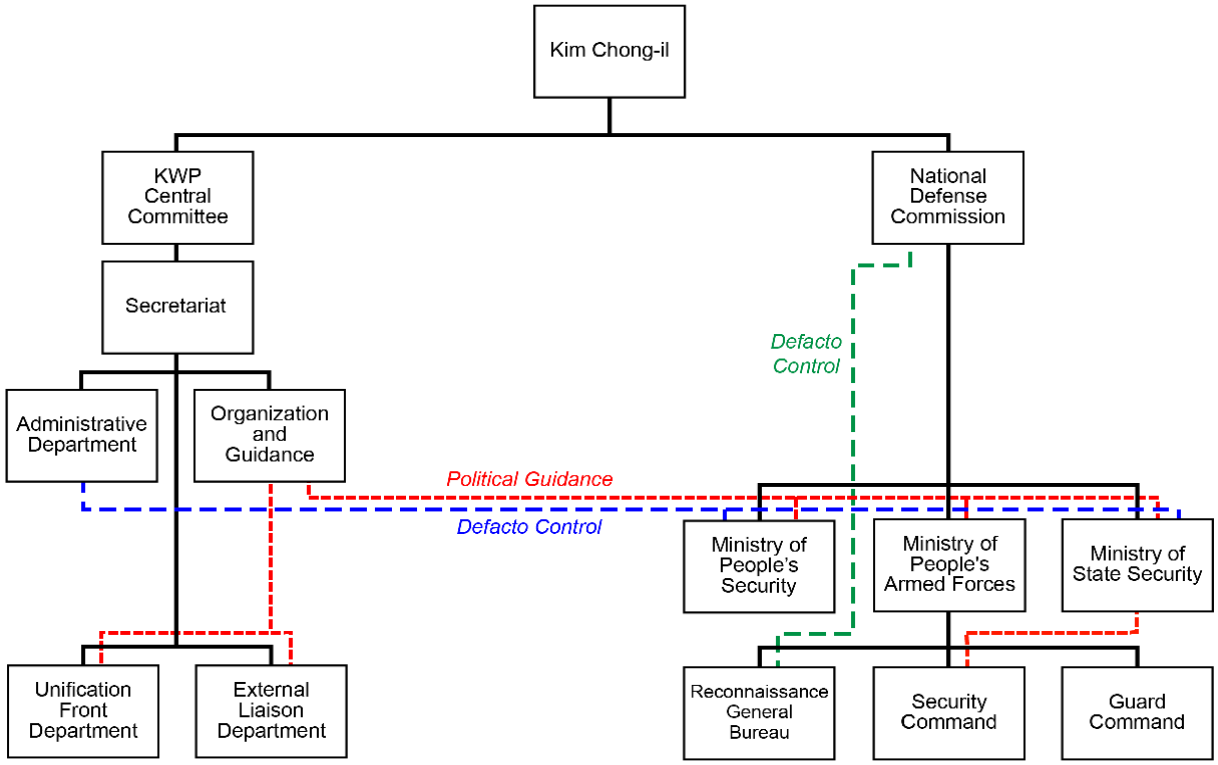


Figure 1, Source: Joseph Bermudez, "38 North Special Report: A New Emphasis on Operations Against South Korea, 38 North, June 11, 2010. http://www.38north.org/wp-content/uploads/2010/06/38north_SR_Bermudez2.pdf.

A more detailed breakdown of the RGB organization is illustrated below.[24] The RGB command group consists of the commander, the deputy commander, and the senior political officer from the General Political Bureau (GPB). The RGB commander also serves as the KPA vice-chief of the General Staff, the second highest position in the KPA.

24 Joseph S. Bermudez, Jr., "Special Report: A New Emphasis on Operations Against South Korea?," 38 North, June 11, 2010. https://www.38north.org/wp-content/uploads/2010/06/38north_SR_Bermudez2.pdf, note that the National Defense Commission is now the State Affairs Commission, the Ministry of People's Armed Forces is now designated the Ministry of Defense, the State Security Department is now the Ministry of State Security and Organization and Guidance refers to the KWP Organization and Guidance Department.

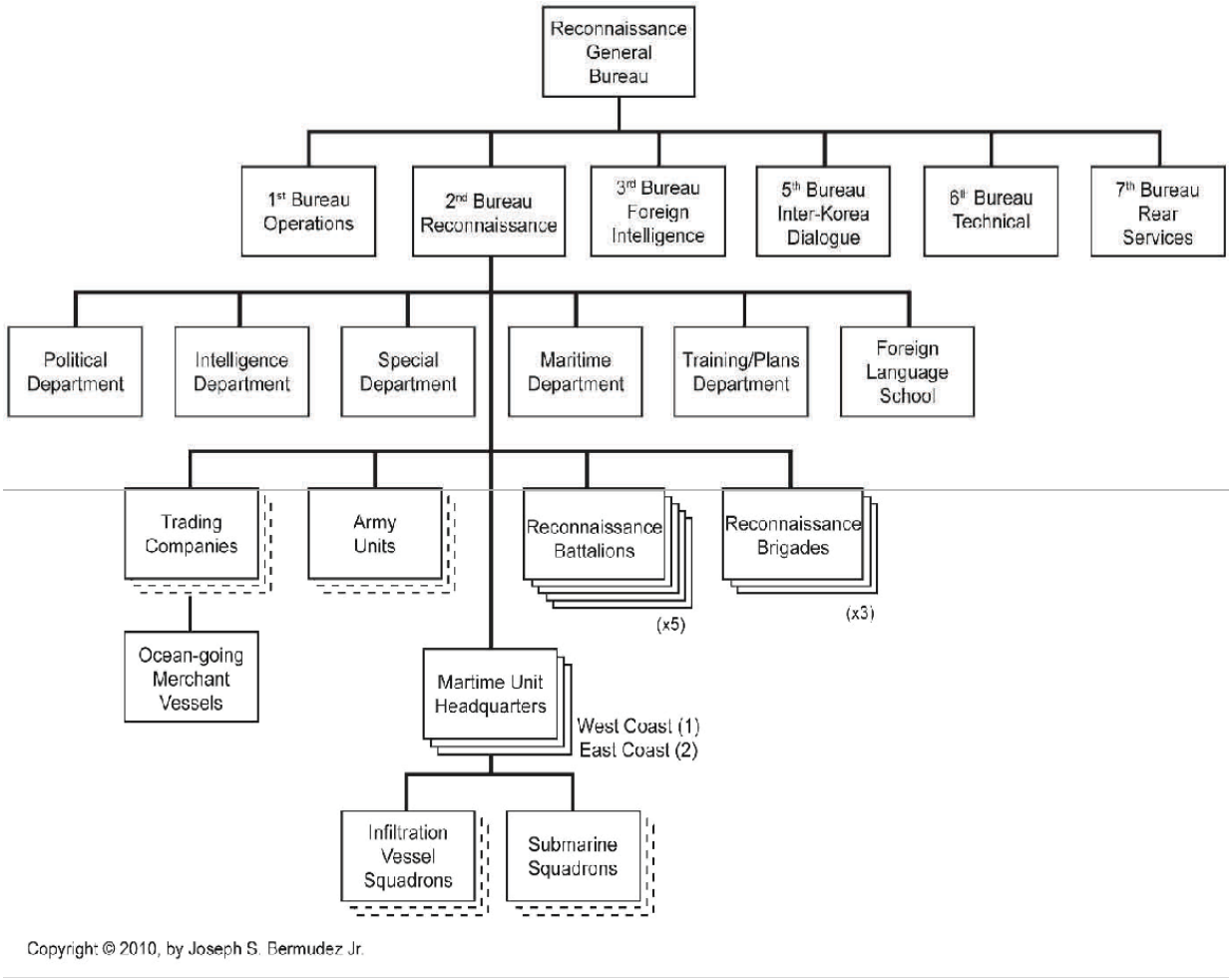


Figure 2, Source: Joseph Bermudez, "38 NORTH SPECIAL REPORT: A NEW EMPHASIS ON OPERATIONS AGAINST SOUTH KOREA?" 38 North, June 11, 2010. https://www.38north.org/wp-content/uploads/2010/06/38north_SR_Bermudez2.pdf.

Within the RGB, operations are further divided into subordinate elements located all over North Korea.[25] The largest divisions are the six RGB bureaus.

The 1st Bureau is known as the Land-Sea Reconnaissance Bureau or the Operations Bureau. Prior to the establishment of the RGB, it was the KWP Operations Department. As the KWP Operations Department did in the past, the 1st Bureau trains infiltration agents, develops infiltration routes, escorts and guides infiltration agents, and conducts terrorist operations against South Korea. The 1st Bureau also trains operatives to destroy military and military-industrial targets in South Korea.

25 "The General Bureau is the 'headquarters of operations against South Korea' that integrates the Party Operations Department and the Military Reconnaissance Bureau." [출처:중앙일보] Korea Joongang Daily, April, 4, 2010. https://www.joongang.co.kr/article/4121510.

This bureau and its predecessor, the KWP Operations Department, have been responsible for major provocations against South Korea, such as the Sokcho City infiltration incident of June 1985, the Tonghae City infiltration incident of July 1998, the Yeosu coast infiltration incident employing a semi-submersible vessel in December 1998, and the bombing of Korean Airlines Flight 858 in 1987. The Bureau operates with an estimated five thousand personnel comprised of the following elements designated as "liaison[26] stations":[27]

- 130 Liaison Station: Kim Jong-Il Political-Military College, which conducts agent training for infiltrators or agent escort operatives infiltrating other agents into South Korea, Japan, and elsewhere.
- 915 Liaison Station: Responsible for hospital drug manufacturing.
- 314 Liaison Station: Responsible for logistical support in weapons, communication equipment, and counterfeit dollars.
- 414 Liaison Station: Supplies counterfeit dollars, identification cards, communication devices, and weapons (Other source states the 414th trains hackers[28]).
- Overland Infiltration Staging Bases:
    - 217th KPA Unit (283rd Liaison Station): Located in Kaesong City, Hwanghae North Province, it is responsible for the western and central front.
    - 25th KPA Unit (715th Liaison Station): Located in Sariwon, Hwanghae North Province, it is responsible for the central and eastern front.
    - 101st KPA Unit (101st Liaison Station): Located in Pyongwon County, Kang-won Province, this station serves as the staging base for overland infiltration.
    - 198th Liaison Station: Located in Pyongwon, this is a second staging base for overland infiltration.
- Seaborne Infiltration Staging Bases: Four bases, three hundred personnel to target South Korea's 15,000 kilometers of coastline for infiltration.
    - 927th Liaison Station: Located in Nampo City, Pyongan South Province, this is a staging base for seaborne infiltration along the Mokpo Straits and the Geoje Island-Jeju Island Straits.

---

26 The term "liaison" originated in the 1950s with the KWP Liaison Department which was responsible at the time for all North Korean actions targeting South Korea. Today, the term "liaison station" refers to military and KWP units.

27 Il-Gi Kim and Ho-hong Kim, "김정은 시대 북한의 정보기구" [North Korean Intelligence Organizations in the Kim Jong-un Era], inss.re.kr, December 31, 2020, https://inss.re.kr/publication/bbs/rr_view.do?nttId=409818.

28 Pil-jae Kim, "북한의 사이버 남침 (North Korea's Cyber Invasion of the South)," Korean Journal of Public Security Association. Vol. 29, No. 4 (2020), 49.

- Haeju Liaison Station: This is the staging base for infiltrations of the western and southern coastlines.
- Wonju Liaison Station: This is the staging base for the South Korean eastern coastline.
- Chongjin Liaison Station: This is the staging base for infiltrations of Japan.
- 448th KPA unit: Located in Nakwon, Hamgyeong South Province, this serves as the staging base for submarine-based seaborne infiltration. The unit uses Yugo-class submarines, semi-submersibles, and shark-class submarines for sea infiltration and, occasionally, ships disguised as fishing boats.[29]

» Support headquarters includes fifty communication sites throughout North Korea. These sites, some stationary and some mobile, send and receive communications with operatives during infiltration missions. There is also a specialized laboratory for code cracking.

- 314 Liaison Station oversees procurement of various weapons, counterfeit identification cards, communication devices, and counterfeit dollars.

The 2nd Bureau, also known as the RGB Reconnaissance Bureau, has seven reconnaissance battalions and headquarters, with the Political Branch, Planning Branch, Special Reconnaissance Branch, and Communications Branch. It contains 4,500 personnel at three dispatch bases along the Demilitarized Zone, as well as the east and west coasts. The 907th Unit in charge of espionage training for spies, and Ma Dong-hui College (formerly known as Yalugang College or Apnokgang College) provide language training to guerrilla fighters.

Each KPA corps and division also have reconnaissance battalions. These units carry out reconnaissance missions to serve military-specific operations, such as collecting information related to South Korean military weaknesses, South Korean defenses against North Korean infiltration, and South Korean communications. The Pyonggang Liaison Station was moved to Sariwon in preparation for emergency situations, such as incidents in the forward DMZ and at industrial facilities, airfields, and ports in the South Korean rear area.[30] The Reconnaissance Bureau includes the 907 Army Unit, the 448 Army Unit, the submersible infiltration unit, the 22nd Squadron, the Nampo Maritime Special Forces, and the Reconnaissance Battalion directly under the Reconnaissance Bureau.

---

29 Kwang-jin Kim, North Korea's Terror Organizations and Their Possible Provocation (북한의 대남테러 조직 및 테러전망) 76. https://kiss.kstudy.com/DetailOa/Ar?key=50168279,, Kim Il-Gi and Kim Ho-hong, "김정은 시대 북한의 정보기구" [North Korean Intelligence Organizations in the Kim Jong-un Era], inss.re.kr, December 31, 2020,. https://inss.re.kr/publication/bbs/rr_view.do?nttId=409818.

30 Ibid.

The eastern department carried out the assassination bombing of Aung San in Burma in 1983, the Gangneung infiltration submarine (shark-class) incident in 1996, and the Hwang Jang-yop attempted assassination incidents in 2010 (carried out by Dong Myeong-Kwan, Kim Myeong-Ho, and Lee Dong-Sam). The department also previously operated a salmon-class submarine, which is known to have sunk the Cheonan in 2010.[31]

The Reconnaissance Bureau also intensively collects information related to South Korean counterintelligence capabilities and weaknesses in South Korean communication systems. In addition, if necessary, these liaison stations carry out missions such as armed infiltration, leadership assassinations, kidnapping, kinetic targeting/sabotage, and terrorism. For these purposes, it is essential to develop infiltration routes in mountainous areas.[32] Lastly, both the 1st Bureau and 2nd Bureau have significant maritime capabilities to infiltrate South Korea and Japan. This will likely lead to some consolidation to one bureau or the other in the near future.[33]

» The Four Seaborne liaison stations:

  - 459th KPA Unit: Located in Chongjin, Hamgyeong North Province, this unit is responsible for missions against Japan and operates twelve "mother ships."[34]
  - 632nd KPA Unit (313th Liaison Station): Located in Kalgo-ri, Wonsan, Kangwon Province, this unit is responsible for missions on the east coast.
  - 755th KPA Unit (aka 755th Liaison Station): Located in Mongkumpo, Haeju City, Hwanghae South Province, it is responsible for missions on South Korea's west coast.
  - 753rd KPA Unit (927th Liaison Station): Located in Nampo City, Pyongan South Province, it is responsible for missions on South Korea's south coast.

» Subordinate special units

  - 38th Airborne Brigade: Located in Sangwon County, Pyongyang.
  - 22nd Submarine Squadron (448th KPA Unit): Located in Wonsan, Kangwon Province, specializes in submarine extraction.
  - 24th Seaborne Sniper Brigade (406th KPA Unit): Located in Munchon County, Kangwon Province.

---

31 Il-Gi Kim and Ho-hong Kim, "김정은 시대 북한의 정보기구" [North Korean Intelligence Organizations in the Kim Jong-un Era], inss.re.kr, December 31, 2020, 66. https://inss.re.kr/publication/bbs/rr_view.do?ntId=409818 See also Korea Institute of Liberal Democracy, "자유민주 사상전 (Liberal Democracy Ideological Warfare), kild.or.kr, July 26, 2019. https://www.kild.or.kr/.

32 Kwang-jin Kim, North Korea's Terror Organizations and Their Possible Provocation (북한의 대남테러 조직 및 테러전망), 76, https://kiss.kstudy.com/DetailOa/Ar?key=50168279.

33 Joseph S. Bermudez, Jr., "38 NORTH Special Report: A New Emphasis on Operations Against South Korea?".

34 Ibid.

- 29th Seaborne Sniper Brigade (252nd KPA Unit): Located in Dongnim County, Pyongan North Province.
- 24th Reconnaissance Battalion (3168th KPA Unit): The Pyongyang Security Unit.
- 71st Reconnaissance Battalion (1313th KPA Unit): Located in Sinchon County, Hwanghae North Province.
- 72nd Reconnaissance Battalion (1314th KPA Unit): Located in Sinchon County, Hwanghae North Province.
- 73rd Reconnaissance Battalion : Location unknown.
- 69th Reconnaissance Battalion: Located in Kwail County, Hwanghae South Province, this battalion conducts overseas infiltration with focus on Okinawa and is comprised of officers only.

» Corps-level units: four battalions

- 70th Reconnaissance Battalion: Fourth Corps, located in Haeju City, Hwanghae South Province.
- 75th Reconnaissance Battalion: Second Corps, located in Pyongsan County, Hwanghae North Province.
- 104th Reconnaissance Battalion: Third Corps, located in Pyonggang County, Kangwon Province.
- 74th Reconnaissance Battalion: First Corps, located in Hwoeyang County, Kangwon Province.

The 3rd Bureau performs the functions of the former KWP External Information Investigation Department (Office 35). It oversees collecting information on South Korea and foreign countries, training and dispatching spies, spying, and carrying out terrorism against South Korea and international targets. There are seven branches: the South Korea Branch, the Japan Branch, the U.S. Branch, the Asia Branch, the Europe Branch, the Middle East-Africa Branch, and the Operations Branch. Its main bases of activity are Tokyo and Osaka in Japan, Macau and Hong Kong, Shanghai, Shenyang and Yanji in China, and Bangkok in Thailand. In Europe, it is active in Paris and Vienna, and in Africa it has reached Nigeria, Ethiopia, and Tanzania. It has also penetrated into the United States and infiltrated Latin America for operations targeting the United States. The Dialogue Coordination Branch is responsible for developing negotiation skills related to inter-Korean military dialogue and coordinating meetings.[35]

35 Kwang-jin Kim, North Korea's Terror Organizations and Their Possible Provocation (북한의 대남테러 조직 및 테러전망) 79. https://kiss.kstudy.com/DetailOa/Ar?key=50168279.

Below is a list of subordinate elements:

» 810th KPA Unit: The special assassination section of the Biological Technical Research Institute.

» Moran Flower Platoon: Oversees female operatives.

» Operations elements (4): South Korea, Asia, Japan, U.S. Group.

» Analysis elements (3): intelligence analysis, cyber security, asset security.

» Support elements (4): personnel, organization, inspection, asset research.

» Organizational elements (7): South Korea Section, Japan Section, U.S. Section, Asia Section, Europe Section, Middle East-Africa Section, Operations Section.

The 4th Bureau: Inter-Korean Dialogue management

» Assessed missions: South-North Talks support, South-North Talks technical development, South-North Talks management, South-North military talks policy development, South-North inter-Korean general-level military talks strategy development, meetings monitoring, and military strategy targeting South Korea.[36]

The 5th Bureau is also known as the Technical Reconnaissance Bureau. It conducts cyber terror, hacking, secret communications analysis, and communications interception.[37] (See Section 5 on RGB Cyber Warfare for more details).

» 121st Bureau: The lead cyber unit for the RGB.

» 110th Research Institute: hacking.

- 100th Research Institute manipulates cyber space to collect strategic intelligence against South Korea and the United States, as well as conducting psychological operations, cyber terror and Distributed Denial of Service (DDOS) attacks against South Korea and the United States.[38]
- 31st Technical Reconnaissance Station handles hacking program development and comprises 50-60 officers.
- 32nd Technical Reconnaissance Station oversees military-related program development with 50-60 officers.

36 Kwang-jin Kim, North Korea's Terror Organizations and Their Possible Provocation (북한의 대남테러 조직 및 테러전망) 79. https://kiss.kstudy.com/DetailOa/Ar?key=50168279; "The General Bureau is the 'headquarters of operations against South Korea' that integrates the Party Operations Department and the Military Reconnaissance Bureau." [출처:중앙일보] Korea Joongang Daily, April, 4, 2010. https://www.joongang.co.kr/article/4121510.

37 Il-Gi Kim and Ho-hong Kim, "김정은 시대 북한의 정보기구" [North Korean Intelligence Organizations in the Kim Jong-un Era], inss.re.kr, December 31, 2020, 66. https://inss.re.kr/publication/bbs/rr_view.do?nttId=409818.

38 Ibid.

- 33rd Technical Reconnaissance Station is responsible for psychological operations targeting South Korean society.
- 56th Technical Reconnaissance Station handles command communications program development with 60-70 officers.

The 6th Bureau provides support operations. It is comprised of the following subordinate elements:

» 128th Liaison Station: radio communications interference, jamming, intercepting and decrypting information from foreign intelligence sites, and hacking major countries as targets.[39]

» 314th Liaison Station: 1st Bureau logistical support.

» 198th Liaison Station: 2nd Bureau information collection.

» 448th Liaison Station: 2nd Bureau submarine infiltration support.

» 907th Liaison Station: Trains 2nd Bureau agents in South Korean social customs.

» 96th Logistical Center: Equipment supply.

» 315th Research Institute: Anti-South Korea operational tactics research.

» 915th Research Institute: Drug manufacturing (aka 915th Hospital).

» 772nd Liaison Station: 91st Reconnaissance Hacking Unit; one colonel, seven captains, eighty personnel. Reportedly, this unit is responsible for developing tactics to disrupt U.S. nuclear control and command.[40]

» 130th Liaison Station: Kim Jong-il Political-Military College in Pyongyang.

» 707th Communication Reception Facility: operates seven reception sites.

» 121st Liaison Station: GPS jamming radio operations along the Military Demarcation Line in the Demilitarized Zone. It is headquartered in Nampo with stations in Haeju and Kaesong.

» 1501 Unit: South Korean infiltration equipment manufacturing.

---

39 Mok Yong-jae, "김정은 집권 이후 신설된 북 해킹조직 6개 (Six New North Korean Hacking Organizations Created Since Kim Jong-un's Rise to Power)," rfa.org, November 22, 2017. https://www.rfa.org/korean/in_focus/ne-my-11222017102238.html.

40 Moon Dong-hee, "정찰총국 인사조치에 對南 사이버공격 우려…어떤 부서길래" [Concerns about reinforcing cyberattacks in South Korea in response to personnel measures by the Reconnaissance General... What kind of department], Daily NK, September 23, 2020. https://www.dailynk.com/%EC%A0%95%EC%B0%B0%EC%B4%9D%EA%B5%AD-%EC%9D%B8%EC%82%AC%EC%A1%B0%EC%B9%98%EC%97%90-%E5%B0%8D%E5%8D%97-%EC%82%AC%EC%9D%B4%EB%B2%84%EA%B3%B5%EA%B2%A9-%EC%9A%B0%EB%A0%A4-%EC%96%B4%EB%96%A4-%EB%B6%80/.

» 519th Liaison Station: Mission unknown.

» Other liaison stations: 26th, 112th, 697th Liaison Stations.

Drone Warfare

Considering advances in drone capabilities, such as identifying, selecting, and attacking targets, drone technology is changing the face of warfare. This is no different for North Korea. Drones are capable of hovering over targets for minutes in order to obtain a clear shot, which enables them to reorient weaponry to other South Korean targets for primary and secondary avenues of approach.[41] North Korean operators must adapt to processing the mission and identifying targets both close and far. At the lower levels, they must communicate with adjacent units. Drone operators must rely on integrating sensors, processors, and shooters to shorten their mission execution time frame. Battlefield information gathering, however, is a weakness for the KPA. While the North has invested heavily in developing its missiles and nuclear weapons capability, it has not adequately developed its drone program to further its real time battlefield intelligence capability.

Based on South Korean military estimates, North Korea's RGB operates three hundred to one thousand drones. Though a weak replacement, drone reconnaissance photographs provide the KPA with intelligence that its air force cannot. However, it should be noted that downloading Google Earth imagery would provide better intelligence than the drone imagery North Korea is capable of collecting today. North Korea's drone program began in the late 1980s by importing Chinese D-4 drones. These were reverse engineered into the KPA's Panghyon-1 and Panghyon-2 drones. The drone development program expanded with the import of VR-3 and Pchela-1T reconnaissance drones from the Middle East and Russia in the 1990s.[42]

During his visit to Russia in September 2023, Kim Jong-un was presented five kamikaze drones and a Geran-25 reconnaissance drone which is capable of vertical takeoff.[43]

The RGB drones can compensate somewhat for KPA air forces' aging capabilities. These drones can be designed to collect imagery intelligence, carry weapons payloads of forty-five to fifty-five pounds, and are capable of dropping biological and chemical weapons onto South Korea and killing tens of thousands of South Korean citizens.[44]

---

41 Frank Bajak and Hanna Arhirova, "Drone advances in Ukraine could bring new age of warfare," C4ISRNET, January 5, 2023. https://www.c4isrnet.com/battlefield-tech/2023/01/05/drone-advances-in-ukraine-could-bring-new-age-of-warfare/?SToverlay=2002c2d9-c344-4bbb-8610-e5794efcfa7d.

42 Shreyas Reddy, "Explainer: How North Korea is developing drones into weapons of war," NK News, December 29, 2022. https://www.nknews.org/2022/12/explainer-how-north-korea-is-developing-drones-into-weapons-of-war/.

43 "Kim given gift of drones on Russian trip," koreatimes.co.kr, September 17, 2023. https://www.koreatimes.co.kr/www/nation/2023/09/103_359387.html.

44 Ibid.

Long-distance drones were unveiled at an exhibition for visiting Russian generals in July 2023. According to North Korean television, the RQ-4 Global Hawk copy is designated Morning Star-4 (샛별-4, Saetbyeol-4), and the MQ-9 copy Morning Star-9 (샛별-9, Saetbyeol-9).

Figure 3, Source: Dagyum Ji, "Seoul to mass produce air defense radars to counter N. Korean drones", NK News, July 14, 2017, https://www.nknews.org/2017/07/seoul-to-mass-produce-air-defense-radars-to-counter-n-korean-drones/.

In May 2017, North Korea sent a drone from Geumgang County 266 km south to photograph the U.S. military's THAAD air defense base in Seongju, South Korea. The drone crash landed in Inje County, South Korea during its return. After recovering the wreckage, the South Korean military determined the drone had taken 551 photographs of South Korean sites, ten of which were of the THAAD base. The drone was made of parts from six different countries: the flight control computer was from Canada; the camera was from Japan; the engine was from the Czech Republic; the wing controls were from South Korea; and other parts from Switzerland and the United States.

In December 2022, North Korea sent five drones into South Korean airspace for the first time since 2017, but South Korea was unable to shoot them down.[45] In 2021, Kim Jong-un acquired new unmanned aerial vehicles (UAVs) capable of ranging five hundred kilometers, all the way to Jeju Island.[46] The North Korean drone threat is serious enough for South Korea to consider purchasing Israel's "electric eye" drone detection system for defense against North Korea's drone infiltration.[47]

Models of North Korean drones include:

» Soviet Tupolev Tu-143-based model that conducts short-range (60–70 kilometer) tactical reconnaissance and has low-level flight capability with retrievable pod after flight.

» Russian Shmel-1-based model is a short-range reconnaissance drone.

» MQM-107 Streaker-based model.

» Sky 09P-based model from China is primarily a photographic reconnaissance drone that is capable of 3D imagery and flying at the nine thousand foot-level.

» UV-10 Cam based model that is a very short-range tactical drone for observing enemy frontline force alignment.

In addition to air drones, North Korea no doubt has imported technology regarding unmanned surface vehicles (USV), small waterborne ships capable of carrying attack munitions against enemy ships. Although there is little information on the North Korean Navy's use of USVs, the most logical target is the South Korean Navy First Fleet craft on the east coast and the 2nd Fleet craft on the west coast and along the Northern Limit Line.

45 Shreyas Reddy, "Explainer: How North Korea is developing drones into weapons of war"; See also Pak Hong-hwang, "북무인기 韓 등 6개국 부품 사용… 정찰총국 소행" Seoul Shinmun, June 21, 2017. https://www.seoul.co.kr/news/politics/diplomacy/2017/06/22/20170622002009; "S.Korea launches jets, fires shots after North flies drones," National Public Radio, December 26, 2022. https://www.npr.org/2022/12/26/1145530094/s-korea-launches-jets-fires-shots-after-north-flies drones#:~:text=The%20military%20responded%20by%20firing,according%20to%20the%20Defense%20Ministry.

46 Ibid.

47 "S Korea considering buying Israeli drone detection system: source," Yonhap News Agency, January 08, 2023. https://en.yna.co.kr/view/AEN20230108000900325?section=nk/nk.

Political Control of the RGB

The ultimate objective of the RGB is to create a revolution in South Korea and foster unification of the peninsula under the Kim regime.[48] The KWP Organization and Guidance Department (OGD), the most powerful of all KWP departments, ensures it does so.

Throughout training and field operations, every member of the RGB is politically controlled by the OGD. It is a department that politically and ideologically organizes and guides all North Korean institutions. Every intelligence agency, regardless of type, is controlled by the 11th Section of the OGD through the KWP committee embedded in that agency. There is a political department (정치부) staffed with GPB political officers assigned to each intelligence agency headquarters.

The RGB is no exception, and each RGB commander has a senior political staff officer assigned to serve alongside them. This political officer is usually more influential on RGB issues other than pure intelligence tasks. Besides conducting political indoctrination, inspections, and evaluations of individual loyalty to the Kim regime, the political officer at every level of the RGB controls personnel assignments. The OGD monitors the ideological life of every RGB operative and reports on their collective and individual performance to the Supreme Leader as necessary, a process critical to the Supreme Leader's direct operational control.[49]

48 Yoo Dong-yol, "북한 정찰총국 해부 (Analyzing North Korea's Reconnaissance General Bureau)," kild.or.kr, July 26, 2019. https://www.kild.or.kr/bbs/board.php?bo_table=activity_08&wr_id=30.

49 Il-Gi Kim and Ho-hong Kim, "김정은 시대 북한의 정보기구" [North Korean Intelligence Organizations in the Kim Jong-un Era], inss.re.kr, December 31, 2020, 85-88. https://inss.re.kr/publication/bbs/rr_view.do?nttId=409818, Dong-yol Yoo, "북한 정보기구의 변천과 현황 (North Korean Intelligence Organizations Change and Status), 178. https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002354345.

Section 4: RGB's History of Provocations Against South Korea

North Korea has a long history of carrying out both kinetic and non-kinetic provocations against South Korea. These provocations have occurred since the division of the peninsula, where the RGB and its predecessors have played a central role in these tactical operations. The purpose of these provocations has been to undermine the South Korean government, which the Kim regime sees as a direct threat to the North's own existence. It is evident that the Kim regime sees these provocations as furthering the regime's policy objectives. Indeed, these provocations disrupt the South Korean public's confidence in their own government and spread fear of violence between the two Korean states.

The type and number of provocations have varied over the decades since the peninsular division. North Korean provocations against South Korea in the 1960s, 1970s, and 1980s focused on infiltration of South Korea, assassinations, abductions, and sabotage. However, nuclear weapons testing, ballistic missile launches, and cyber warfare have become the dominant provocations since the turn of the century. The RGB and its predecessor components have played an integral role in the military aspects of these efforts through espionage, sabotage, terrorism, cybercrime, and cyber warfare.

North Korean provocations have gone through five distinct periods in terms of focus and technical capability, with the RGB and its predecessors adapting to each of them. The 1960s through 1972 focused primarily on direct military assaults and localized terrorism along the DMZ with the KPA Reconnaissance Bureau playing the predominant role. During the period from 1973 to 1982, North Korea focused on diplomatic use of limited force but shifted to focus on terrorism between 1983 and 1992. The period of 1993 to 2000 was dominated by the combination of diplomatic and military operations.[50] However, from 2000 to present, the RGB's cyber warfare has dominated North Korean efforts.

During the period between the founding of the North Korean state in September 1948 and the outbreak of the Korean War in June 1950, North Korea initiated ten significant provocative infiltrations into South Korea using more than two thousand Kangdong Political College graduates.[51]

Some success was achieved in gaining local sympathy for North Korea in the Kangwon Province area, but no such success occurred during the Korean War. Reportedly the predecessor of the RGB, the 766th Independent Reconnaissance Regiment was activated during this time. At the Hoeryong Cadres School, which replaced the Kangdong Political College, the 766th was

50 Narushige Michishita, "Calculated Adventurism: North Korea's Military-Diplomatic Campaigns," Korean Journal of Defense Analysis 16, no. 2 (2004).

51 Kangdong Political College was led by South Korean communist Pak Hon-yong. It trained graduates to infiltrate into South Korea to lead revolutionary uprisings against the South Korean government.

trained by O Jin-u, who eventually became the KPA commander under Kim Jong-il in the 1990s. The 766th was successful in operating in the Kangwon Province area.[52]

After the Korean War in the 1950s, the Kim regime focused on consolidating power by eliminating political factions considered a threat to Kim Il-sung. As a result, North Korea engaged in few provocations against the South during that period.

However, in the 1960s, the North Korean military took the lead in anti-South operations of all types. The KPA Reconnaissance Bureau, one of the many predecessor elements of the RGB, was the main actor in conducting these provocations. Most of these provocations took place along the DMZ, at the Joint Security Area in Panmunjom, or along South Korea's east and west coasts. However, the actions of the KPA Reconnaissance Bureau were not carried out in defense of North Korea. Unsurprisingly, they were expended at the whim of North Korea's Supreme Leader. In October 1966, Kim Il-sung stated that the U.S. military was "dispersed to the maximum everywhere and on every front of the world."[53] North Korea's defense treaties with the Soviet Union and China gave the Kim regime some assurance that there was a deterrent factor when directing provocations at the South Korea-U.S. Alliance. The U.S. involvement in Vietnam at the time was also an important factor in the Kim regime's strategy. Domestically, these provocations enhanced Kim Il-sung's prestige.[54]

During the Korean War and during many of the land and-sea-based provocations, North Korean brutality against South Korean citizens was overwhelmingly evident. The North Korean slaughter of Christians when withdrawing from Seoul is a notable example. When General MacArthur successfully conducted the landing at Incheon in September, the KPA began to withdraw from South Korea to avoid getting trapped and surrounded by United Nations Command forces. But as the KPA withdrew, they massacred 1,026 Protestants and 119 Catholics because they were considered "reactionary forces."[55]

Frequently referred to as the Second Korean War, North Korea's aggression against South Korea and the South Korea-U.S. Alliance forces in the late 1960s resulted in numerous killed-in-action and wounded-in-action soldiers, both South Korean and American. Many South Korean civilians suffered similar fates also. In the 1960s, 928 North Korean infiltrations of South Korean territory via land and sea resulted in the deaths of 75 U.S. soldiers, with 112 wounded. 321 South Korean soldiers were also killed and 566 wounded. There were 645 North Korean soldiers killed and 147 known to be wounded. In the 1970s, 255 infiltrations/provocations resulted in seven U.S. soldiers killed and 12 wounded. The South Korean soldiers killed numbered 38, and the wounded 69. North Koreans suffered 108 deaths and 11 known wounded. In the 1980s, 29

52 Joseph S. Bermudez, Jr., North Korean Special Forces, 25, 34-35.

53 Narushige Michishita, North Korea's Military-Diplomatic Campaigns, 1966-2008 (Routledge: New York; 2010), 17.

54 Ibid, 31.

55 Cheong-mo Yoo, "N.Korea massacred over 1,100 Christians, Catholics during Korean War: report," Yonhap, February 22, 2022. https://en.yna.co.kr/view/AEN20220222002800315?section=search.

infiltrations/provocations resulted in no deaths or wounded among the Americans, with South Korea suffering five deaths and 13 wounded. North Korea suffered 37 deaths and three known wounded. In the 1990s, 31 land and sea infiltrations resulted in zero deaths or wounded among American soldiers, zero deaths and 11 wounded among South Korean soldiers, and roughly 65 deaths on the North Korean side.[56]

Assassinations

Arguably, the most infamous terrorist provocation against South Korea was a raid launched by North Korean commandos on January 21st, 1968, to assassinate the South Korean President Park Chung-hui in his residence at the Blue House. Following orders from KPA Lieutenant General Kim Chung-tae, who instructed them to "go to Seoul and cut off the head of Park," 31 armed commandos belonging to Unit 124 of the KPA Reconnaissance Bureau, equipped with South Korean military uniforms, grenades, and submachine guns, crossed the DMZ and infiltrated the Seoul metropolitan area at midnight on January 17th. Over the next eight days the commandos engaged in numerous firefights with South Korean and U.S. forces. Four U.S. soldiers and 26 South Korean soldiers were killed in action while 66 South Korean personnel, including 24 civilians, were wounded.[57] The sweeping operation against them continued until January 31st. In the end, 28 of the 31 commandos were killed, Kim Shin-jo was arrested, and two of them fled to North Korea. One of those that returned was General Park Jae-kyung, who rose to be the deputy director of propaganda of the KPA GPB. President Park was unharmed.[58]

56 Narushige Michishita, North Korea's Military-Diplomatic Campaigns, 1966-2008 (Routledge: New York; 2010), 17. https://www.routledge.com/North-Koreas-Military-Diplomatic-Campaigns-1966-2008/Michishita/p/book/9780415666893?srsltid=AfmBOopV5xcIANJHm7nxd5jprV-sREaQKhmIhO8U-dQFUlXHiI49dd-R.

57 Mike Coppock, "The Korean War That Almost Was," HistoryNet, undated, accessed February 23, 2022. https://www.historynet.com/the-korean-war-that-almost-was/?f.

58 Kwang-jin Kim, North Korea's Terror Organizations and Their Possible Provocation (북한의 대남테러 조직 및 테러전망), 76. https://www.inss.re.kr/activity/bbs/academic_view.do?nttId=405324&bbsId=academic&page=10&searchCnd=0&searchWrd=.

A map of the invasion route is depicted on the below.[59]

Figures 4 and 5, Source: Park Sun-yeong, "N. Korea threatens use of weapons to control border with China," Korea Joongang Daily, March 29, 2009. https://koreajoongangdaily.joins.com/2009/03/29/features/A-lethal-trail-to-the-Blue-House/2902872.html.

In June of 1970, North Korea made its second attempt at assassinating President Park. Three North Korean operatives infiltrated South Korea, and after arriving in Seoul, they planted a remote-controlled bomb at the South Korean National Cemetery front gate before President Park was due to arrive to make a speech. However, the assassination attempt failed when the bomb exploded prematurely.[60]

The third North Korean attempt to assassinate the South Korean President happened on August 15th, 1974, when Mun Se-kwang murdered President Park's wife, Yuk Young-su, while trying to shoot President Park as he was giving a speech in Seoul. Mun was recruited by North Korea through contacts in the Chosen Soren, a pro-North Korea group of Koreans living in Japan. Mun, a Korean born in Japan and a well-known North Korean sympathizer, was provided a false passport by his North Korean handlers and smuggled in a stolen .38 caliber pistol into South Korea to conduct the assassination attempt. He was arrested, convicted of murder, and executed by the South Korean authorities.[61]

---

59 Sun-young Park, "A Lethal Trail to the Blue House." Korea Joongang Daily, March 29, 2009. https://koreajoongangdaily.joins.com/2009/03/29/features/A-lethal-trail-to-the-Blue-House/2902872.html.

60 Narushige Michishita, North Korea's Military-Diplomatic Campaigns, 1966-2008, 17.

61 Michael Keon, Korean Phoenix: A Nation from the Ashes. Prentice-Hall International, 1977, 199 https://archive.org/details/koreanphoenixnat00keon; Don Oberdorfer, The Two Koreas: A Contemporary History. Reading: Addison-Wesley, 1997, 53-57 https://archive.org/details/twokoreascontemp00ober.

Figure 6, Source: North and South Development, [Special Feature on National Liberation Day of Korea], North and South Development, August 16, 2024.

In the fourth North Korean attempt to assassinate a South Korean President, President Chun Doo-hwan was targeted while he was visiting Burma (now Myanmar). The attack took place at the Aung San Cemetery on October 9th, 1983. A bomb was placed in the shrine by three North Korean special forces members, including Shin Ki-cheol. The bomb exploded while the South Korean delegation was visiting the cemetery, killing 17 South Korean government ministers and attendants, including Deputy Prime Minister Seo Seok-jun, Foreign Minister Lee Beom-seok, and Minister of Commerce and Industry Kim Dong-hwi, while injuring dozens of others.

President Chun, who was on an official tour to five Southeast Asian countries, was thirty minutes late due to traffic congestion and a scheduling conflict. Burma, enraged at this, immediately cut off diplomatic relations with North Korea. Among the three criminals, Shin Ki-cheol was shot and killed, and Kim Jin-soo and Kang Min-cheol were arrested. Kim Jin-soo was executed in 1986, and Kang Min-cheol died of severe liver disease on May 18th, 2008 at the age of fifty-three while serving his life sentence in a Myanmar jail.

North Korea insisted to the end that it was not their actions. South Korea also rejected Kang Min-cheol's possibility of naturalization.[62]

62 Kwang-jin Kim, North Korea's Terror Organizations and Their Possible Provocation (북한의 대남테러 조직 및 테러전망) 79. https://kiss.kstudy.com/DetailOa/Ar?key=50168279.

There was one other unsuccessful attempt to kill the South Korean President. In 1981, North Korea hired two Canadians, Charles Yanover and Alexander Gerol, to kill South Korean President Chun Doo-hwan on his planned visit to the Philippines. The two were arrested before the attempt took place.[63]

On February 13th, 2017, Kim Jong-nam, the elder half-brother of Kim Jong-un, was assassinated at the Kuala Lumpur International Airport in Malaysia. Two women, one from Indonesia and one from Vietnam, were duped by North Korean agents into believing they were acting for a TV part. The women used rags soaked with the two elements of VX, a highly toxic binary chemical poison, to smother Kim from behind. He died within a few minutes.[64] One of Japan's leading newspapers, the Asahi Shimbun, reported that Section 19 of the RGB's 2nd Bureau led the operation assassinating Kim Jong-nam. It also reported that Section 19 specializes in operations using poison for assassinations. However, one North Korean defector has insisted that Section 19 does not exist.[65]

RGB defector Colonel Kim Kuk-song (alias) insisted that the Kim regime leadership ordered the formation of a "terror task force" that would conduct the assassination of Hwang Jang-yop. Colonel Kim stated that he personally ordered the operation. In 2010, North Korea sent three spies to South Korea to assassinate Hwang Jang-yop, the highest ranking North Korean escapee. Prior to Hwang's escape from North Korea in 1997, he served as the North Korean Chairman of the Standing Committee of the Supreme National Assembly. Known as the father of Juche ideology, Hwang was ranked 22nd in the Kim regime protocol ratings. Upon his defection through China and the Philippines, Hwang was considered by the Kim regime to be the ultimate traitor, and thus his death was ordered. The three RGB operatives – Dong Myong-kwan, Kim Myong-ho, and Lee Dong-sam – failed in their attempt to assassinate Hwang. Two were arrested and are now serving time in South Korean jails. Dong Myong-kwan and Kim Myong-ho held the military rank of major and were assigned to the RGB.[66]

---

63 "Database: North Korean Provocations," Beyond Parallel, December 20, 2019. https://beyondparallel.csis.org/database-north-korean-provocations/.

64 Kyodo, "Kim Jong-nam, half-brother of North Korean leader, met with suspected U.S. spy days before he was killed, court hears," SCMP, January 29, 2018. https://www.scmp.com/news/asia/east-asia/article/2131104/kim-jong-nam-half-brother-north-korean-leader-met-suspected-us.

65 Choi Woo-suk, " 정찰총국 해외정보국에서 김정남 암살" [Assassination of Kim Jong-nam by the Reconnaissance General Bureau's Overseas Intelligence Bureau], Monthly Chosun, May 2017. https://monthly.chosun.com/Client/News/print.asp?ctcd=G&nNewsNumb=201705100040.

66 Laura Bicker, "Drugs, arms, and terror: A high-profile defector on Kim's North Korea," BBC, October 11, 2021 https://www.bbc.com/news/world-asia-58838834; "The General Bureau is the 'headquarters of operations against South Korea' that integrates the Party Operations Department and the Military Reconnaissance Bureau." 〔출처:중앙일보〕 Korea Joongang Daily, April, 4, 2010. https://www.joongang.co.kr/article/4121510; See also Yang Man-soo, "황장엽 암살기도 지령내린 북한 정찰총국은 " [The North Korean Reconnaissance General Bureau, which ordered the assassination of Hwang Jang-yop], Today Korea April 14, 2021. https://www.todaykorea.co.kr/news/articleView.html?idxno=107567.

Yi Han-Yong, the nephew of Kim Jong-il's consort Sung Hye-rim, defected in 1982 to South Korea. He was assassinated in 1997 outside his Seoul apartment by North Korean operatives who were never caught.[67]

RGB assassination operations are not only directed at political-military targets. Pastor Han Chung-yol was a leader of Christian church in Changbai Korean Autonomous County, Jilin Province, China, near the North Korean border. He was known for supporting defections across the Yalu River. He was found stabbed to death nearby.[68]

North Korean defector, Colonel Kim Kuk-song, who served in a high position in the RGB, claimed in an interview with British media that a North Korean agent had infiltrated the South Korean Presidential Palace (known as the Blue House) in the early 1990s. The South Korean NIS insists that claim is groundless. Colonel Kim also insisted that a North Korean spy had served in the Blue House in the 1950s.[69]

Major Air Provocations

Over the decades, the Kim regime has chosen to commit air provocations on several occasions. Below is a list of some of those:[70]

» 1958: North Koreans hijack a South Korean airplane from Busan to Seoul. Kidnapped passengers numbered 28, all taken to Pyongyang.

» 1959: Two North Korean MiG jets attack a U.S. Navy patrol aircraft.

» 1964: U.S. Air Force aircraft attacked by North Korea near DMZ and pilots taken hostage for nearly one year.

» 1965: North Korean jets attack a U.S. reconnaissance plane over the East Sea.

» 1970: A North Korean agent hijacked Korean Airlines YS-11. 39 passengers were returned, but the plane's crew and seven other passengers were not.

» 1971: North Korean agent Kim Sang-tae attempted to hijack a South Korean airliner only to be killed by his own bomb, along with the co-pilot and 22 others.

» 1987: Korean Air Flight 858 was a scheduled international passenger flight between Baghdad, Iraq and Seoul, South Korea. On November 29th, 1987, the air-

67 Nadia Khomami, "North Korea: isolated State with a Long History of Assassinations," The Guardian, February 15, 2017. https://www.theguardian.com/world/2017/feb/15/north-korea-isolated-state-with-a-long-history-of-assassinations.

68 Ha-young Choi, "Korean-Chinese pastor-activist killed on North Korean border," NK News, May 2, 2016. https://www.nknews.org/2016/05/korean-chinese-pastor-activist-killed-on-north-korean-border/.

69 YTN News, "탈북자 '90년대초 청와대에 남파간첩 근무' …국정원 '사실무근'" [North Korean Refugee 'Working as a South Korean spy at the Blue House in the early 1990s'...NIS 'groundless'), youtube.com, October 11, 2021 https://www.youtube.com/watch?v=Q9w0GCfPDTE&list=PLG0wy_ZMVm9Ybr8asUTmSG3OJ28KpcVBT&index=10.

70 "Database: North Korean Provocations," Beyond Parallel.

craft flying that route exploded in mid-air upon the detonation of a bomb planted inside an overhead storage bin in the airplane's passenger cabin by two North Korean agents. The male agent committed suicide and the female agent, Kim Hyon-hui, was captured.

Major Naval Provocations

The Kim regime has also committed naval provocations, including those listed below:[71]

- 1967: South Korean PCE-56 patrol boat sunk in the East Sea by North Korean coastal artillery.
- 1968: The most notable naval provocation by North Korea is the capture of the U.S. Navy intelligence ship USS Pueblo in the East Sea, which led to the death of one American servicemember and the yearlong captivity of the surviving crew.
- 1970: South Korean Navy sinks North Korean espionage ship.
- 1974: North Korea sinks South Korean fishing boats; 12 South Koreans die.
- 1974: Three North Korean ships sink South Korean coast guard ship; 28 die.
- 1996: North Korea sent a Sango-class submarine filled with infiltration agents to the coast of Kangnung in the northeast Province of Kangwon, South Korea. The agents were stranded as the submarine became stuck on the shoals along the shore, and its mission was never accomplished. After the crew and infiltration agents disembarked, the agents killed the crew and attempted to exfiltrate back to the North. Of the 26 North Korean agents, 24 died, one was captured, and the last was never found.[72]
- 1999: The first Yeonpyeong Island naval clash between North Korean Navy ships and the South Korean Navy. One North Korean ship was sunk and there were casualties on both sides.
- 2002: The second Yeonpyeong Island naval clash resulted in North Korea sinking a South Korean naval vessel with several casualties on both sides.
- 2010: North Korea sinks the ROKS Cheonan in April and bombards Yeonpyeong Island in November.
- Over the decades, there were numerous sinkings of North Korean infiltration boats by South Korean naval patrols.

71 "Database: North Korean Provocations," Beyond Parallel.

72 Stephen Silver, "North Korea's Spy Strategy: Pose as Defectors," nationalinterest.org, January 22, 2022. https://nationalinterest.org/blog/reboot/north-koreas-spy-strategy-pose-defectors-199480.

Abductions

North Korea has a long history of abducting South Korean citizens and taking them back to the North. Over six decades, a total of at least 108 South Korean citizens have been kidnapped and brought to the North. Although not part of RGB operations, North Korea's KPA abducted 82,959 South Koreans during the first four months of the Korean War. Since the end of the Korean War, there have been more cases of abductions of South Koreans, either crew members of fishing boats hijacked by the North Korean Navy or those kidnapped by North Korean infiltrators operating along the South Korean coastlines. The North Korean Navy, the RGB, and the RGB's predecessor have abducted 3,824 South Koreans, 3,721 of whom were fishermen.

Before that, more than 93,000 Koreans who were compelled to work in Japan during Japan's 1910-1945 occupation of the Korean Peninsula were persuaded to return to North Korea during the 1960s and 1970s. Once there, they were regarded as untrustworthy. Many of the abducted South Koreans subsequently served as advisors on South Korean political culture to train RGB operatives on how to infiltrate South Korea. Abducted non-Koreans, including Japanese nationals, also provided language training to RGB operatives for overseas operations.

Figure 7, Source: Kim Chae Hwan, "南탈북 가족 때문에… 김정일정치군사대학 졸업생, 전투원 임명 배제 [Because of family members who defected to the South… Graduates of the Kim Il Sung Political-Military University excluded from appointment as combat troops]," Daily NK, January 25, 2022. https://www.dailynk.com/20220125-4/.

South Korean citizens who were kidnapped by North Korean agents in South Korean territory or foreign countries after the armistice was signed in 1953 are known as postwar abductees. Most of them were captured while fishing near the Korean DMZ, but some were abducted by North Korean agents in South Korea. North Korea continued to abduct South Koreans into the 2000s, as is shown by the cases of the Reverend Kim Dong-shik who was abducted on January 16th, 2000. Additionally, Jin Gyeong-suk, a North Korean defector who had resettled in South Korea, was abducted on August 8, 2004, after returning to the China–North Korea border area using her South Korean passport.

Abductions of Japanese citizens from Japan by North Korea took place from 1977 to 1983. Although only 17 Japanese (eight men and nine women) are officially recognized by the Japanese Government as having been abducted, there may have been hundreds of others. The North Korean government has officially admitted to abducting 13 Japanese citizens. Approximately 200 Chinese of Korean ethnicity were abducted and brought to North Korea, and about 25 other foreign nationals were abducted worldwide.[73]

Japanese groups estimate 100 Japanese were kidnapped by the North. In addition to South Korea and Japan, at least 12 other countries have been identified as having had one or more of their citizens kidnapped by the North.[74]

One of the more bizarre abduction incidents conducted by the Kim regime was the kidnapping of South Korean actress Choi Eun-hui and movie director Shin Sang-ok. Choi was lured to Hong Kong where she was forced to board a boat and was subsequently transported to North Korea, where she directly met the young Kim Jong-il, known for his addiction to movies. Once Shin realized Choi was not coming back from Hong Kong, he went there himself, only to be kidnapped and, like Choi, was transported by boat to North Korea. When both arrived, they were welcomed to the "socialist fatherland." Kim Jong-il asked them to seek financing in Austria for a movie in 1986. While there, they escaped their minders, sought refuge at the U.S. embassy in Vienna, and then returned to South Korea.[75]

Espionage

There are numerous incidents of North Koreans spying on South Korea. Between 1953 and 1980, the South Korean military detected 5,500 North Korean spies. During the same period, the South Korean military and police captured or killed 2,973 North Korean operatives.[76]

---

73 "Taken! North Korea's Criminal Abduction of Citizens of Other Countries," Yoshi Yamamoto, HRNK, 2011. https://www.hrnk.org/uploads/pdfs/Taken_LQ.pdf.

74 Ibid.

75 Ibid; Larry Getlen, "How North Korea's dictator once kidnapped stars to make movies" New York Post, January 18, 2015.https://nypost.com/2015/01/18/how-north-koreas-dictator-once-kidnapped-stars-to-make-movies/.

76 북한/대남 도발, National Intelligence Service, https://www.nis.go.kr/AF/1_1_1.do .

One of the more famous was the Wangjaesan group of five North Korean spies who were under orders from North Korea's 225th Bureau (now the Cultural Exchange Bureau) operating in South Korea. The group was captured by South Korean authorities in 2011. The Wangjaesan group, given the honorific name of Daeho-myeong by the Kim regime, attempted to infiltrate the upper echelons of the South Korean political structure. This included the Office of the Secretary to the Speaker of the South Korean National Assembly. Wangjaesan reported back to the Kim regime on the movements of Presidents Lee Myung-bak and Roh Moo-hyun, Presidential Palace aides, the South Korean Democratic Party, and liberal organizations. Wangjaesan was also ordered to be prepared to destroy major infrastructure facilities in the Incheon area and to strike South Korean Army units south of Panmunjom and Munsan.[77]

Even at the time of the Wangjaesan espionage incident in 2011, it was revealed that the 225th Bureau had ordered the underground party members to "abolish the National Security Law and participate in the fight against mad cow disease in order to rally anti-government and anti-American forces." 2,000 members of the National Democrats' Union participated in the 'Pre-Conference of the Federation of Trade Unions' during the demonstration. The National Democrats' Union is a non-regular labor union of local governments, which includes environmental cleaners and road maintenance workers.[78]

North Korea specifically focuses on recruiting North Korean escapees living in South Korea to report to the Kim regime on informational and intelligence matters, along with recruiting other North Korean escapees to provide information to the Kim regime. They do so by manipulating the escapee's relationships with relatives still living in the North.[79] A North Korean intelligence service, presumably the RGB, recruited a North Korean escapee living in South Korea to provide personal information about other escapees living in South Korea, as well as their families in North Korea. South Korean counterintelligence services arrested this escapee who gave the information to North Korea, and he was sentenced to three years in prison.[80]

77 Jeong-hwan Kim, "북한225국 지령 받는 간첩단 왕재산 적발" [North Korea's 225 Bureau Gives Orders to Spy Group's Wangjaesan], Nodongilbo, September 3, 2011. https://www.nodongilbo.com/news/articleView.html?idxno=7527.

78 Dong-hyeon Pak, "<간첩협의 목사> 북한의 225국에 직접 연계 적발은 최초" [Spy Pastor: The first direct link to North Korea's 225th Bureau], PE News, November 24, 2015. https://www.penews.co.kr/news/articleView.html?idxno=1101.

79 Ifang Bremer, "Second North Korean defector this year found guilty of spying for Pyongyang," NK News, May 13, 2022. https://www.nknews.org/2022/05/second-north-korean-defector-this-year-found-guilty-of-spying-for-pyongyang/.

80 Ifang Bremer, "How a North Korean defector was coerced into spying for Pyongyang," NK News, May 3, 2022, https://www.nknews.org/2022/05/how-a-north-korean-defector-was-coerced-into-spying-for-pyongyang/.

Demilitarized Zone Tunnels

Kim Il-sung ordered the construction of tunnels under the DMZ in 1971 after the fortification of that zone that separated the North from the South. Kim believed that "one tunnel can be more powerful than ten atomic bombs put together and the tunnels are the most ideal means of penetrating the South's fortified front line."[81]

The four tunnels that were discovered were designed to enable thousands of North Korean infantry to pass under South Korean defenses and increase the North's subsequent offensive advantage on the forward edge of the battlefield. The location and functionality of the four North Korean tunnels were:

- The first tunnel was discovered November 15th, 1974, 8 km north of Korangpo (directly north of Seoul); the tunnel width was 0.9 m, capable of accommodating one infantry regiment.
- The second tunnel was discovered March 19th, 1975, 13 km north of Chorwon; the tunnel width was 2 m and was capable of accommodating 8,000 infantrymen per hour, in addition to heavy equipment.
- The third tunnel was discovered October 17th, 1978, 4 km south of Panmunjom; the tunnel width was 2.1 m; accommodation unknown.
- The fourth and last tunnel was discovered March 3rd, 1990, 26 km north of Yanggu on the central-east front; the tunnel width was 1.7 m and was capable of accommodating one infantry regiment.[82]
- There were several other areas along the DMZ that were suspected of being dug by the North Koreans but were discontinued (presumably) due to South Korea-U.S. Alliance detection.[83]

81 ROK Defense White Paper, 1990, 75; as cited in Joseph S. Bermudez, Jr., North Korean Special Forces, 251.
82 Joseph S. Bermudez, Jr., North Korean Special Forces, 253.
83 Megan Specia, "Built for Invasion, North Korean Tunnels Now Flow With Tourists", New York Times, November 4, 2017. https://www.nytimes.com/2017/11/04/world/asia/north-korea-south-korea-demilitarized-zone-tunnel-tourism.html.

Section 5: RGB Cyber Warfare

In 2009, the United Nations warned that the next great war would be a cyber war. Today, this proves particularly true. Cyber warfare is often referred to as the fifth warfighting domain after land, sea, air, and outer space. It is comprised of command-and-control warfare, military intelligence warfare, electronic warfare, psychological warfare, economic information warfare, hacking warfare as well as cyber warfare itself.

The RGB's cyber warfare capabilities, organizational structures, tactics, and techniques have evolved significantly since 2009. North Korea's current cyber activities are focused on three strategic purposes: causing disruption, conducting espionage, and generating revenue. Cyber operations are thought to be a cost-effective way for North Korea to maintain an asymmetric military option, as well as to gather intelligence. So, as the significance of cyber warfare increased, so did the importance of the RGB's role in national defense and in supporting the Kim regime. RGB hackers are highly motivated, largely because they receive relatively high compensation compared to much of the population.

The groundwork for North Korea's cyber operations was laid in the 1990s, when North Korean computer scientists, after returning from overseas, proposed using the Internet as a tool for espionage and for launching attacks against militarily superior adversaries like the United States and South Korea. Subsequently, students were sent abroad to China to study and participate in top computer science programs.

The RGB's primary intelligence targets are South Korea, Japan, and the United States.[84] After the U.S. military operations commenced in Iraq, North Korea elevated its cyber warfare unit to its top priority[85] and the North's cyber warfare has grown significantly over the past two decades. The RGB's cyber warfare has been effective in the areas of foreign affairs, cybercrime, and security. Through its cyber warfare, the RGB conducts hacking operations, deception operations, and psychological operations, with little risk of exposure to third countries. The RGB conducts cyber operations through its cyber warriors posing as third-party, non-state actors employing plausible deniability so that there is no connection to the Kim regime, the North Korean government, or the KWP.[86]

---

84 Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the Democratic People's Republic of Korea." 2013. https://irp.fas.org/world/dprk/dod-2013.pdf.

85 David E. Sanger, David D. Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More," New York Times, October 15, 2017. Accessed January 1, 2022. https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

86 Pil-jae Kim, 북한의 사이버 남침 (North Korea's Cyber Invasion of the South), Seoul: Baeknyun Dongahn, 2014. 15-16.; Il-Gi Kim and Ho-hong Kim, "김정은 시대 북한의 정보기구" [North Korean Intelligence Organizations in the Kim Jong-un Era], inss.re.kr, December 31, 2020, 91. https://inss.re.kr/publication/bbs/rr_view.do?nttId=409818.

Kim Jong-un graduated from Kim Il-sung Military College with a senior thesis focused on GPS targeting of artillery. Reportedly, Kim led a DDOS attack in 2009 against South Korea, the success of which Kim Jong-il used as justification to promote Kim Jong-un to the rank of four-star general.[87] Today, GPS jamming is one of North Korea's preferred cyber warfare techniques, and North Korea consistently jams South Korean naval ships, aircraft and communications.[88]

North Korean cyber operations are generally overseen by three entities:

» The RGB, which carries out the bulk of North Korea's cyber operations.

» KPA General Staff Department's Command Automation Bureau, which oversees cyber program development and cyber warfare integration.

» The UFD, which conducts cyber operations targeting the South Korean population.

According to South Korean Government analysis, North Korea has approximately 5,900 "cyber warriors." Different sources peg this number slightly higher or slightly lower, and it is unclear whether this number refers exclusively to operational cyber units or if it includes staff and support members.[89] The U.S. National Security Strategy Institute has estimated that, as of 2016, North Korea had about 1,700 specialized hackers in seven different hacking organizations. There are 13 hacking support organizations comprising approximately 4,200 personnel.[90]

According to the Central Intelligence Agency (CIA), North Korea has 12,000 personnel that support the North's cyber operations. When combined with research centers, this number reaches 30,000.[91]

Kim Jong-un has been quoted by the KPA as stating, "If the internet is like a gun, cyber-attacks are like atomic bombs."[92] North Korea has also expanded RGB cyber warfare to focus on bank and cryptocurrency theft, ransomware, military and government systems hacking, psychological operations, and individual email targeting. The RGB employs malicious cyberwarfare to collect intelligence, conduct attacks, and produce revenue worldwide, but the organization is primarily aimed at South Korea. North Korea is utilizing cyberspace as a tool to advance its vision of establishing a global Juche ideology.

87 Pil-jae Kim, 북한의 사이버 남침 (North Korea's Cyber Invasion of the South), 23.
88 Ibid, 76.
89 Jenny Jun, Scott LaFoy, and Ethan Sohn, "The Organization of Cyber Operations in North Korea," Center for Strategic and International Studies, December 18, 2014. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/141218_Cyber_Operations_North_Korea.pdf.
90 In-soon Kim, "North Korea's cyber-terrorism capabilities," Daum News, February 21, 2016. https://news.v.daum.net/v/20160221170027854.
91 Pil-jae Kim, 북한의 사이버 남침 (North Korea's Cyber Invasion of the South), 22.
92 Ed Caesar, "The Incredible Rise of North Korea's Hacking Army".

The RGB's cyberwarfare directly supports its resultant strategy of espionage, retaliation against political-military rivals, and monetary support of the Kim regime's nuclear and missile programs.[93] The Kim regime's strategic goal for the RGB's cyberwarfare has evolved from DDOS, to espionage, and to now being dominated by financial gain.[94] Since the 1990s, faced with economic challenges that hindered the expansion of its conventional military, North Korea has intensified efforts to enhance its cyber capabilities, recognizing their potential to deliver significant impact at a relatively low cost.[95]

Cyber warfare, by nature, is indirect and thrives on anonymity, making it challenging to detect attacks or identify the perpetrators. It is not confined to specific targets or timeframes. North Korea consistently denies any involvement in cybercrimes, with the Kim regime refusing to acknowledge wrongdoing. Since cyberattacks can occur in both wartime and peacetime, they provide North Korea with a powerful tool to advance its revolutionary agenda against South Korea.[96]

According to the South African organization Technolytics, North Korea ranks behind China (rated 4.2 out of 5), Russia (4.0), and Iran (3.4) in terms of cyberattack capabilities, with a score of 2.8.[97] Rating notwithstanding, cyber operations are thought to be a cost-effective way for North Korea to maintain an asymmetric military option, as well as to gather intelligence.

The RGB Technical Reconnaissance Bureau, previously known as the Electronic Reconnaissance Bureau, is responsible for a range of activities including hacking operations, cyber terrorism, cyber espionage, signal decoding, communications interception, infiltration technology, and anti-South Korean technical research—blending cyber and electronic warfare tactics. Oversight of RGB cyber operations falls under the 110th Research Institute (also referred to as the 110th Lab), which also manages the 31st Technical Reconnaissance Center, the 32nd Center, and the 56th Center. Additionally, the 128th Liaison Station and the 198th Liaison Station operate under its broader structure.[98] The 121st Bureau (formally known as the Technical Reconnaissance Team) and the 100th Research Institute together collect strategic information on South Korea and the United States. North Korea does not seem to have yet organized these units into an overarching Cyber Command.[99]

---

93 Chong Woo Kim and Carolina Polito, "The Evolution of North Korean Cyber Threats," The Asian Institute for Policy Studies, February 23, 2022. https://en.asaninst.org/contents/the-evolution-of-north-korean-cyber-threats/.

94 Ibid.

95 Pil-jae Kim, 북한의 사이버 남침 (North Korea's Cyber Invasion of the South), 9.

96 Ibid, 19.

97 In-soon Kim, "North Korea's cyber-terrorism capabilities," Daum News, February 21, 2016. https://news.v.daum.net/v/20160221170027854.

98 Kwang-jin Kim, North Korea's Terror Organizations and Their Possible Provocation (북한의 대남테러 조직 및 테러전망) 79. https://kiss.kstudy.com/DetailOa/Ar?key=50168279.

99 Jenny Jun, Scott LaFoy, and Ethan Sohn, "The Organization of Cyber Operations in North Korea," Center for Strategic and International Studies, December 18, 2014. https://csis-website-prod.s3.amazonaws.com/s3fspublic/legacy_files/files/publication/141218_Cyber_Operations_North_Korea.pdf.

North Korea's Korea Computer Center (KCC) was established on October 24th, 1990, with the assistance of the Chochong-ryon,[100] an organization of Koreans living in Japan who support North Korea. Reportedly, the KCC is also known as the Information Industry Guidance Bureau (the term guidance bureau strongly implies an affiliation with the KWP).[101] The KCC is responsible for North Korea's information industry and cyber warfare development. Located in the Mangyongdae district of Pyongyang, it operates under the authority of the North Korean General Bureau of Software Industry.

The facility employs more than 1,200 personnel, including 800 dedicated to research and development, with over 100 holding Ph.D. degrees. Many North Korean cyber warfare agents disguise themselves as employees of the KCC. The KCC's top experts are graduates of Kim Il-sung University, Kimchaek University of Technology, and the Pyongsong College of Science. The KCC has eight R&D centers, a doctoral program, an information technology university, a training program, and 11 regional information centers. The KCC has six administrative departments: financing, marketing, planning and production, research, legal, and other affairs.[102]

The KCC is comprised of eight research and development centers:

1. Odoksan Information Center: Develops "Red Star" and other Korean language programs, and it adapts "Windows" for North Korean application.
2. Mankyong Information Center: Develops North Korean intranet systems including the national intranet "Kwangmyong," the MSS' intranet "Shield," the KPA's intranet "Goldstar," and the Ministry of Social Safety's intranet "Red Sword."
3. Oun Information Center: Develops security programs for organizations that use the North Korean intranets.
4. Samilpo Information Center: Develops various personal digital assistance programs such as "Uri," "Mokran," "Hana," "Koryopen."[103]
5. Chongbyon Information Center: Develops automation for factories.
6. Subaeksu Information Center: Develops semiconductors.
7. Milyong Information Center: Treatment devices and information technology that will match up with health treatment methodologies.
8. Samjiyon Information Center: Develops games and multimedia products.[104]

---

100 Also known as Chosen Soren in Japan, this pro-North Korean organization is comprised of Korean residents in Japan.

101 Jin-kyu Kang, "베일에 쌓인 북한 정보산업성 (North Korea's Ministry of Information Industry in Veil)", NK Economy, July 7, 2021. https://www.nkeconomy.com/news/articleView.html?idxno=4440.

102 Seong Choi, "Korea Computer Center – The Core of North Korea's IT Strategy," Korea IT Times, November 4, 2010. http://www.koreaittimes.com/news/articleView.html?idxno=11397.

103 Martyn Williams, "North Korea Gets a New PDA," North Korea Tech, November 5, 2010. https://www.northkoreatech.org/2010/11/05/north-korea-gets-a-new-pda/.

104 Pil-jae Kim, 북한의 사이버 남침 (North Korea's Cyber Invasion of the South), 55-56.

The RGB's 121st Bureau is the lead organization focusing on the Kim regime's cyber operations. The number of RGB hackers in the 121st has grown from approximately 1,000 in 2010 to approximately 6,000 currently. The dominant subordinate elements of the RGB 121st Bureau are the Lazarus Group, the Bluenoroff Group, the Andariel Group, and the Electronic Warfare Jamming Regiment.

The Lazarus Group (undetermined number of hackers) focuses on social chaos in targeted countries' cyber systems. It places malware on targeted computers that lies dormant until desired conditions for activation are met, presumably during a crisis. The Bluenoroff Group had approximately 1,700 hackers in 2020 and focused on cybercrime. The Andariel Group had approximately 1,600 hackers in 2020 and targeted enemy computer systems. The Electronic Warfare Jamming Regiment is located in Pyongyang and commands three electronic warfare battalions, presumably located in Kaesong, Haeju and Kumgang.[105]

The Lazarus Group has also hacked the South Korean National Election Commission eight times in recent years. Since November 2022, the Lazarus Group has spread malicious code in 61 South Korean government institutions accessing 207 computers.[106] The South Korean Cybersecurity firm AhnLab Security Emergency Response Center has assessed that "The Lazarus Group is researching the vulnerabilities of various other software and is constantly changing its tactics, techniques and procedures by altering the way it disables security products and carries out anti-forensic techniques to interfere or delay detection and analysis in order to infiltrate South Korean institutions and companies."[107]

Hacking units of the 121st Bureau typically operate from locations outside North Korea. One known base is the Chilbosan Hotel in Shenyang, China.[108] Many RGB hacker elements operate in major Chinese cities such as Shenyang, Dalian, Guangzhou, and Beijing using trade companies as a front. They also conduct cyber gambling and game program development, as well as operating illegal cyber gambling businesses. Reportedly, these elements have earned approximately 100 million dollars for the Kim regime.[109]

105 North Korean Tactics (ATP 7-100.2), Washington, D.C., Department of the Army, 2020.
106 Tara O, "North Korea Hacks South Korea's National Election Commission," eastasiaresearch.org, May 11, 2023. https://eastasiaresearch.org/2023/05/11/north-korea-hacks-south-koreas-national-election-commission/.
107 Ravie Lakshmanan, "Lazarus Group Exploits Zero-Day Vulnerability to Hack South Korean Financial Entity," The Hacker News, March 8, 2023. https://thehackernews.com/2023/03/lazarus-group-exploits-zero-day.html.
108 Michael Daly, 'Inside the 'Surprisingly Great' North Korean Hacker Hotel,' The Daily Beast, December 20, 2014. https://www.thedailybeast.com/inside-the-surprisingly-great-north-korean-hacker-hotel.
109 "The General Bureau is the 'headquarters of operations against South Korea' that integrates the Party Operations Department and the Military Reconnaissance Bureau." [출처:중앙일보] Korea Joongang Daily, April, 4, 2010. https://www.joongang.co.kr/article/4121510.

Crypto businesses have recently been warned by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the U.S. Treasury Department to be cautious of North Korean hackers. These organizations specifically mentioned the Lazarus Group, APT38, BlueNoroff, and Starfall Chollima.[110] Furthermore, North Korean hackers from APT38 introduced a new ransomware variant designated "VHD" to support the Kim regime's cybercrime campaign.[111] The United States, Japan and Canada are favorite targets of Lazarus' energy hacking efforts.[112] Also known as TA444 group, RGB APT38 hackers stole more than $1 billion in cryptocurrencies and other blockchain holdings in 2022.[113] These cyber hacking efforts have proven to be an effective way to get around international sanctions against North Korea.[114] Additionally, the Lazarus Group stole $1.7 Billion in 2022 through several cyber theft attacks, exceeding the group's previous record for yearly success.[115]

RGB hackers employ malware to steal cryptocurrency. This is referred to by the U.S. Government as "AppleJeus." There are seven versions of AppleJeus. RGB hackers have targeted the following countries using AppleJeus malware: Argentina, Australia, Belgium, Brazil, Canada, China, Denmark, Estonia, Germany, Hong Kong, Hungary, India, Ireland, Israel, Italy, Japan, Luxembourg, Malta, the Netherlands, New Zealand, Poland, Russia, Saudi Arabia, Singapore, Slovenia, South Korea, Spain, Sweden, Turkey, the United Kingdom, Ukraine, and the United States. These hackers target energy, finance, government, industry, technology, and telecommunications.[116] North Korean RGB cyber actors have targeted organizations for cryptocurrency theft in over thirty countries in 2022 alone.[117]

On the next page is a map of countries that have been targeted by Applejeus malware:[118]

110 Vishal Chawla, "U.S. government warns that North Korea is targeting crypto firms," The Block, April 19, 2022. https://www.theblockcrypto.com/post/142478/us-government-warns-that-north-korea-is-targeting-crypto-firms?utm_source=rss&utm_medium=rss.

111 "New Ransomware Variant Linked to North Korean Cyber Army," Dark Reading, May 5, 2022. https://www.darkreading.com/threat-intelligence/new-ransomware-variant-linked-to-north-korean-cyber-army.

112 Cedric Pernet, "North Korean cyberespionage actor Lazarus targets energy providers with new malware," Tech Republic, September 14, 2022. https://www.techrepublic.com/article/lazarus-targets-energy-providers/.

113 Nate Nelson, "North Korea's Top APT Swindled $1B From Crypto Investors in 2022," Dark Reading, January 25, 2023. https://www.darkreading.com/remote-workforce/north-korea-apt-swindled-1b-crypto-investors-2022.

114 Ed Caesar, "The Incredible Rise of North Korea's Hacking Army."

115 Josh Smith, "Crypto hacks stole record $3.8 billion in 2022, led by North Korea groups – report," reuters.com, February 7, 2023. https://www.reuters.com/technology/crypto-hacks-stole-record-38-billion-2022-led-by-north-korea-groups-report-2023-02-01/.

116 "AppleJeus: Analysis of North Korea's Cryptocurrency Malware," Cybersecurity and Infrastructure Security Agency. April 15, 2021. https://www.cisa.gov/uscert/ncas/alerts/aa21-048a.

117 Ibid.

118 Da-gyum Ji, "Tale of North Korea's cyberterrorists: How they break into 'unbackable' crypto platforms and cash out," The Korea Herald, December 12, 2022. https://www.koreaherald.com/view.php?ud=20221212000714.

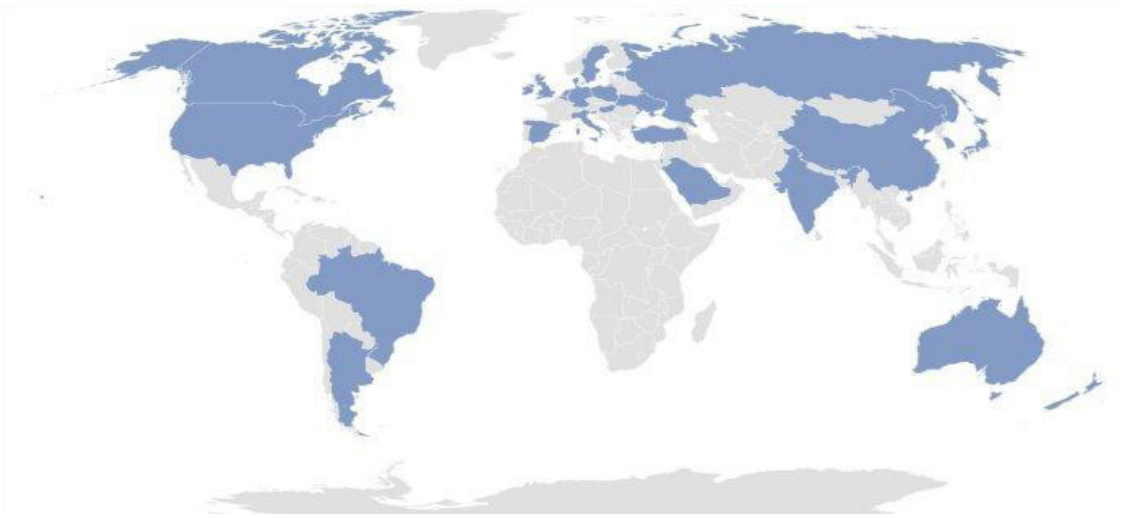


Figure 8, Source: Dagyum Ji, "Tale of North Korea's cyberterrorists: How they break into 'unhackable' crypto platforms and cash out", Korea Herald, December 12, 2022. https://www.koreaherald.com/article/3017774.

According to the U.S. Office of the Director of National Intelligence, "North Korea's cyber program poses a sophisticated and agile espionage, cybercrime, and attack threat. Pyongyang is well positioned to conduct surprise cyber-attacks given its stealth and history of bold action."[119] The White House has also stressed the need to improve cyber security in the face of RGB hacking success.[120]

Consistent with that assessment, North Korea has conducted cyber theft against financial institutions and cryptocurrency exchanges worldwide, potentially stealing hundreds of millions of dollars. The UN Panel of Experts on North Korea assessed that North Korean hackers had also stolen technical data about hypersonic missiles.[121] These experts also assessed that North Korean hackers' success at stealing money and cryptocurrency online is directly and indirectly supporting the Kim regime's nuclear and missile programs.[122] In its 2022 report, Harvard University's Belfer Center ranks North Korea first in the world at cybercrime (financial), 14th in overall cyber capability, but 30th in overall cyber defense.[123]

---

119 "Annual Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, February 7, 2022; 17.

120 Duk-kun Byun, "White House highlights cryptocurrency risks, citing N.Korean cyber theft," Yonhap, January 28, 2023. https://en.yna.co.kr/view/AEN20230128000200325?section=news.

121 Nils Weisensee, "Hackers likely helped North Korea build hypersonic missile: United Nations report," NK News, February 8, 2022. https://www.nknews.org/2022/02/hackers-likely-helped-north-korea-build-hypersonic-missile-un-report/.

122 Jason Bartlett, "Following the Crypto: Using Blockchain Analysis to Assess the Strengths and Vulnerabilities of North Korean Hackers," Center for a New American Security, February 2022. https://www.cnas.org/publications/reports/following-the-crypto.

123 Julia Voo, Irfan Hemani, and Daniel Cassidy, "National Cyber Power Index 2022," Harvard Belfer Center, September 2022. https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf.

Eric Penton-Voak, coordinator on the Panel of Experts on UN Security Council sanctions against North Korea, stated: "We see that DPRK (North Korea) cyber actors always go to the weakest point. They look at non-regulated areas. They look at really interesting and very gray, new areas of cryptocurrency because actually, A, no one really understands them, and B, they can exploit weakness."[124] North Korea's thefts of cryptocurrency fell between 2018 and 2020, but the total value of such thefts increased between 2019 and 2021. In its 2022 Crypto Crime Report, cryptocurrency analysis company Chainalysis stated that North Korean hacking organizations stole $400 million in digital assets in 2021. Additionally, North Korea stole $300 million worth of digital currency in 2020.[125]

According to Chainalysis, the Kim regime has carried out at least seven cyberattacks on cryptocurrency sites in efforts to pilfer the aforementioned $400 million from the United States.[126] Chainalysis also identified the RGB's Lazarus Group as the primary North Korean hacking threat.[127] Perhaps best known for its attack on Sony Pictures in 2014, the Lazarus Group has been conducting cybercrimes for the Kim regime since 2010. In 2015 alone, the group stole 1 million U.S. dollars from the Tien Phong Bank in Vietnam and 12 million U.S. dollars from the Banco del Austro in Ecuador.[128] Furthermore, the U.S. FBI reported that Lazarus group members stole Ethereum[129] worth $620 million from Axie Infinity, a blockchain-based video game, to further pad their bank accounts.[130]

According to RGB defector Colonel Kim Kuk-song (alias), North Korean cyberhackers are desperate to secure money in any manner they can.[131] In 2019, officials from the United Nations announced North Korea had amassed $2 billion through cyber-attacks alone.[132]

---

124 Duk-kun Byun, "N.Korea increasingly relies on cyber crimes to fund weapons programs: U.N. expert," Yonhap, April 21, 2022. https://en.yna.co.kr/view/AEN20220421000200325?section=nk/nk.

125 Sung-mi Ahn, "NK hackers stole $400m in cryptocurrency last year: report," The Korea Herald, March 20, 2022. http://www.koreaherald.com/view.php?ud=20220320000127&ACE_SEARCH=1.

126 "North Korean hackers stole $400m in digital assets last year, says report," The Guardian, January 14, 2022. https://www.theguardian.com/world/2022/jan/14/north-korean-hackers-stole-400m-in-digital-assets-last-year-says-report.

127 Michael Lee, "North's hackers cash in on cryptocurrency," Korea JoongAng Daily, February 17, 2022. https://koreajoongangdaily.joins.com/2022/02/17/national/northKorea/blockchain-cryptocurrency-North-Korea/20220217175935352.html.

128 A.L. Johnson, "SWIFT attacker's malware linked to more financial attacks," Broad Community, May 26, 2016. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8ae1ff71-e440-4b79-9943-199d0adb43fc&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

129 Ethereum is the community-run technology powering the cryptocurrency ether (ETH) and thousands of decentralized applications.

130 Ethan Jewell, "North Korean hackers stole $620 million from Pokemon-like blockchain game: FBI," NK News, April 15, 2022. https://www.nknews.org/pro/north-korean-hackers-stole-620-million-from-pokemon-like-blockchain-game-fbi/.

131 Laura Bicker, "Drugs, arms, and terror: A high-profile defector on Kim's North Korea".

132 Lubomir Tassev, "Cryptocurrency Theft Remains Key Revenue Source for North Korea, UN Report Says," Bitcoin, February 6, 2022. https://news.bitcoin.com/cryptocurrency-theft-remains-key-revenue-source-for-north-korea-un-report-says/.

Even after the United Nations placed sanctions on North Korea's foreign currency earnings, RGB hackers were still able to steal $571 million worth of virtual currency.[133] A North Korean ransomware operation named Holy Ghost played a role in this success, as the operation infected computers and demanded anywhere from $30,000 to $100,000 to remove the ransomware. Ransomware is a program that creates a virus in one's computer system and encrypts stored data and then demands money to resolve the issue. Microsoft's Threat Intelligence Center tracked Holy Ghost to the Lazarus Group.[134]

The U.S. National Security Agency also assessed that RGB was behind the WannaCry ransomware attack that took place in 2017 and hit 150 countries around the world. WannaCry is a program created by exploiting vulnerabilities in MS Windows operating system and can only attack MS Windows. In May 2017, there were a total of three hundred thousand ransomware attacks in 150 countries worldwide. WannaCry 2.0 has also impaired railroad, aviation and medical networks in the United States, Asia and Europe since 2017.[135] Recently, frequent cyberattacks in the field of foreign affairs and security have one thing in common. All of them were subjected to a 'spear phishing' method in which documents or links with malicious code were placed in emails impersonating government departments or experts.[136]

According to the NIS, North Korean hackers have stolen U.S. $1.72 billion in cryptocurrencies since 2017.[137] Consequently, South Korea has recently sanctioned four RGB hackers and seven organizations under the RGB, including Lazarus, Bluenoroff, and Andariel.[138] The NIS predicts that North Korea will increase these cyberattacks in South Korea to steal technology, as well as diplomatic and security intelligence.[139] South Korea is not the only nation in danger, either. Other sources report that North Korean hackers have accounted for 30% of cryptocurrency theft throughout the world since 2017, stealing $721 million in the process.

---

133 Jin-young Bae, "북한 정찰총국, 가상화폐 거래소 해킹해 5억 7100만 달러 절취" [North Korea's Reconnaissance Bureau hacked cryptocurrency exchanges and stole $571 million], Monthly Chosun, March 9, 2019. http://monthly.chosun.com/client/mdaily/daily_view.asp?Idx=6385&Newsnumb=2019036385.

134 Sead Fadilpašić, "Microsoft links Holy Ghost ransomware operation to North Korean hackers," TechRadar, July 15, 2022. https://www.techradar.com/uk/news/microsoft-links-holy-ghost-ransomware-operation-to-north-korean-hackers.

135 NSA '워너크라이 공격 배후 北 정찰총국" 최종 확인 중국 내 북한 정찰총국 IP 발견" (NSA "North Korea Reconnaissance General Bureau behind WannaCry attack" final confirmation North Korean Reconnaissance General Administration IP found in China), Clien, June 16, 2017. https://www.clien.net/service/board/park/10869637. And Jung-seok Lee, "미외교협회 "북한 사이버 공격 위협적" …' 군사 역량 보고서' 평가 (U.S. Council on Foreign Relations: North Korea threatens cyberattacks…Evaluation of 'Military Capability Report')," Liberty Korea Post News, December 27, 2021. http://www.lkp.news/news/articleView.html?idxno=18434.

136 Geoffrey Cain, "North Korea: How the Least-Wired Country Became a Hacking Superpower", CNBC, May 27, 2013.https://www.cnbc.com/2013/05/26/north-korea-how-the-leastwired-country-became-a-hacking-superpower.html.

137 Jaewoo Park and Hyung Jun, "Interview: U.S. cyber crime czar discusses readiness to stop North Korean threats," Radio Free Asia, January 18, 2023. https://www.rfa.org/english/news/korea/fick-01182023163022.html.

138 Dong-woo Chang, "S.Korea slaps first sanctions on N.Korea over crypto theft, cyberattacks," Yonhap, February 10, 2023. https://en.yna.co.kr/view/AEN20230210003300325?section=news.

139 Soo-yeon Kim, "N.Korea to step up cyber-attacks against S. Korea next year: Seoul spy agency," Yonhap, December 22, 2022. https://en.yna.co.kr/view/AEN20221222005900325.

The primary targets were Asian states,[140] primarily South Korea. Cyber-attacks from North Korea that target South Korea consist of DDOS, APT, MBR wiper attack, GPS botnet, malicious code, code obfuscation, trace deletion, and steganography. The North also employs the use of internet games and malicious statements on the internet. Targets include the South Korean Blue House (former Presidential Building), South Korean National Assembly, South Korean Ministry of National Defense, and think tanks.[141] North Korean hackers also consistently attack South Korean TV, Incheon Airport, the Seoul subway system, and South Korean train lines.[142]

Although South Korea was often the focus of the attacks, a United Nations report found other popular targets included countries in Africa, South America, the Middle East, and Europe.[143] It is not surprising, therefore, that North Korea has been described as a "criminal syndicate with a flag."[144]

Individuals participating in the North Korean cyberwarfare effort have developed a strong working relationship with Russian cybercrime operatives as well.[145] This relationship allowed North Korean cyber operatives to steal even more money because they had access to worldwide financial institutions, causing great security concern to other countries. At a press briefing on March 22nd, 2022, in Washington, D.C., U.S. national security adviser Jake Sullivan stated that North Korea was cooperating with foreign cyber warfare agents, including those from Russia.[146] Although Sullivan refused to elaborate on the topic, the U.S. Treasury Department has since identified the methodology of North Korean (RGB) hackers:

- "Abuse the entire ecosystem of freelance work platforms to surreptitiously obtain IT development contracts from client companies around the world—as well as abuse many social media platforms—to communicate with clients and payment platforms to receive payment for their work.
- Develop applications and software spanning a range of sectors, including, but not limited to, business, cryptocurrency, health and fitness, social networking, sports, entertainment, and lifestyle.

140 Silviu Stahie, "North Korea Responsible for 30% of All Cryptocurrency Stolen Since 2017," Bitdefender, May 18, 2023. https://www.bitdefender.com/blog/hotforsecurity/north-korea-responsible-for-30-of-all-cryptocurrency-stolen-since-2017/.

141 Jeong Yoon Yang, So Jeong Kim, and Il Seok Oh, "Analysis on South Korean Cybersecurity Readiness Regarding North Korean Cyber Capabilities," Information Security Applications, August 2016. https://www.researchgate.net/publication/315858994_Analysis_on_South_Korean_Cybersecurity_Readiness_Regarding_North_Korean_Cyber_Capabilities.

142 Pil-jae Kim, 북한의 사이버 남침 (North Korea's Cyber Invasion of the South), 99.

143 Jack Martin, "UN Report: South Korea Hardest Hit By North Korean Cyber Attacks," Coin Telegraph, August 13, 2019. https://cointelegraph.com/news/un-report-south-korea-hardest-hit-by-north-korean-cyber-attacks.

144 Ed Caesar, "The Incredible Rise of North Korea's Hacking Army."

145 Benjamin R. Young, "The Emerging North Korean-Russian Cybercrime Partnership," National Interest, March 21, 2022. https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/emerging-north-korean-russian.

146 Sung-mi Ahn, "NK working with Russian cybercriminals: Sullivan," The Korea Herald, March 23, 2022. http://www.koreaherald.com/view.php?ud=20220323000619.

» In many cases misrepresent themselves as foreign (non-North Korean) or U.S.-based teleworkers, including by using virtual private networks (VPNs), virtual private servers (VPSs), purchased third-country IP addresses, proxy accounts, and falsified or stolen identification documents.

» Use privileged access gained as contractors for illicit purposes, including enabling malicious cyber intrusions by other North Korean actors."[147]

The chart below presents the basics of how RGB hackers steal money over the cyber-sphere.[148]

Figure 9, Source: Dagyum Ji, "Tale of North Korea's cyberterrorists: How they break into 'unhackable' crypto platforms and cash out", Korea Herald, December 12, 2022. https://www.koreaherald.com/article/3017774.

147 "Guidance on the Democratic People's Republic of Korea Information Technology Workers," U.S. Treasury Department, May 16, 2022. https://ofac.treasury.gov/media/923131/download?inline.

148 Da-gyum Ji, "Tale of North Korea's cyberterrorists: How they break into 'unbackable' crypto platforms and cash out," The Korea Herald, December 12, 2022. https://www.koreaherald.com/view.php?ud=20221212000714.

Included below is a separate chart that also describes how North Korean hackers have schemed to steal money online.[149]

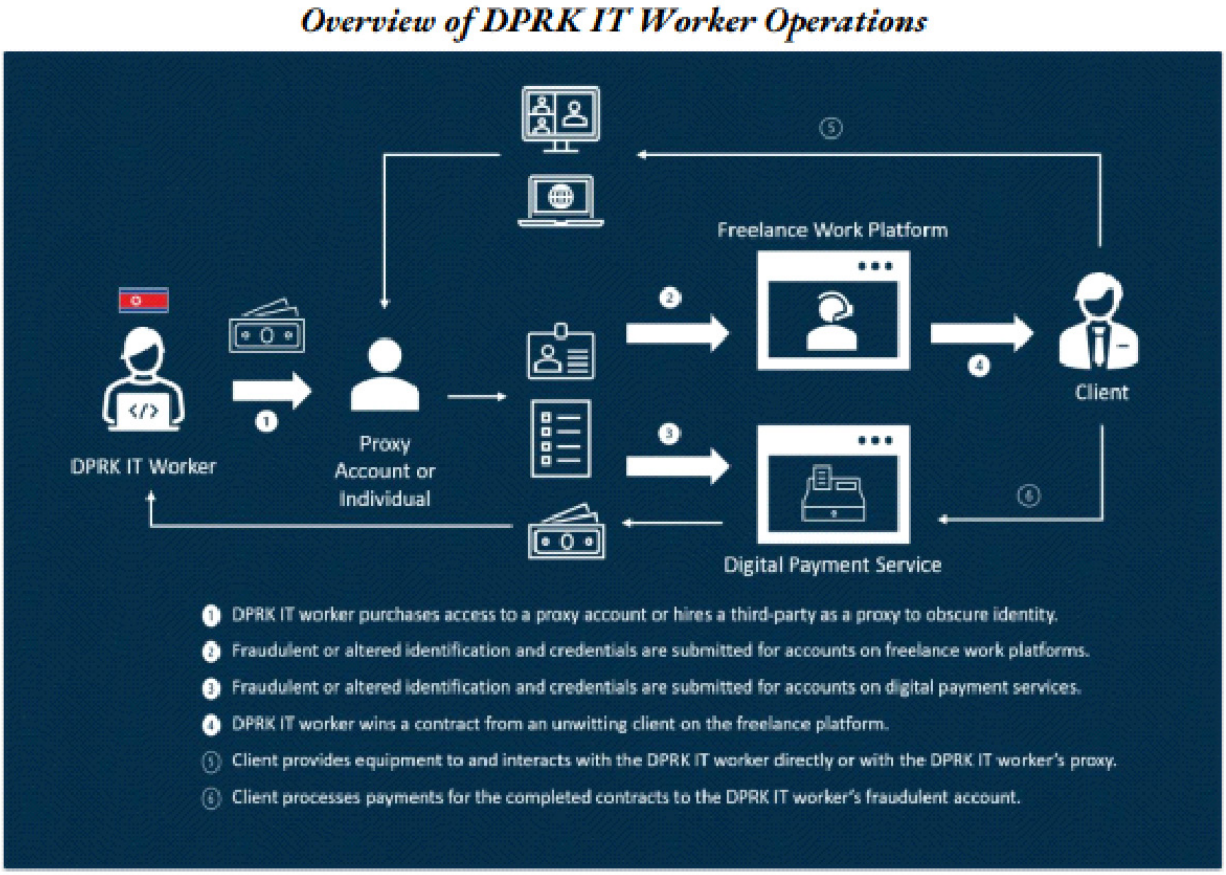


Figure 10, Source: U.S. Department of Treasury, "GUIDANCE ON THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS" U.S. Department of Treasury, May 16, 2022. https://ofac.treasury.gov/media/923126/download?inline.

According to a recently retired agent of the NIS, RGB hackers use the following strategies to move stolen funds into banks in North Korea:

- First, cybercriminals hack and embezzle money.
- With the stolen money, hackers buy forms of cryptocurrency, including Bitcoin and Ethereum.
- Hackers then transfer cryptocurrency to cities like Tehran, Damascus, and Dubai via email links and PayPal and begin the trading process.
- After multiple small transactions, hackers begin to transfer cryptocurrency to China where it can be turned into cash in the form of South Korean won.

149 "Guidance on the Democratic People's Republic of Korea Information Technology Workers," U.S. Treasury Department, May 16 2022, https://ofac.treasury.gov/media/923131/download?inline.

» The South Korean won is then exchanged for dollars, and these dollars are transferred into North Korean banks for regime profit.[150]

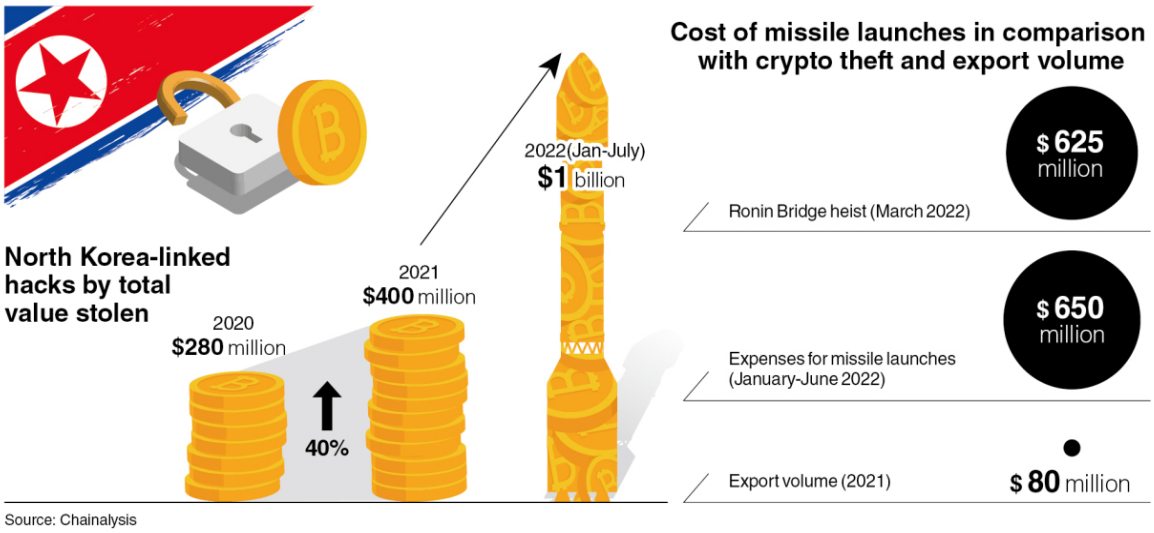


Figure 11, Source: Dagyum Ji, "Crypto hacking behind N. Korea's renewed nuclear ambition", Korea Herald, December 6, 2022, https://www.koreaherald.com/article/3015095.

The implications of the crypto theft go well beyond money-laundering, too, as the Kim regime uses this money to presumably pay for parts of North Korea's missile development program. The graphic included above explores this connection in greater detail.[151] In May of 2022, the United States Treasury Department, State Department, and the FBI delivered a warning that North Korean hackers were posing as online IT workers offering technical assistance. Some of them made up to $300,000 annually, and many of these 'earnings' were reportedly given to the Kim regime to support the North Korean nuclear and missile programs.[152]

Another group linked to the RGB is APT37. Also known as the Reaper and Mazel Chollima, APT37 is a North Korean state-sponsored cyberespionage group that uses malware to infiltrate computer networks, targeting aerospace and defense networks.

150 Tara O, "How North Korea Launders Money Using Cryptocurrency to Evade Sanctions," East Asia Research, October 8, 2022. https://eastasiaresearch.org/2022/10/08/how-north-korea-launders-money-using-cryptocurrency-to-evade-sanctions/. And Anonymous Former South Korean Intelligence Officer Interviewed by Robert Collins. Seoul, South Korea. April 2024.

151 Da-gyum Ji, "Crypto hacking behind N.Korea's renewed nuclear ambition" The Korea Herald, December 6, 2022. http://www.koreaherald.com/view.php?ud=20221206000676&ACE_SEARCH=1.

152 Lily Hay Newman, "Good Luck Not Accidentally Hiring a North Korean Scammer," Wired, May 30, 2022. https://www.wired.com/story/north-korean-it-scammer-alert/.

Formerly focused on South Korea, APT37 has expanded its target to other countries as well, including Japan, Vietnam, and countries in the Middle East.[153] The Reaper is adept at exploiting 'Zero-Day'[154] vulnerabilities of organizations and individuals, including human rights activists, North Korean escapees, journalists, and policy makers.[155] Other common targets include:

- A company from the Middle East that established a joint venture with a North Korean telecommunications service.
- Personnel working in trade and international affairs, including the Olympics.
- Individuals working on North Korean human rights issues.
- A Japanese organization connected to the United Nations that focused on North Korean sanctions and human rights.[156]

Another North Korean APT, Kimsuky, is part of the greater cyber espionage network. Kimusky is also known as Thallium, Black Banshee, and Velvet Chollima and it's developed into a significant cyber security threat since its attack on South Korea's Hydro & Nuclear Power Company in 2014.[157] Indeed, "from less than one hundred C2 servers in 2019, Kimsuky had 603 malicious command centers as of July 2022."[158] The South Korean National Police also found that 892 foreign policy experts in South Korea were hacked by Kimsuky in 2022 and discovered 150 former South Korean cabinet minister officials had been under the surveillance of this North Korean group.[159]

Furthermore, Kimsuky has also been identified by the South Korean Defense Acquisition Program Administration as being responsible for hacking into the Korea Atomic Energy Research Institute and the Korea Aerospace Industries. South Korea suspects that the South Korean KF-21 fighter plane and FA-50 drone designs were the primary target of the hacking.[160]

---

153 David Taylor, "Study reveals North Korean cyber-espionage has reached new heights," The Guardian, February 20, 2018. https://www.theguardian.com/world/2018/feb/20/north-korea-cyber-war-spying-study-fire-eye.

154 The term "Zero-Day" is used when security teams are unaware of their software vulnerability, and they've had "0" days to work on a security patch or an update to fix the issue.

155 Lorenzo Franceschi Bicchierai "North Korean hackers exploited Chrome zero-day to steal crypto," Tech Crunch, August 30, 2024. https://techcrunch.com/2024/08/30/north-korean-hackers-exploited-chrome-zero-day-to-steal-crypto/.

156 David Taylor, "Study reveals North Korean cyber-espionage has reached new heights."

157 Cheong-mo Yoo, "N.K. hacking group monitored ex-ministers' emails for months: police," Yonhap, June 7, 2023. https://en.yna.co.kr/view/AEN20230607006200315?section=nk/nk.

158 Catherine Knowles, "Kaspersky uncovers details about active cyber-espionage campaign," IT Brief, September 13, 2022. https://itbrief.co.nz/story/kaspersky-uncovers-details-about-active-cyber-espionage-campaign.

159 Dong-hwan Ko, "North Korea hacked 892 foreign policy experts," The Korea Times, December 25, 2022. https://www.koreatimes.co.kr/www/nation/2022/12/113_342329.html.

160 Hyo-kyung Kim, "항공우주산업 내부시스템도 해킹 당해..방사청 '조사 중'" (The aerospace industry's internal system was also hacked…Defense Acquisition Program Administration "Investigating"), Daum, June 30, 2021. https://v.daum.net/v/20210630215208595?f=o.

The chart below explains the peril of Advanced Persistent Threat (APT).[161]

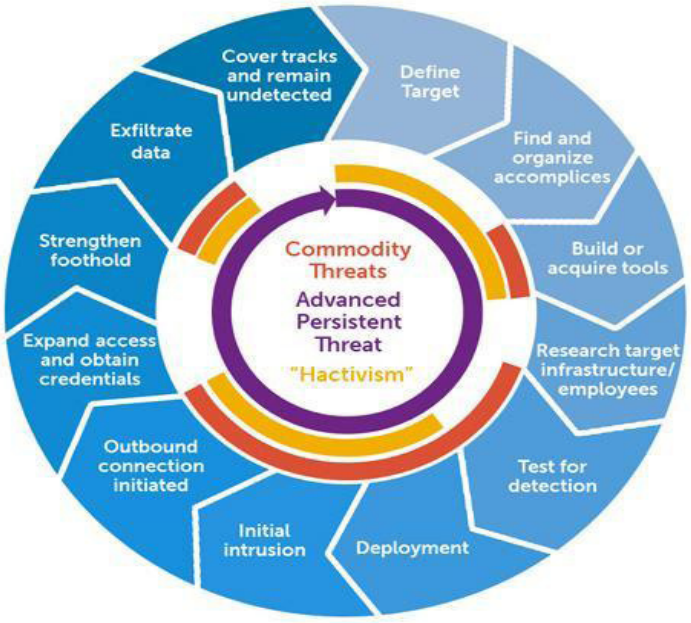


Figure 12, Source: Emagcom Security. "APT (Advanced Persistent Threat) Group"https://emagcomsecurity.wordpress.com/2015/04/09/apt-advanced-persistent-threat-group/.

To collect intelligence information on South Korea, North Korean hacking groups target South Korean security services, national organizations, research institutes, and public platforms. In particular, the South Korean Ministry of Foreign Affairs, Ministry of Defense, and Ministry of Unification are primary targets as well as the Incheon Airport, Seoul subway system, and South Korean train lines. Cyber security criminals target leaders of prominent South Korean organizations using phishing emails that carry malware and allow them to exploit their personal and professional information. Other North Korean cyber warfare tactics include spreading misinformation.[162]

RGB hackers use South Korean government agencies to launch cyberattacks.[163] For instance, hackers prevent South Korean agencies from blocking pro-North Korean websites by changing IP addresses and replacing links with pro-North Korean sites.[164]

161 APT GROUP," Emagcon Security, April 9, 2015. https://emagcomsecurity.wordpress.com/2015/04/09/apt-advanced-persistent-threat-group/.
162 Pil-jae Kim, 북한의 사이버 남침 (North Korea's Cyber Invasion of the South), 101, 106-7.
163 Dong Hui Mun, "Hackers use S.Korean internet security agency as a disguise to mount cyberattacks," Daily NK, November 14, 2022. https://www.dailynk.com/english/hackers-use-south-korean-internet-security-agency-as-disguise-mount-cyberattacks/.
164 N.Korea's Vast Cyber Warfare Army," Chosun Daily, August 13, 2013. http://english.chosun.com/site/data/html_dir/2013/08/13/2013081300891.html.

North Korean agents also employ malware that targets academia, think tanks, and news media sectors and impersonates the sources to collect intelligence.[165] Furthermore, North Korean hackers employ a remote code to target users of Google Chrome through remote code vulnerability CVE-2022-0609, specifically attacking news outlets, software vendors and fintechs. Ten news outlets and eighty-five people from fintechs have been targeted.[166] South Korean citizens may think these attacks have no impact on them; however, these attacks pose a direct threat to South Korean national security and financial stability, which can have consequential ripple effects throughout the community.

As for North Koreans themselves, the internet is very restricted in North Korea for most of the population. Even citizens who have some access to the internet are restricted to the Kwangmyong intranet. Individuals who work at North Korean research institutes and educational organizations are the only exception to this rule, but even these individuals do not have access to the worldwide web.[167] To make matters worse, most North Korean websites are primarily focused on spreading propaganda that extols the virtues of Kim Il-sung and promotes anti-Japanese resistance. North Korea's Korean Central News Agency even publishes information in Korean, English, Russian, and Spanish to reach a broader group of people and 'inform' them of North Korean events and issues.[168] The Kim regime also targets diplomats with New Year's greetings that use spear phishing tactics to employ North Korean malware.[169]

165 "U.S., ROK Agencies Alert: DPRK Cyber Actors Impersonating Targets to Collect Intelligence," National Security Agency, June 1, 2023. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3413621/us-ROK-agencies-alert-dprk-cyber-actors-impersonating-targets-to-collect-intell/.

166 Cedric Pernet, "North Korean threat actors target news outlets and fintechs with a Google Chrome vulnerability," TechRepublic, March 30, 2022. https://www.techrepublic.com/article/north-korean-threat-actors-target-news-outlets-fintechs-google-chrome-vulnerability/.

167 Pil-jae Kim, 북한의 사이버 남침 (North Korea's Cyber Invasion of the South), 57.

168 Ibid.

169 Ethan Jewell, "North Korea hackers weaponize holiday cheer in latest cyberattack against Russia," NK News, January 4, 2022. https://www.nknews.org/pro/north-korea-hackers-weaponize-holiday-cheer-in-latest-cyberattack-against-russia/.

The chart below describes the chain of control and command of the SAC that includes these and other operations.[170]

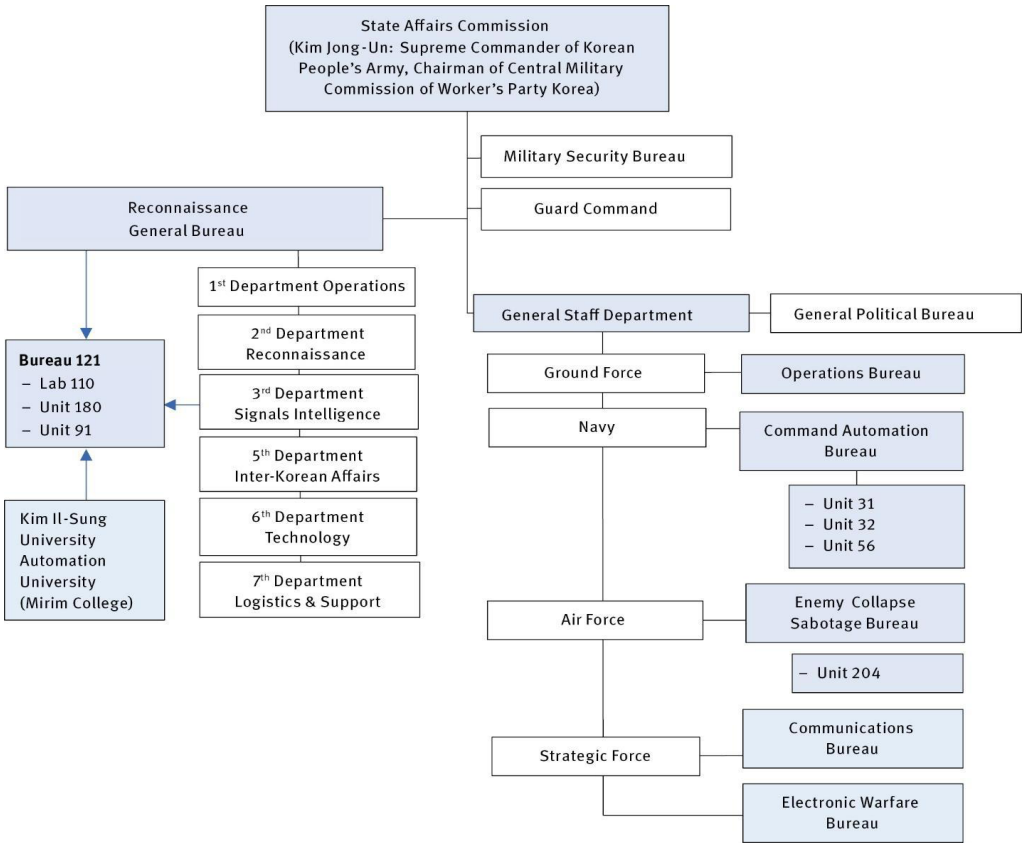


Figure 13, Source: Michael Raska, "North Korea's Evolving Cyber Strategies: Continuity and Change", De Gruyter Brill, September 8, 2020. https://www.degruyterbrill.com/document/doi/10.1515/sirius-2020-3030/html?lang=de.

The RGB evidently uses both software and hardware as weapons. Besides hacking operations, North Korean cyber groups also utilize internet worms, email bombs, logic bombs, DDOS attacks, autonomous mobile cyber weapons, malicious code, global positioning system jamming, electromagnetic pulse, nanomachines, chipping, and high energy radio frequency guns, the sum of which illustrates the power of North Korea's arsenal in the cyberwarfare space.[171]

170 Michael Raska, "North Korea's Evolving Cyber Strategies: Continuity and Change," De Gruyter, September 8, 2020. https://www.degruyter.com/document/doi/10.1515/sirius-2020-3030/html?lang=de.

171 Pil-jae Kim, 북한의 사이버 남침 (North Korea's Cyber Invasion of the South), 65-66.

Section 6: RGB Targeting the ROK-U.S. Military Alliance

Since the 1990s, North Korea has initiated efforts to strengthen its cyber power. Kim Jong-il, who saw the collapse of Saddam Hussein's regime in Iraq in 2003, said, "up to this point, war has been about bullets and oil, but the war in the 21st century will be about information warfare."[172] The RGB is especially aware of this reality. In the past few years, the RGB has utilized computer hacking operations, specifically those that target South Korean and U.S. military forces, to gain foreign intelligence. Indeed, the RGB has collected information related to South Korean military leaders, naval deployments, and military training through thousands of hacking operations per year.[173]

The (former) South Korean-U.S. Combined Forces Command Operational Plan 5027 was an exceptionally important target.[174] In 2016 alone, the RGB hacked 3,200 South Korean military computers. North Korean hackers seized 235 gigabytes of information during the operation, including the United Nations Command / South Korean-U.S. Combined Forces Command Operations Plan 5015 which contained information about decapitating the Kim Jong-un regime.[175]

After learning about this plan, the RGB instructed Kim to begin using the cars of his aides to protect himself. The operation was thereby deemed successful because it allowed North Korean authorities to get ahead of the attacks.[176] The mission was also useful because it enabled the North Korean military to evaluate South Korean and U.S. confidence in their weapons, tactics, strategy, and personnel systems.

In addition to these hacking operations, the RGB attempted to shut down the South Korean electrical grid, threatening all South Korean banks, computer networks, medical facilities, and environmental support structures. The move caused great concern among South Korean leaders because if the South Korean electrical grid collapsed, so too would the country's civilian infrastructure.[177]

---

172 Pil-jae Kim, 북한의 사이버 남침 (North Korea's Cyber Invasion of the South).

173 Ibid. 88-89.

174 Ibid. 93.

175 The South Korean-U.S. Alliance war plan for defending South Korea.

176 Jong-seok Song, "Cybersecurity emerges as top priority," Korea JoongAng Daily, June 2, 2022. https://koreajoongangdaily.joins.com/2022/06/02/opinion/columns/cybersecurity-military/20220602195420736.html. See also Ed Caesar, "The Incredible Rise of North Korea's Hacking Army." See also Sang Hun Choe, "North Korean Hackers Stole U.S. South Korean Military Plans, Lawmaker Says," New York Times, October 10, 2017. https://www.nytimes.com/2017/10/10/world/asia/north-korea-hack-war-plans.html.

177 Anonymous Former South Korean Intelligence Officer Interviewed by Robert Collins. Seoul, South Korea. April 2024.

RGB hackers have also shut down support networks in South Korea in areas adjacent to U.S. military bases, including Yongsan military base networks in Seoul which has been home to the South Korean-U.S. Combined Forces Command since 1978.[178] Indeed, North Korea's cutting-edge cyber weapons systems shut down unprotected South Korean-U.S. Alliance national defense systems in one shot, showing the threat the RGB poses in the cybersecurity space.[179]

One successful North Korean cybercriminal group has been the Andariel Group, which is a sub-section of the RGB's Lazarus Group. Andariel is infamous for hacking the personal computer of the South Korean Minister of Defense in 2019.[180] The Andariel Group also targets defense industries, military organizations, financial companies, and political establishments. The success of groups like Andariel highlights the shortcomings within South Korea's response to North Korean cyber-attacks. Cyber-attacks on the North Korean infrastructure are not as impactful as attacks on South Korea because North Korean citizens do not have access to the internet, but rather an intranet. Thus, in a war on the peninsula, the South Korea-U.S. Alliance would have to employ sophisticated electro-magnetic pulse bombs and kinetic targeting to disrupt North Korean infrastructure, which is more expensive than North Korea's cyber target attacks.[181]

These shortcomings are exacerbated by the fact that North Korean cyberthreats are not taken seriously. Many people assume North Korea's hacking abilities do not comprise the capacity to kill people, but nothing could be further from the truth. Shutting down South Korean infrastructure, disrupting South Korean energy systems, disabling South Korean healthcare systems, and/or damaging power plants would have a substantial domino effect. The RGB has already begun to cripple South Korean power plants. In over 2,000 cases, North Korean cyber hackers found their way into 700 South Korean plants that handle harmful chemicals. RGB members have also hacked into South Korea's Chemical Accident Response Information System for the purpose of understanding where chemical plants are located and how much damage they would cause if they exploded.[182] South Korean military analysts see this as part of North Korea's chemical warfare strategy.[183]

If North Korea can damage South Korean chemical and nuclear power plants, thus disrupting local area populations and infrastructure, the North Korean military will be able to adjust the targeting of its chemical, biological and nuclear weapons to complement its wartime strategy. It is worth noting, however, that South Korea-U.S. Alliance military sources reportedly insist North Korea's cyber-attack systems can be shut down immediately.[184]

178 Pil-jae Kim, 북한의 사이버 남침 (North Korea's Cyber Invasion of the South) 100–01.
179 Ibid.
180 Jamie Tarabay, "Korean Cybersecurity Experts Play Cat-and-Mouse with the North's Hackers," Bloomberg, September 2, 2022. https://www.bloomberg.com/news/articles/2022-08-31/north-korea-hackers-sometimes-leave-k-pop-clues-in-code?sref=hhjZtX76.
181 Ibid.
182 Pil-jae Kim, 북한의 사이버 남침 (North Korea's Cyber Invasion of the South), 89. Furthermore, this is reminiscent of a 1984 incident in Bhopal, India where a chemical plant explosion killed nearly 4,000 people and hurt 600,000.
183 Ibid, 88-91.
184 Ibid, 102.

Section 7: RGB Training and Education

RGB education varies due to the different skill sets the organization is looking to develop, i.e., differences between cyber warriors, reconnaissance personnel, and espionage operatives. Under the direction of the KWP, North Korea has established 85 educational programs at 37 universities which focus on developing skills in science, technology, engineering, and math (STEM).[185]

In October 2009, Kim Jong-un instructed every No.1 school[186] in North Korea to educate and train students in the computer sciences. The training proceeds as follows: Middle and high school students are provided with Pentium computers and compelled to study 80 hours of computer hardware as well as 280 hours of C# and C++ languages in their first year. They spend 120 hours studying computer math, 180 hours on Linux servers and open-source operating systems, and 200 on data recovery and algorithms the following year. Finally, they study 160 hours of artificial intelligence and natural language processing, 140 hours of computer communications and networking, and 120 hours of artificial intelligence language by the time of graduation. North Korean computer students end up spending twice the number of hours studying computer sciences than their South Korean counterparts.[187]

Unsurprisingly, grade school is where most hackers get their start in the cyberespionage industry. Most North Korean hackers are often recruited out of grade school. Each year the Kim regime selects the brightest computer students at every school and sends them to the First and Second Kumsong Middle Schools in Pyongyang. There, the students learn hacking skills after which they go on to institutions such as Kim Il-sung University, Kim Chaek University of Technology, Pyongsong College of Science, and Mirim University.

Cyber warfare students also attend Pyongyang Computer Technology College, Hamhung Computer Technology College, and Moranbong College before beginning their careers. Hamhung College and Moranbong College specialize in cyber engineering,[188] and students spend so much time there that they leave with roughly ten years of training by graduation.[189] Kim Heung-kwang, a former professor of computer science at Hamhung Industrial University in North Korea who defected to South Korea in 2004, said, "North Korea's 'information warriors' are the most talented people in the country."[190]

---

185 "Guidance on the Democratic People's Republic of Korea Information Technology Workers," U.S. Treasury Department, May 16 2022, https://ofac.treasury.gov/media/923131/download?inline.

186 No.1 schools – both middle school and high school – are located in every city, county and province of North Korea. These schools are attended by the brightest students in North Korea. These students are identified by teachers at the grade school level and recommended for attendance at No.1 schools.

187 Pil-jae Kim, 북한의 사이버 남침 (North Korea's Cyber Invasion of the South), 59–60.

188 Ibid.

189 Seong-min Kim, "北, 對南 사이버테러요원 3000명… 댓글 다는 전문 요원만 200여명" [3,000 North anti-South terrorist agents…200 experts who comment], Chosun Ilbo, August 13, 2013. https://www.chosun.com/site/data/html_dir/2013/08/13/2013081300176.html.

190 Tae-woo Im, "정보전사는 상위 0.001% 영재죠" (North Korean intelligence warriors are in the top 0.001% gifted), Maeil Business News, July 17, 2009. https://www.mk.co.kr/news/society/view/2009/07/389655/.

Moranbong College is an especially prominent institution. Moranbong was established in 1997 to train and educate RGB operatives in codebreaking and computer hacking. The 1996 submarine infiltration incident on the South Korean coast served as a catalyst for the establishment of this school. After the Kangnung submarine incident, the KWP Operations Department's anti-South Korea liaison stations' operatives and sleeper agents emphasized the need for a new intelligence collection methodology.[191]

Today, 30 students are selected every year to participate in Moranbong's five-year curriculum. Most of these students are appointed to first lieutenant in the KPA upon entry to the university. For the first two years, they study military arts, and the next three years, they study computer language, communications intercept, code breaking, and hacking to maximize their ability to collect information.

Upon graduation, many students are assigned to the RGB or to one of the regional liaison stations that gather intelligence on South Korea, the U.S, and/or Japan. Some students are even assigned to collect foreign currency and technology while operating out of China to give to the Korea Computer Center. Moranbong College is reportedly more advanced than the other universities in terms of equipment, technology, and curriculum. Moreover, Moranbong College's existence is a closely kept secret, even within the RGB, making it even more exclusive.[192]

The Kim Chaek University of Technology is also notable for its students' technology prowess. Students from this university placed eighth in the 2019 International Collegiate Programming Contest. By comparison, South Korea's Seoul National University placed seventh, Great Britain's Cambridge University was 13th, and Harvard University placed 21st.[193] Kim Chaek University of Technology and Mirim College of Automation play a critical role in developing most of the skills needed to be a hacker for the RGB. The Mirim College of Automation graduates 100 student hackers per year,[194] and 10 to 20 of these graduates are ultimately selected by the RGB.

The RGB Operations Bureau also runs its own university, which specifically trains spies and fighters. The Kim Jong-Il Political-Military College, also known as the "130th Liaison Station, and the 695 Military Unit," or the Central Committee Political-Military College, is the successor to the former Kumsung College. Although it is in the Gyeongsan District of Pyongyang City, it uses a fake address of Pyeonghwa 2-dong, Moranbong District, Pyongyang City.[195]

---

191 Pil-jae Kim, 북한의 사이버 남침 (North Korea's Cyber Invasion of the South), 61.

192 Ibid, 62.

193 The ICPC, the "ACM International Collegiate Programming Contest", is an extra-curricular, competitive programming competition of the universities of the world. ICPC competitions provide gifted students opportunities to interact, demonstrate, and improve their teamwork, programming, and problem-solving prowess. The ICPC is a global platform for academia, industry, and community to shine the spotlight on and raise the aspirations of the next generation of computing professionals as they pursue excellence.

194 Geoffrey Cain, "North Korea: How the Least-Wired Country Became a Hacking Superpower", Department of the Army, North Korean Tactics (Army Techniques Publication No. 7-100.2: Washington DC, 2020); 9-16.

195 Chae-hwan Kim, "Because of the North Korean defector family… Graduates of Kim Jong-Il Political and Military College, excluded from appointment as combatants," Daily NK, January 25, 2022. https://www.dailynk.com/20220125-4/.

This university has a four-year training program for combat reconnaissance officers and a special one-year system for training foreign operatives in South Korea. The program trains 100 to 200 infiltrators and graduates 60 to 80 agents per year. The college celebrated its 35th anniversary in 1992, and it used the name of Kim Jong-il for the first time in the history of North Korean educational institutions during this celebration.[196]

North Korea began training spies targeting South Korea in September 1947 with the founding of the Kangdong Political Academy. This academy started as a training institute for executives but was converted in October 1948 to train anti-South Korea operatives. Approximately 1,200 operatives were trained at Kangdong Political Academy in 1949 when the students studied four curriculum classes per day along with guerrilla training. The academy's curriculum was composed of Marxist-Leninist philosophy, history of liberation struggle, political party establishment, political economy, history of the Communist Party of the USSR, history of Korea, new democracy, guerrilla tactics, marksmanship and engineering. The academy was disbanded in 1950 because of its purported loyalty to South Korean communist leader Pak Hon-yong instead of Kim Il-sung.[197]

During the Korean War, Kumgang Political Academy was the primary spy-training institute in North Korea. Founded in January 1951 in Seoheung County, Hwanghae Province, this academy was designed to train operatives to serve as mid-level officials in Seoul after the second conquest of the South Korean capital city. The majority of the 1,500 graduates in the class of 1952 were deployed to various districts in South Korea. The Kumgang Political Academy was disbanded in March 1953 and later replaced by Central Party School No.1 and No.2.[198]

Selection for field operative training follows very strict guidelines. Selected operative candidates must have good songbun,[199] strong party spirit, good academics, and strong language skills. They must also be in excellent physical shape. Experience living in a foreign country environment is also a plus when it comes to recruitment. In 1975, Kim Jong-il designated the anti-South Korea Cadre Section of the KWP to be responsible for field operative candidate selection. Once selected, candidates then had to undergo a physical examination at the 915th Hospital.

196 Ibid; see also Joseph S. Bermudez, Jr., "Special Report: A New Emphasis on Operations Against South Korea"; see also Pil-jae Kim, "북한의 암살 전문가' 양성조직: 김정일정치군사대학 (North Korea's Assassins to Organization: Kim Jong-il Political College)," January 25, 2013. https://www.chogabje.com/board/view.asp?C_IDX-=40332&C_CC=AB.

197 "North Korean Miliary and Political Schools, CIA, September 22, 1952, https://www.cia.gov/readingroom/docs/CIA-RDP82-00457R013900350003-1.pdf.

198 Ibid.

199 Songbun is the term for the Kim regime's socio-political classification of every North Korean citizen for the purpose of profiling those most likely to support the regime and those most likely to not support the regime. For a detailed discussion of songbun, see *Robert Collins, "Marked for Life: Songbun – North Korea's Social Classification System"* (Washington, D.C.: Committee for Human Rights in North Korea, 2012).

Upon passing all qualifications, candidates are then sent to the Kim Jong-il Political-Military College where they study a curriculum that includes not only operational tactics and skills, but also a heavy dose of Juche ideology. Students spend much of their time studying this ideology and conducting physical training, with less time spent on tactical operations.[200]

Infiltration training includes basic shooting and dagger drills, long-distance swimming, snorkel and air tank diving practice, navigation and engine operation, underwater fighting, underwater detonation training, obstacle passage, etc. The basics of these courses teach students how to approach terrorists, subdue an enemy in this process, perform missions and exfiltration, and utilize martial arts in dangerous situations. Swimming instruction is an exceptionally important part of military training. In this part of the curriculum, students learn how to survive for days in a sea or river. They are also taught how to speed walk 150 li (36.6 miles) in one evening, regardless of terrain challenges.[201]

The Tokyo Shimbun obtained the Kim Jong-il Political-Military College curriculum "Kim Jong-Il-ism and foreign intelligence studies," thereby providing greater insight into the university's programs. Kim Jong-il's instructions are clear in the curriculum guidelines, saying "we must make the information organization deeply rooted."

The idea is to accelerate the revolution and reunification in South Korea by recruiting or infiltrating the existing staff within South Korean institutions. In addition to the presidential secretary's office, major agencies of the administration such as the Joint Chiefs of Staff, the Land, Sea and Air Forces Headquarters, and the NIS are also listed as target agencies for the infiltration of intelligence sources. Specific infiltration methods include "recruiting due diligence using human relationship, and purchase of human resources managers."[202]

In addition to the Kim Family Regime's ideological education, the curriculum includes instruction about South Korea's socio-political situation and topography as well as engineering skills. For example, the curriculum includes classes such as "Electrical Engineering" and "Nuclear Engineering." which teach students how to identify and destroy nuclear power plants. Predictably, there is also a class on how to manufacture homemade explosives and explosives handling.

Kim Jong-il also included instruction about 'self-destruction' into the curriculum.[203] "Whether you are a fighter or an agent, you must learn the theory of self-destruction." RGB agents must learn how to effectively commit suicide by exploding a hand grenade under their chin. An example of this is the textbook 'Philosophical Material.'"

200 Pil-jae Kim, "북한의 암살 전문가' 양성조직: 김정일정치군사대학 (North Korea's Assassins Training Organization: Kim Jong-il Political College)," January 25, 2013. https://www.chogabje.com/board/view.asp?C_IDX-=40332&C_CC=AB.

201 Ibid.

202 Kwang-jin Kim, North Korea's Terror Organizations and Their Possible Provocation (북한의 대남테러 조직 및 테러전망), 79.

203 Ibid.

With a total of five chapters and 21 verses, this book consists of:[204]

» Chapter 1 - What is Philosophy

» Chapter 2 - Juche's Revolutionary Worldview

» Chapter 3 - Juche's Revolutionary View of The Supreme Leader

» Chapter 4 - Juche's Revolutionary Life View

» Chapter 5 - Revolutionary Self-destruction

By the end of the first year of training, informants and former students from the university state that self-destruction is "at the same level of going to the house next door to get water."

At the Kim Jong-il Political-Military College and its branch school, Bonghwa Political Academy, agents learn most of these skills during their freshman year. Bonghwa[205] trains combatants and anti-South Korea operatives (see Cultural Exchange Bureau in Section 9) in courses that last one to three years. Students also learn guerrilla tactics training on land, raids, ambushes, and assassinations as well as kidnap training, combat team training, and equipment training. Basic assault and combat team training also takes place as students participate in simulations of two to three people who work together to detonate facilities, improve military reconnaissance skills, practice liaison operations between fixed spies, and learn how to handle machine equipment.

Handling various military equipment is an equally vital skill, as students learn how to handle different kinds of weapons, ranging from small handguns to larger artillery. They also learn how to employ weapons on various means of transport, on land, and on sea. Maritime tactical training includes practice with navigation tactics, engine operation methods, underwater explosives, and underwater diving. Tactical seaborne navigation training is imperative as it teaches students how to perform a mission independently and how to utilize navigation technology correctly to guide the ship in the right direction. Usually, ships of five to 200-ton class can be operated independently by anyone who has graduated from college.[206]

Kim Jong-il began to demand strong physical and mental strength from reconnaissance agents after 1979. In that year, three North Korean infiltration agents spent ten days in South Korea and then successfully exfiltrated back to North Korea. From that point on, the combatants began to undergo rigorous marching training, carrying more than 20 kilograms of sand backpacks every day. Initially, the operatives were not given this training because the main activities were data collection or recruitment of people, but by 1984 they were also expected to march.

---

204 Pil-jae Kim, "북한의 암살 전문가' 양성조직: 김정일정치군사대학 (North Korea's Assassins Training Organization: Kim Jong-il Political College)."

205 Bonghwa Political Academy was formerly known as Kangdong Political Academy.

206 Pil-jae Kim, "북한의 암살 전문가' 양성조직: 김정일정치군사대학 (North Korea's Assassins Training Organization: Kim Jong-il Political College)," New Daily, January 25, 2013. https://www.newdaily.co.kr/site/data/html/2013/01/25/2013012500066.html.

In the fall of that year, North Korean agents working in Nepal were exposed and had to return to North Korea without bringing their passports or money home. After 40 days full of hardship, they breached the borders of three countries, including the Chinese border, on a march and returned to North Korea. They later emerged as heroes and met with Kim Jong-il.

From this point on, all North Korean agents had to run 4 km every day, 20 km on weekends, and 40 km at the end of the month. Upon graduation, they served in the KWP Operations Department. Many students who were expelled from school due to poor health were later hired as leaders of county-level KWP committees because of their high status and skills.[207]

Up to the 1990s, and before the internet became a popular form of communication, North Korean spies and other operatives employed Morse Code transmissions as a primary means of communication with their supervisors. The Kim regime would send out directions after midnight on the 1st, 11th, and 21st of every month via Pyongyang Broadcasting Radio. North Korean spies in South Korea had random number tables and a decryption table to interpret the transmission, and if they did not use these methods, they could not communicate.

207 Ibid; see also Pil-jae Kim, 북한의 사이버 남침 (North Korea's Cyber Invasion of the South) 59–60.

Section 8: RGB Leaders

Kim Jong-un (김정은)

As North Korea's Supreme Leader, Chairman of the Korean Workers' Party (KWP), Supreme Commander of the KPA, Chairman of the KWP Central Military Committee, and Chairman of the North Korean SAC, Kim Jong-un maintains great power over the RGB. Indeed, he demands that the RGB report to him directly rather than through the administrative military chain.

Kim was educated in Switzerland and therefore has a better understanding of the West and modern science than his father or grandfather. North Korea's cyber warfare capabilities have grown dramatically under his leadership. Kim Jong-un modernized his intelligence organizations during his reign, particularly North Korea's cyber warfare facilities.[208] In 2012, Kim Jong-un visited the 110th Research Institute to declare the unit to be North Korea's cyber headquarters.[209] During a visit to their unit on April 7th, 2013, Kim Jong-un told RGB hackers that RGB soldiers can use their outstanding capabilities to overpower other nations, especially those who have imposed sanctions against North Korea. In August 2013, Kim Jong-un told the RGB cadre that North Korea's nuclear, missile, and cyber warfare programs give North Korea a valuable strike capability. On June 28th, 2014, Kim Jong-un visited the RGB's 121st Bureau and told 121st personnel that they should thoroughly prepare to dominate the enemy's strongpoints.[210]

Kim Yong-chol. (김영철)

Kim Yong-chol was the first commander of the RGB when it was established in February 2009. In January 2016, he moved to serve as the KWP UFD Director. The UFD was responsible for all North Korean relations with South Korea, both diplomatic and politically aggressive. Kim commanded UFD sub-elements that addressed propaganda, psychological operations, spying, and subversion against South Korea. He was present with Kim Jong-un when directly negotiating with President Trump in Hanoi. Any assessment of Kim Yong-chol must be viewed through class-based family ties to the ruling family of the Kim regime and its related privilege. Kim Yong-chol has provided a lifetime of service in fighting militarily and diplomatically against South Korea.

208 Il-Gi Kim and Ho-hong Kim, "김정은 시대 북한의 정보기구" [North Korean Intelligence Organizations in the Kim Jong-un Era], inss.re.kr, December 31, 2020, 10. https://inss.re.kr/publication/bbs/rr_view.do?ntItId=409818.

209 To date, there is no further information indicating which unit is North Korea's cyber headquarters.

210 Il-Gi Kim and Ho-hong Kim, "김정은 시대 북한의 정보기구" [North Korean Intelligence Organizations in the Kim Jong-un Era]."

Kim served as a junior officer in the early 1960s in a DMZ police company (infantry company serving along North Korea's barrier fence line on the north side of the DMZ) of the KPA 15th Division. As a major, he served as a liaison officer with the KPA Military Armistice Commission at Panmunjom. This means Kim was a political officer in the KPA's GPB, since the GPB manages the North Korean side of Panmunjom (or Joint Security Area). Each DMZ police company has one political officer assigned to it for political training and indoctrination.

After being promoted to one-star brigadier general in February 1989 and serving as a deputy bureau chief at the MPAF, Kim participated in preparatory sessions of the North-South High-level Meetings, iterations one through eight, and then in the formal meetings one through eight from 1989 to July 1990. He served as the North-side Military Committee Chair of the North-South High-Level Meetings, sessions one to seven from September 1990 to September 1992, and as a member of the North-South Joint Military Committee, May 1992. He later served as North Korea's representative to the North-South General Officer Talks, March 2006 to December 2007. He also served as senior member of the Protocol Protection Element at the First North-South Summit in April 2000 in Pyongyang. Kim was promoted to two-star major general in March 2006, a three-star general in 2010, and a four-star general in February 2012, when he was awarded the prestigious Kim Jong-il Medal. He was demoted to Major General (two-star) in November 2012 (reason unknown). He was promoted again to General (four-star) in February 2013 and subsequently appointed Vice-chief of KPA General Staff circa 2013, concurrent with his then position of RGB Commander. His experience as both a political and intelligence officer has facilitated his path to the rank of 4-star general, North Korea's lead military intelligence officer, North Korea's lead civilian intelligence officer, and the party position of KWP vice-chairman.[211]

As with other North Korean elites, Kim's political experience is based on surviving the North's domestic political culture, which is rooted in personal competition for, and loyalty to, the Supreme Leader. As required of a military officer in the KPA, Kim has been a KWP member since his commissioning. Consequently, participation in political events has been the norm during his career, albeit in a political-military context. As for governmental political experience, Kim was voted into the Tenth Supreme People's Assembly (SPA), Songogu District #670, in July 1998; voted into the 12th SPA in April 2009; and voted into the 13th SPA in April 2014 in the Pukchang District. However, like nearly all other SPA assemblymen, political activities to attain their position are not a requirement as the KWP merely makes up the name list for nomination and election.

211 "북한주요인사 (North Korean Key Personnel)," Republic of Korea Ministry of Unification, 123-4. https://nkinfo.unikorea.go.kr/nkp/pblictn/view.do; see also "김영철 (Kim Yong-chol)," Republic of Korea Ministry of Unification. https://nkinfo.unikorea.go.kr/nkp/search/search.do?eicode=P_945&query=%EA%B9%80%EC%98%81%EC%B2%A0.

South Korean media generally identifies Kim Yong-chol as a political hardliner due to his consistent confrontational stance against South Korea during political and military activities. This appears to be a justified description of Kim Yong-chol due to his aggressive negotiation tactics during military diplomacy with South Korea throughout bilateral military talks in the 1980s and 1990s. Another solid reason for the hardliner reputation is Kim's reported role in North Korea's sinking of the South Korean Navy's frigate, Cheonan, and the shelling of Yeonpyeong Island in 2010, the hacking of the Sony USA Corporation in 2014, and the DMZ mine incident in 2015 that killed two South Korean soldiers. Confirming the hardliner attitude, Kim told a foreign businessman in late February shortly after becoming the new UFD director that "no matter what the level of sanctions, we will not falter."[212]

To add to this reputation, Kim visited the now closed Kaesong Industrial Complex (KIC) several times in the past decade while serving as the Director of the RGB. In doing so, South Korean workers at the KIC were very intimidated by Kim Yong-chol's aggressive attitude. The South Korean workers felt Kim Yong-chol only looked at the KIC from a military standpoint rather than from an economic one.[213] Kim also contributed to the North's December 1st measure, which prevented South Koreans from entering the KIC in 2008, and threatened to end the Armistice Agreement and to transform the South into a "sea of fire" after Pyongyang's third nuclear test.[214]

Kim was born in 1946 in Taesaeng, Ryanggang (Yanggang in South Korean toponymic terminology) Province and lived his life going to military schools and then entered the military as a career. Kim Yong-chol comes from a politically advantaged family background[215] that enabled him to go to the most prestigious military schools from kindergarten through college. From elementary through high school he attended Mangyongdae Academy, North Korea's most prestigious school for the nation's elite families. The school is reserved for the most privileged of North Korean families whose forebearers fought with Kim Il-sung against the Japanese in the 1930s and the 1940s or served honorably during the Korean War. From there, Kim attended the Kim Il-sung Military Academy, from which he was commissioned in the KPA.[216]

---

212 Song-un Cho, "김영철 '제재 많이 한다해도 우린 죽지 않는다'" [Kim Yong-chol: 'Although There are Many Sanctions, We Will Not Die'], Kukmin Ilbo, February 28, 2016. http://news.kmib.co.kr/article/view.asp?arcid=0923445004&code=11121400&cp=nv.

213 Ju-hwan Kim, "軍 '북한 사이버 도발 가능성 커' [Military: "High Probability of a North Korean Cyber Provocation"], YTN, February 14, 2016. http://www.ytn.co.kr/_ln/0101_201602141700419216.

214 "Kim Yong Chol reportedly named as N.K.'s United Front Department chief," DongA Ilbo, January 19, 2016. http://english.donga.com/List/3/01/26/520636/1.

215 In the Kim Regime, every individual North Korean is classified politically and socially based on their family background as of August 15, 1945. The "songbun" policy focuses on rating the Kim Il-sung family highest, families of the anti-Japanese partisan movement led by Kim Il-sung second, and Korean War loyalists and communist revolutionaries third as the upper echelons of North Korean society. See Robert Collins, *Marked for Life: Songbun – North Korea's Social Classification System*, Committee for Human Rights in North Korea, 2012.

216 "북한주요인사 (North Korean Key Personnel)," Republic of Korea Ministry of Unification, 123-4.; see also "김영철 (Kim Yong-chol)," Republic of Korea Ministry of Unification.

General Rim Kwang-il (림광일)

At the Plenary Meeting of the KWP in December 2019, Rim was promoted to a member of the Party Central Committee and assumed the post of Director, RGB.[217] In September 2021, Rim Kwang-il was appointed head of the general staff of the KPA according to the decision of the Politburo of the Party Central Committee. At the same time, he was elected as a candidate member of the Politburo of the Party Central Committee. Until May 2016, Col Gen Rim had been identified in the North Korean media as a KPA General Staff Vice Chief and the KPA General Staff Operations Bureau Director, equivalent to the U.S. Joint Staff J3. The North Korean media has stated that KPA Operations Bureau is now the KPA Operations General Bureau, a new expansive designation.[218] Since the Seventh Party Congress, then Col Gen Ri Yong-gil had been acknowledged as holding that position.[219] Before these positions, Rim was the Commander of the Second Combat Training Bureau, a special operations unit. South Korean intelligence has assessed that Rim is directly responsible for mission implementation of the landmine incident in August 2015 that maimed South Korean soldiers at the DMZ and was promoted to the Operations Bureau director position soon thereafter.[220]

Jang Gil-sung (장길성)

Born in 1947, Jang Gil-sung began serving as a leader within the Reconnaissance Bureau of the General Staff of the KPA in 1970. In 1984, Jang served as the KPA Reconnaissance Bureau Deputy Director, and then in 1993 he became Director. After the RGB was established in 2009, Jang served as the RGB Deputy Director. In 2017, he became the RGB Director and was promoted to the rank of Lieutenant General (also referred to as Colonel General) in the KPA. That same year he was also appointed a member of the North Korean Central Military Committee and was elected as a member of the KWP Central Committee at the Seventh Second Plenary Meeting of the KWP in October 2017. Reportedly, he was directly responsible for leading the operation to sink the South Korean Navy corvette Cheonan in 2010. Jang was replaced by General Rim Kwang-il in 2019.[221]

---

217 Seung-hyun Lee, "North Korea reorganizes party, government, and military leadership for 'frontal breakthrough'", Tongil News, January 1, 2020, https://www.tongilnews.com/news/articleView.html?idxno=130908.

218 Ji Seong-rim, "목함지뢰 도발 北림광일, 軍 작전총국장 승진 (Landmine Provocation – North's Rim Kwang-il Promoted to Korean People's Army Operations Bureau Director)," Yonhap, January 5, 2016. https://www.yna.co.kr/amp/view/AKR20160105118200038.

219 Yong-gol Lee and Byong-kwan Han, "북한 리영길 '화려한 부활' 배경과 의미 (The Background and Meaning of North Korea's Ri Yong-gil's Revival)", Ilyo Newspaper, November 18, 2016. https://ilyo.co.kr/?ac=article_view&entry_id=214567.

220 "N.Korea Honors Brass Behind DMZ Box Mine Attack," Chosunilbo, November 25, 2015. http://english.chosun.com/site/data/html_dir/2015/11/25/2015112501590.html.

221 Hyeon-woo In, "도쿄신문 '북한 신임 정찰총국장에 장길성 임명' [Tokyo Shimbun: 'North Korea Appoints Jang Gil-sung as New Reconnaissance General Director']," Hankook Ilbo, October 13, 2017. https://www.hankookilbo.com/News/Read/201710131796062755; Yoo Dong-yol, "대남간첩공작 본산, 정찰총국 [Headquarters of Anti-South Korean Espionage, Reconnaissance General Bureau]," Monthly North Korea (월간 북한), no. 524 (August 2015). Ministry of Unification, Republic of Korea. https://www.unikorea.go.kr/books/monthly/northkorea/?boardId=bbs_0000000000000045&mode=view&cntId=45744.

Han Chang-sun (한창선)

Colonel General Han Chang-sun, a three-star general, was appointed acting director of the RGB in 2016 after former commander Kim Yong-chol was promoted to KWP UFD Director. Before entering the RGB, Han served as commander of the KPA Seventh Corps and was promoted to three stars in 2010. He is also a member of the KWP Central Committee and holds the 128th position in the Kim regime's protocol ranking.[222]

Kim Son-il (김선일)

Kim was appointed RGB Deputy Director in September 2020, raising concerns that North Korea's cyber-warfare capability might be strengthened.[223]At the same time, he was promoted to KPA three-star rank (colonel general). Kim, who is in his fifties, previously served as Director of KWP Office 35 (also known as the External Intelligence Department).[224]

General Oh Kuk-ryol (오극렬)

Though now retired, General Oh remains one of the most influential figures in the Kim Regime, thanks to his extremely close family ties to the ruling Kim Family and highly competent, diverse military career. He is the son of Oh Jung-sung, one of Kim Il-sung's fellow resistance fighters against the Japanese in the 1930-1940s.[225] His father was part of a group known in North Korean propaganda as the partisan with the "five brothers of the guerrillas". Among the brothers, Oh Jung-hop is celebrated as a revolutionary who lost his life protecting Kim Il-sung during a Japanese attack (according to North Korean propaganda). In his honor, the KPA's "Seventh Regiment" carries the honorary title "Oh Jung-hop."[226] After Kim Jong-il's mother died, Kim was raised in Oh's household, and Oh became like an older brother to him, solidifying their lifelong relationship. Oh graduated from the Soviet Union's Frunze Academy (Russia's command and staff college) and rose through the ranks as an air force officer, eventually being appointed KPA Air Force Commander. In 1979, he became KPA Chief of General Staff, where he founded the Mirim Electronic Warfare College, now one of North Korea's premier cyber-warfare institutions.

---

222 Ik-Jae Choi and Jin-Kyu Kang, "Pyongyang Names New Spymaster," Korea Joongang Daily, July 29, 2016. http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=3021915.

223 Tae Joo Jeong, "Kim Son Il appointed as deputy director of Reconnaissance General Bureau," Daily NK. September 21, 2020. https://www.dailynk.com/english/kim-son-il-appointed-deputy-director-reconnaissance-general-bureau/.

224 Ibid.

225 "北오극렬 국방위 부위원장은 누구" [Who Is North Korea's New Vice Chairman of the National Defense Commission, O Kuk-ryol?], Daily NK, February 20, 2009 https://www.dailynk.com/%E5%8C%97%EC%98%A4%EA%B7%B9%EB%A0%AC-%EA%B5%AD%EB%B0%A9%EC%9C%84-%EB%B6%80%EC%9C%84%EC%9B%90%EC%9E%A5%EC%9D%80-%EB%88%84%EA%B5%AC/.

226 "『오중흡 7연대 모범 따라배우기』 궐기모임 진행" ['Learn from O Jung-hup's 7th Regiment Model' Campaign in Progress], North Korea Information Portal, January 31, 1996, https://nkinfo.unikorea.go.kr/nkp/trend/view.do?menuId=MENU_494&trendMngNo=2371.

Oh was dismissed from the Chief of Staff role in 1988 by Kim Il-sung after arguing that political commissars harmed military efficiency. Following reeducation, Kim Jong-il reinstated him in 1989 as Director of the KWP Military Department, and in 1992 as Director of the KWP Operations Department, where he oversaw the infiltration of North Korean agents into South Korea. Defector testimony portrays him, even in his 60s, as a "soldier's general," living and training alongside his field operatives under harsh conditions, relying on survival-style food. When the KWP Operations Department merged into the KPA Reconnaissance General Bureau, General Oh was appointed one of the three vice-chairmen of the National Defense Commission. As an expert in second-front operations, electronic warfare, and air operations, he became North Korea's foremost authority on hybrid warfare.[227]

Born in Jilin Province, China, he returned to North Korea with his family after liberation and enrolled in the Mangyongdae Revolutionary Academy. During the Korean War, he served as a fighter pilot in the Korean People's Army. After the war, he graduated from Kim Il-sung University and in 1962 spent two years at Frunze Military University. Upon his return, he was promoted to Major General of the Air Force (equivalent to a South Korean brigadier general), appointed dean of Kim Chaek Air Force University, and in 1967 received another promotion within the KPA Air Force.

Subsequently, he simultaneously served as a deputy member of the Supreme People's Assembly, a member of the KWP Central Committee, and deputy chief of the General Staff. In 1979, he was promoted to Chief of the General Staff of the KPA. He enjoyed a strong relationship with Kim Jong-il and continued rising through the ranks into the 1980s, eventually reaching lieutenant general.

However, Oh Kuk-ryol then questioned whether the political commissar system undermined field commanders' authority and asked Kim Jong-il if it could be abolished or weakened. Though Kim Jong-il responded positively, following the intervention by Kim Il-sung, he was chastised and dropped the issue. Oh also served as head of the KWP Civil Defense Department.

In February 2009, upon his election as Vice Chairman of the National Defense Commission, Oh re-emerged into high-level political prominence. At the Fourth Party Representatives' Meeting of the KWP, he was elected as a candidate member of the Central Politburo. According to reporter Joo Seong-ha, rather than returning to a civil-defense role after stepping down as chief of staff, he moved to the KWP Operations Department, where he held influence for two decades.

He wielded significant political and military influence due to his Korean War experience and being the son of one of Kim Il-sung's close associates. A hardliner, he favored tough policies toward South Korea and was instrumental in introducing advanced weapon systems, such as missiles, likely shaped by his Soviet education.

227 Operations Department Defector interviewed by Robert Collins. Seoul, South Korea. 1993.

However, his intense focus on military issues drew criticism from rivals such as Cho Myung-rok and Oh Jin-woo. Despite this, he weathered the regime transitions from Kim Il-sung to Kim Jong-il to Kim Jong-un. He passed away in February 2023. Meanwhile, Colonel General Ri Chang-ho has led the RGB since 2022.

Colonel Kim Kuk-song (alias) (김국송)

RGB Colonel Kim defected to South Korea in January 2014. Prior to that, he had an extensive career in North Korean intelligence. He served six years as an operational planner in the KWP Overseas Liaison Department, followed by ten years as operational strategy chief to the Director of the KWP Operations Department. He then spent five years as operational tactician assistant to the Director of the KWP Office 35,[228] and another five years as the strategy planner of the RGB's 5th Bureau.

Colonel Kim graduated from Pyongyang's Kumsong Middle School, then earned a degree in Computer Engineering from Kim Chaek Technology University and also completed studies at People's Economic College. Finally, he attended the Kim regime's premier operational agent training institute, the Kim Jong-il Political-Military College. He worked across four different intelligence agencies, contributing to projects such as implementing the 2007 Inter-Korea Summit, developing strategies on South Korea's political subjugation, and mapping North Korea's responses to U.S. nuclear forces. He was awarded the Kim Jong Il Medal.

Colonel Kim claims that Kim Jong-un "does not fully understand the lower levels of intelligence organization or personnel," and that the RGB reports directly to Kim Jong-un, while government institutions have access to much of its reporting. He also maintains that the KWP exerts more influence over the RGB than the KPA does. In interviews, he has stated that he knows who will be sent to assassinate him – the same team that killed Kim Jong-un's cousin, Ri Hanyong.[229]

Lee Son-sil (리선실)

Lee Son-sil is North Korea's most renowned female spy in South Korea, originally operating under the KWP Operations Department (now the RGB's 1st Bureau). Known as the "grandmother" of North Korean RGB spies, she used the alias Shin Son-nyo during her missions in South Korea and Lee Sun-hwa for her activities within the North Korean party network there.

228 KWP Office 35 was designated as such because it was located in the Fifth office on the third floor of the KWP's main office building.

229 "BBC 출연 고위 탈북자 김국성의 대남공작 비화 "남파간첩 너무 많아 일시 중단…청와대・국정원・국방부・국회가 활동무대 (BBC appearance Secret story of high-ranking North Korean refugee Kim Kook-song's spying on South Korea "Temporarily suspended due to too many South Korean spies... The Blue House, the National Intelligence Service, the Ministry of National Defense, and the National Assembly are active targets)." YouTube. December 16, 2021. https://www.youtube.com/watch?v=qFzDv66aSoo.

Originally from South Korea's Jeju Island, Lee defected to North Korea after losing her family during the 1948 rebellion on Jeju Island.[230] On October 6th, 1992, the NIS (then named National Security Planning Agency, or NSPA) identified that the South Korean Workers' Party (SKWP, a subversive organization of North Korea) had been disbanded. Lee Son-sil had been the SKWP leader, operating from the SKWP Central Regional Party (externally known as the National Liberation Patriotic Front) headquartered in Kangwon Province, South Korea. The SKWP was organized into four regional branches: Central South Korea, Gyeongin, Yeongnam, and Honam. The SKWP led the following South Korean liberal organizations: the August 28th Student Union, the May 1st Labor Union, and the November 11th Farmers' Union. There were several "assault teams" and covert cells operating under the Labor Union, as well as the "Voice of Salvation" broadcasting unit. The NSPA successfully arrested North Korean spies working under Lee Son-sil's management – Hwang In-o, Choi Ho-kyong, Eun Jae-hyong, and Jong Kyongsoo – at Hosan Beach in Samchok City, Kangwon Province, South Korea.[231]

Kim Jo-guk (김조국)

Kim Jo-guk serves as the First Vice-Director of the KWP Organization and Guidance Department (OGD) for the North Korean military. In this role, he oversees the ideological indoctrination and political loyalty of every member of the RGB.[232]

Choe Ryong-hae (최룡해)

General Choe served as GPB Director from 2012 to 2014. He is a long-time close friend of the ruling Kim family which has enabled his storied career. He began his career as a professor of politics at Kim Il Sung University. He has held senior posts in the KWP Central Committee, the Kim Il Sung Youth League, and the DPRK Supreme People's Assembly. After his service in the GPB, Choe served as the Vice Chairman of the former National Defense Commission (now the SAC). He also served as the Director of the powerful KWP Organization and Guidance Department. Most importantly, he has served in the KWP Politburo and the KWP Central Military Committee.

230 Young-woong Nam, "1992.10.06: 남한조선노동당 중부지역당 사건 (역사) (October 6, 1992: South Korea Workers' Party Central District Party Incident (History)," blog.naver, June 14, 2022. https://blog.naver.com/heronam78/222772941492.

231 Ibid.

232 Kim Il-Gi and Kim Ho-hong, "김정은 시대 북한의 정보기구" [North Korean Intelligence Organizations in the Kim Jong-un Era], inss.re.kr, December 31, 2020, 92. https://inss.re.kr/publication/bbs/rr_view.do?nttId=409818.

Hwang Pyong-so (황병서)

A career political officer, Hwang served as the GPB director from 26 April 2014 to 9 February 2018. His career's significant positions included Supreme People's Assembly, first Vice-director of the OGD, Vice-Chairman of the NDC, Vice-Chairman of the SAC, First Vice-Department Director of the KWP Central Committee. He retired with the rank of KPA Vice Marshal (five-star general).

Kim Jong-gak (김정각)

KPA Vice Marshal Kim served as GPB Director for a short time from February to May 2018. He also served as a member of the KWP Politburo, Minister of MPAF, and President of Kim Il-sung Military University.

Kim Su-gil (김수길)

General Kim served as GPB Director from May 2018 to January 2021. Other significant assignments include Chairman of the Pyongyang City KWP Committee (as important as senior party or cabinet positions), KWP Politburo member, 13th Supreme People's Assemblyman, Central Military Committee member, SAC member, and Gangwon Province KWP Secretary.

Kwon Yong-jin (권영진)

Vice Marshal Kwon served as GPB Director from 2021 to 2022. Significant assignments include member of the KWP Politburo, KWP CMC, and Minister of Defense.

Jong Kyong-taek (정경택)

General Jong served as the GPB Director from 2022 to present. Other significant assignments of his career include Minister of State Security, member of the KWP Politburo, the KWP CMC, and the SAC.

Cho Il-u (조일우)

Cho Il-u is the RGB Fifth Bureau Director. He was sanctioned by the European Union in June 2017.[233]

Oh Jong-gil (오정길)

Oh is believed to serve as the Deputy Director for RGB Operations in Southeast Asia.[234]

233 "유럽연합, '북한 미사일 발사 관련 유엔 결의 반영해 14명 추가 제재' [EU 'Imposed Additional Sanctions on 14 People in Response to UN Resolution Regarding North Korean Missile Launches']," SPN News, June 9, 2017.

234 Choi Woo-suk, "정찰총국 해외정보국에서 김정남 암살" [Assassination of Kim Jong-nam by the Reconnaissance General Bureau's Overseas Intelligence Bureau], Monthly Chosun, May 2017. https://monthly.chosun.com/Client/News/print.asp?ctcd=G&nNewsNumb=201705100040.

Section 9: RGB Sanctions and Arrests

In the past, the RGB used the Cheongsong Federation and the Yalu River Development Bank as a "money chain" to support its operations. This led the United Nations Security Council to sanction both organizations. The Yalu River Development Bank is affiliated with the Dancheon Commercial Bank, which had already been subject to sanctions for its involvement in North Korea's weapons of mass destruction.[235] South Korea's Defense Acquisition Program Administration reported that North Korea attempted to hack into Daewoo Shipbuilding & Marine Engineering's databases to obtain information on naval vessels and submarine designs, particularly nuclear-powered submarines.[236]

On January 2nd of 2015, President Obama signed Executive Order No. 13687, targeting the North Korean RGB, the Chosun Mining Development and Trading Company, the Chosun Dangun Trading Company, and ten individuals. This followed his December 19th, 2015 statement identifying North Korea as the mastermind of the Sony Pictures studio hacking incident, promising a proportional response. U.S. intelligence agencies, including the FBI, have pointed to the RGB as the primary perpetrator of the attack.[237]

The U.S. Department of Justice announced on February 17th, 2021, that it had indicted three North Korean hackers from the RGB on charges of extorting and soliciting more than $1.3 billion in cash and cryptocurrencies from banks and businesses worldwide.[238] The indictment, which was filed in December 2020, names the perpetrators as Park Jin-hyeok, Jeon Chang-hyeok (also spelled Jon Chang Hyok) and Kim Il, all tied to North Korea's top intelligence agency, the RGB. The RGB has operated hacking units known by various names such as 'Lazarus Group' and 'APT38' for an extended period.[239]

---

235 Eui-geun Ahn, "유엔 대북제재위, 북한 정찰총국 '돈줄' 묶었다 (UN Sanctions Committee on North Korea Ties Up Reconnaissance General Bureau's 'Money Chain')," JTBC News, May 3, 2012. https://news.jtbc.joins.com/article/article.aspx?news_id=NB10103251.

236 Yong-Han Park and Michael Lee, "Documents on South's naval vessels hacked," Korea Joongang Daily, June 21, 2021. https://koreajoongangdaily.joins.com/2021/06/21/national/defense/submarine-nuclear-hacking/20210621182100321.html.

237 Dong-yeol Yu, "북한 정찰총국 분석 (Analysis of North Korea's Reconnaissance General Bureau)," Korea Institute of Liberal Democracy, January 16, 2015, http://kild.or.kr/bbs/board.php?bo_table=policy&wr_id=180.

238 For an in-depth analysis of North Korea's cybercrime effectiveness, see Chain Analysis Team, "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High," chainanalysis.com, January 13, 2022. https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/.

239 Hyun-ki Lee, "북한 정찰총국의 실체" [Status of North Korea's Reconnaissance General Bureau], RFA, February 25, 2021. https://www.rfa.org/korean/weekly_program/c548cc2cc77c-bc15c0acc758-c8fcac04c9c4b2e8-1/weeklydiagnosis-02252021090845.html.

WANTED
BY THE FBI

JON CHANG HYOK

Conspiracy to Commit Wire Fraud and Bank Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

Aliases: Quan Jiang, Alex Jiang	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English, Korean, Mandarin Chinese

REMARKS

Jon is a North Korean citizen last known to be in North Korea. Jon has traveled to China in the past and has reported a date of birth in 1989.

CAUTION

Jon Chang Hyok is allegedly a state-sponsored North Korean hacker who is part of an alleged criminal conspiracy responsible for some of the costliest computer intrusions in history. These intrusions caused damage to computer systems of, and stole currency and virtual currency from, numerous victims.

Jon was alleged to be a participant in a wide-ranging criminal conspiracy undertaken by a group of hackers of the North Korean government's Reconnaissance General Bureau (RGB). The conspiracy comprised North Korean hacking groups that some private cybersecurity researchers have labeled the "Lazarus Group" and Advanced Persistent Threat 38 (APT38). For his part in the conspiracy, Jon is alleged to have been directly involved in the development and dissemination of malicious cryptocurrency applications targeting numerous cryptocurrency exchanges and other companies. On December 8, 2020, a federal arrest warrant was issued for Jon in the United States District Court, Central District of California, after he was charged with one count of conspiracy to commit wire fraud and bank fraud, and one count of conspiracy to commit computer fraud (computer intrusions).

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Los Angeles

Figure 14, Source: Eric Tucker, "US charges North Korean computer programmers in global hacks", AP News, February 17, 2021. https://apnews.com/article/us-charges-north-korea-global-hacks-3c8145431462830e8f80e1576f731577.

When the U.S. Department of Justice released its December 2020 indictment, attention turned to the possible impact on U.S.-North Korea relations. Even though the indictment was filed during the first Trump administration, the public release came as the Biden administration was reviewing its North Korea policy.[240] The indictment builds on the 2018 U.S. case against Park Jin-hyeok, who was involved in the 2014 Sony Pictures cyber-attack. This was the first time the U.S. charged a North Korean agent in a cybercrime, during which North Korea strongly opposed Sony Pictures' production and distribution of The Interview, a comedy film about the assassination of a North Korean leader.[241]

Park Jin-hyeok is also accused of hacking into the Central Bank of Bangladesh, stealing $81 million in 2016; orchestrating the WannaCry ransomware in 2017; and attempting to breach Lockheed Martin, a U.S. defense company, from 2016 to 2017. He is affiliated with the North Korean hacking group 'Lazarus' and the covert 'Joseon Expo Joint Venture Company,' a disguised company promoted by North Korea.

240 Hyun-ki Lee, "북한 정찰총국의 실체" [Status of North Korea's Reconnaissance General Bureau], RFA, February 25, 2021. https://www.rfa.org/korean/weekly_program/c548cc2cc77c-bc15c0acc758-c8fcac04c9c4b2e8-1/weeklydiagnosis-02252021090845.html.

241 Ibid.

This case is a criminal act that shows North Korea's increasing reliance on financial cyber-theft targeting its major exporting countries - many of which are subject to United Nations and U.S. sanctions. The U.S. Department of Justice also announced that a Canadian American man known to have aided North Korean hackers via money laundering pleaded guilty to the allegations.

"North Korean agents who use their keyboards and not guns to steal cryptocurrency wallets instead of bundles of cash are the world's bank robbers," said John Demers, assistant secretary of state for national security at the U.S. Department of Justice. Acting Prosecutor General Tracy Wilkinson of the Central District of California also said, "The criminal activity of North Korean hackers is widespread and long-lasting."[242]

In 2015, the year following the hacking incident, the Obama administration issued an executive order imposing significant sanctions on North Korea and the RGB.

On July 6th, 2020, U.S. Department of Justice announced its intent to prosecute North Korean Park Jin-hyeok for his role in the Sony Pictures hacking incident.[243] On July 25th, 2020, the U.S. Department of Justice filed a legal complaint against the RGB, targeting four companies for money laundering. Two of these entities were identified as having close ties to the RGB. The U.S. government claimed $1.91 million in damages from these companies due to "illegal financial activities."[244]

The Lazarus Group has also been sanctioned by the U.S. Department of Treasury, as designated below:

> Lazarus Group (a.k.a. "Appleworm"; a.k.a. "APT-C-26"; a.k.a. "Group 77"; a.k.a. "Guardians Of Peace"; a.k.a. "Hidden Cobra"; a.k.a. "Office 91"; a.k.a. "Red Dot"; a.k.a. "Temp.Hermit"; a.k.a. "The New Romantic Cyber Army Team"; a.k.a. "Whois Hacking Team"; a.k.a. "Zinc"), Potonggang District, Pyongyang, Korea, North; Secondary sanctions risk: North Korea Sanctions Regulations, sections 510.201 and 510.210 [DPRK3].[245]

242 Hyun-ki Lee, "북한 정찰총국의 실체" [Status of North Korea's Reconnaissance General Bureau], RFA, February 25, 2021. https://www.rfa.org/korean/weekly_program/c548cc2cc77c-bc15c0acc758-c8fcac04c9c4b2e8-1/weeklydiagnosis-02252021090845.html.

243 "' 북한 정찰총국, 대규모 자금세탁 배후' 美 연방검찰 (North Korea's Reconnaissance General Bureau Behind Massive Money Laundering, Say U.S. Federal Prosecutors)," Cheonji Ilbo, July 25, 2020. http://www.newscj.com/news/articleView.html?idxno=762182.headquarter.

244 Ibid.

245 "North Korea Designations; Global Magnitsky Designation," U.S. Department of the Treasury, September 13, 2019. https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20190913.

Andariel, a sub-group of the Lazarus Group, was sanctioned by the United States in 2019 for hacking gambling sites, including the Tornado Cash cryptocurrency tumbler, and stealing funds. Under Executive Order 13722, the Lazarus Group, Bluenoroff, and Andariel were sanctioned based on their ties to the RGB.[246] Two other important subsidiaries of the Lazarus Group are Silence Chollima and Starfall Chollima. The former is the organization that is infamous for hacking Sony Pictures in 2014 whereas the latter focuses on hacking financial institutions to steal money. Starfall Chollima also targeted International Financial Organization Society for Worldwide Interbank Financial Telecommunications (SWIFT) banking networks.[247]

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designated the RGB on January 2nd, 2015, under Executive Order 13687 for being an entity controlled by the North Korean government. Earlier, the RGB was included in the annex to Executive Order 13551 on August 30th, 2010. The United Nations also imposed sanctions on the RGB on March 2nd, 2016.[248]

On November 8th, 2022, the U.S Treasury Department sanctioned two individuals – North Korean national Ri Sok and Chinese national Yan Zhiyong – under North Korea Sanctions Regulations section 510.214. Both were employed by North Korea's Air Koryo, and they were sanctioned for transporting banned military equipment to North Korea. The RGB was named as one of the recipients of these transactions.[249]

246 Jamie Tarabay, "Korean Cybersecurity Experts Play Cat-and-Mouse With the North's Hackers," Bloomberg, September 2, 2022. https://www.bloomberg.com/news/articles/2022-08-31/north-korea-hackers-sometimes-leave-k-pop-clues-in-code?sref=hhjZtX76.

247 Seo-hee Choi, "북한 사이버공격 '세계적 위협..' 인터넷 연결 안돼도 해킹'" (North Korean cyber attack 'global threat,'" Hacking even without internet connection,)" Daum, February 21, 2018. https://news.v.daum.net/v/20180221033725718.

248 "Treasury Sanctions North Korea State-sponsored Malicious Cyber Groups," U.S. Department of the Treasury, September 13, 2019. https://home.treasury.gov/news/press-releases/sm774.

249 "Treasury designates DPRK Weapons Representatives," U.S. Department of the Treasury. November 8, 2022. https://home.treasury.gov/news/press-releases/jy1087.

Section 10: RGB and Human Rights

The RGB's operations have denied the human rights of countless South Korean citizens and other foreign nationals. This section will examine the denial of these human rights.

I. "Cybercrime" and International Human Rights Law

The RGB's cyber activities may constitute human rights violations, namely of the right to privacy (ICCPR, Art. 17) and freedom of expression (ICCPR, Art. 19). This is separate from the fact that these cyber activities can constitute other crimes, such as robbery. In the case of the Sony Pictures attack, it was reported that, to keep the movie The Interview from playing and expressing ideas unfavorable to the Kim family, North Korean hackers stole Sony executives' emails and personal data.[250]

Also, there is a broader point to be made that RGB cybercrimes benefit the regime and allow it to continue carrying out crimes against humanity. Money derived from cybertheft, for example, feeds the Pyongyang elite and strengthens the regime, emboldening North Korean leaders to bolster the nuclear weapons program despite sanctions. The utilization of such illegal profits in this way violates the International Covenant on Economic, Social and Cultural Rights (ICESCR), which protects every individual's right to an adequate standard of living. The Kim regime is not taking the appropriate steps to ensure the realization of this right, as resources are unequally distributed in North Korean society. Indeed, many housing resources are filtered towards the Pyongyang elite, military cadre, and weapons manufacturing groups.[251] The rest of North Korean citizens are thereby neglected and not given their right to a quality standard of living. Additionally, some wonder if the RGB may be behind the increasing numbers of "re-defections," having used cybercrime and threats to target North Korean escapees.

The fact that there is not an agreed-upon way to apply international law to cybercrime, nor a universal definition of "cybercrime," complicates the question of accountability as it relates to international cybercrimes. Although the United Nations is currently in the process of negotiating a "cybercrime treaty," the legislation is being met with criticism by non-governmental organizations who claim it could unintentionally harm the same people it intends to protect. Indeed, there are concerns that the treaty could be used by states like North Korea to carry out additional surveillance that targets individuals and groups and infringes on privacy and freedom of expression in the process.

250 Elias Groll, "Internal Emails Show Sony Struggling to Comprehend North Korea Threat," *Foreign Policy* (blog), June 25, 2025, https://foreignpolicy-com.ezproxy.princeton.edu/2015/04/16/internal-_emails_show_sony_struggling_to_comprehend_north_korea_threat/.

251 North Korea acceded to the ICESCR on September 14th, 1981.

The relevant International Covenant on Civil and Political Rights (ICCPR) articles are given below.[252] For context, North Korea acceded to the ICCPR in 1981.

ICCPR Article 17

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

ICCPR Article 19

1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others;

(b) For the protection of national security or of public order (ordre public), or of public health or morals.

II. Terrorism and International Human Rights Law

Many of the RGB's activities constitute acts of terrorism, specifically assassinations, kidnappings/abductions, and the bombing of Korean Air Flight 858. According to the UN, "terrorism can be broadly understood as a method of coercion that utilizes or threatens to utilize violence in order to spread fear and thereby attain political or ideological goals… The attack spreads fear as the violence is directed, unexpectedly, against innocent victims, which in turn puts pressure on third parties such as governments to change their policy or position. Contemporary terrorists utilize many forms of violence, and indiscriminately target civilians, military facilities and State officials among others."[253]

252 "International Covenant on Civil and Political Rights." *United Nations OHCHR*.. Adopted December 16, 1966. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

253 United Nations Office on Drugs and Crime, *Module 1: Introduction to International Terrorism.* In *Education for Justice University Module Series.* (2018), 1, https://www.unodc.org/documents/e4j/18-04932_CT_Mod_01_ebook_FINALpdf.pdf.

The human rights violations implicated in these activities—assassinations, kidnappings and abductions, and the bombing of Korean Air Flight 858 include the right to life, the right to liberty and security of person, the right to not be held in slavery or servitude, and the right to be free of torture or inhumane acts.

Abductions/kidnappings may also constitute enforced disappearance, which can be a crime against humanity if additional legal requirements are met. According to the United Nations:

> "Enforced disappearances occur when persons are arrested, detained or abducted against their will or otherwise deprived of their liberty by officials of different branches or levels of government or by organized groups of private individuals acting on behalf of, or with the support, direct or indirect, consent or acquiescence of the government, followed by a refusal to disclose the fate or whereabouts of the persons concerned or a refusal to acknowledge the deprivation of their liberty, which places such persons outside the protection of the law."[254]

The 2014 report of the UN Commission of Inquiry on the human rights situation in North Korea states that, according to a witness, the abduction of Mr. Chu (full name withheld) occurred in 2010. Mr. Chu, from Yanji City, Jilin Province, China, and a "Chinese man of Korean ethnicity were also involved in helping people flee North Korea."[255]

Article 2 in the International Convention for the Protection of All Persons from Enforced Disappearance states that an enforced disappearance is—

> "...the arrest, detention, abduction or any other form of deprivation of liberty by agents of the State or by persons or groups of persons acting with the authorization, support or acquiescence of the State, followed by a refusal to acknowledge the deprivation of liberty or by concealment of the fate or whereabouts of the disappeared person, which place such a person outside the protection of the law."[256]

The United Nations Working Group on Enforced Disappearance states:

> Enforced disappearance "is characterized by three cumulative elements (defined in A/HRC/16/48/Add.3):
>
> (1) Deprivation of liberty against the will of the person;
> (2) Involvement of government officials, at least by acquiescence;

254 United Nations Commission of Inquiry on Human Rights in the Democratic People's Republic of Korea, *Report of the detailed findings of the commission of inquiry on human rights in the Democratic People's Republic of Korea*, A/HRC/25/CRP.1, *UN OHCHR*, February 7, 2014. 270-271. https://documents.un.org/doc/undoc/gen/g14/108/71/pdf/g1410871.pdf (hereinafter "UN COI Detailed Findings Report").

255 UN COI Detailed Findings Report, 311.

256 *International Convention for the Protection of All Persons from Enforced Disappearance*, Article 2. *UN OHCHR*. Adopted December 20, 2006. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-protection-all-persons-enforced.

(3) Refusal to acknowledge the deprivation of liberty or concealment of the fate or whereabouts of the disappeared person.

A disappearance has a doubly paralyzing impact: on the victim, who is removed from the protection of the law, frequently subjected to torture and in constant fear for their lives; and on their families, ignorant of the fate of their loved ones, their emotions alternating between hope and despair, wondering and waiting, sometimes for years, for news that may never come. Enforced disappearance has frequently been used as a strategy to spread terror within societies. The feeling of insecurity generated by this practice is not limited to the close relatives of the disappeared but also affects their communities and society as a whole."

Below are the specific human rights violations as outlined in the International Covenant on Civil and Political Rights[257] organized by type of terroristic act employed by the RGB:

RGB Action	Rights Violated
Bombing of Korean Air Flight 858	ICCPR, Art. 6 – inherent right to life
Assassinations	ICCPR, Art. 6 – inherent right to life
Kidnapping/Abductions	ICCPR, Art. 7 – no one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment ICCPR, Art. 8 – no one shall be held in slavery or servitude ICCPR, Art. 9 – right to liberty and security of person. No one shall be subjected to arbitrary arrest or detention. No one shall be deprived of his liberty except on such grounds and in accordance with such procedure as are established by law.

Figure 15, Source: Credit to Lilli Duberstein, "RGB Action: Rights Violated", HRNK, June 17, 2025.

257 UN COI Detailed Findings Report, 311.

Section 11: The Future of the RGB

As we have explored, RGB operations have evolved in several ways since its inception as the major intelligence arm of the Kim regime.

First, provocations have become more intense and are larger in scope. Nuclear and missile tests, the sinking of the South Korean Navy corvette Cheonan, the KPA artillery bombardment of Yeonpyeong Island, and repeated cyber-attacks exemplify this escalation.

Secondly, infiltration routes into South Korea have expanded from traditional overland and seaborne routes to infiltration via third countries.

Third, the RGB is increasingly directing infiltrators to pose as North Korean escapees and then support North Korean operations in South Korea. As land and seaborne infiltration becomes more difficult, exploiting North Korean defector policies has become more common.

Fourth, communications between North Korea and RGB operatives in South Korea have changed from coded radio signals to connecting via the internet and social media.

Fifth, the RGB has expanded its operations to increase the effectiveness of pro-North Korean elements and information warfare in South Korea. Sixth, North Korea's cyberespionage capabilities are stronger than ever, as demonstrated by the hacking operations of the Lazarus Group.

Lastly, the Kim regime is expanding its operations against the South through technology. This latter effort is designed to isolate the South Korean Government, protect North Korea's policy lines, and further the regime's propaganda. These efforts target North Korean escapees and 2.4 million out of 7 million Koreans living in third countries.[258]

Keeping up with the times, the RGB is even beginning to move into the space warfighting domain. The North Korean leader has issued directives to the KPA to build an integrated command system that would link reconnaissance satellite feed with the RGB. Such linkage would aim to analyze enemy maneuvers and dispatch orders in real time.[259]

The vital interest of the Kim regime is survival. Its strategic aim is unification of the Korean Peninsula. The key conditions for this are the split of the ROK-U.S. alliance and the removal of U.S. forces from the peninsula.

---

258 Dong-yol Yoo, "대남간첩공작 본산, 정찰총국 [Headquarters of Anti-South Korean Espionage, Reconnaissance General Bureau]," Monthly North Korea (월간 북한), no. 524 (August 2015): 68–74. Ministry of Unification, Republic of Korea. https://www.unikorea.go.kr/books/monthly/northkorea/?boardId=bbs_0000000000000045&mode=view&cntId=45744.

259 Jeong Tae Joo, "Kim Jong Un orders creation of unified satellite intelligence command system," *Daily NK,* October 3, 2025. https://www.dailynk.com/english/kim-jong-un-orders-creation-of-unified-satellite-intelligence-command-system/?tztc=1.

The RGB plays a key role in serving these aims through subversion, coercion, extortion, and use of force.[260] As technology advances, the RGB will adjust its techniques and practices accordingly, continuing its violations of the human rights of the South Korean people, as well as the citizens in the North.

RGB operations will continue to impact the global community, as it further develops its conventional and cyber capabilities. Conventional capabilities are likely to benefit from North Korean involvement in the Russian aggression against Ukraine, especially in the use of drones as well as combined operations comprising drones, infantry, and artillery.

Cyber capabilities also appear to be enhanced through cooperation with Russian cyber-criminals. Shared infrastructure between the Lazarus and Gamaredon groups may reportedly set the stage for joint crypto theft, and also for espionage.[261] Lastly, based on past performance, one should expect Kim Jong-un to shift missions among intelligence agencies, rename and reorganize his intelligence community, further complicating the fight against these forces.

260 Colonel (Ret.) David Maxwell, Personal Communication with Author, December, 2022.

261 Anton Sokolin and Shreyas Reddy, "North Korean, Russian cybercriminals join forces for first time," *NKNews*, November 24, 2025. https://www.nknews.org/2025/11/north-korean-russian-cybercriminals-join-forces-for-first-time-report/.

Bibliography

1. Books, Journal Articles, and Official Sources

"Annual Report to Congress: Military and Security Developments Involving the Democratic People's Republic of Korea." Office of the Secretary of Defense. 2013. https://irp.fas.org/world/dprk/dod-2013.pdf.

"Annual Threat Assessment of the U.S. Intelligence Community." Office of the Director of National Intelligence. February 7, 2022.

Anonymous Former South Korean Intelligence Officer interviewed by Robert Collins. April 2022. Seoul, South Korea.

Bartlett, Jason. "Following the Crypto: Using Blockchain Analysis to Assess the Strengths and Vulnerabilities of North Korean Hackers." Center for a New American Security. February 2022. https://www.cnas.org/publications/reports/following-the-crypto.

Bermudez, Joseph Jr. North Korean Special Forces. Naval Institute Press. Annapolis, Maryland. 1998.

Collins, Robert. Marked for Life: Songbun – North Korea's Social Classification System. HRNK. Washington, D.C. 2012.

EC Members. "ACM International Collegiate Programming Contest." International Collegiate Programming Contest. July 28, 2022. https://icpc.global/community/history/factsheet/world-finals-2021-factsheet.pdf.

"Guidance on the Democratic People's Republic of Korea Information Technology Workers." U.S. Treasury Department. May 16, 2022. https://ofac.treasury.gov/media/923131/download?inline.

International Covenant on Civil and Political Rights. United Nations Office of the High Commissioner for Human Rights (OHCHR). Adopted December 16, 1966. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

International Convention for the Protection of All Persons from Enforced Disappearance, Article 2. United Nations Office of the High Commissioner for Human Rights (OHCHR). Adopted December 20, 2006. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-protection-all-persons-enforced.

Jun, Jenny, Scott LaFoy, and Ethan Sohn. "The Organization of Cyber Operations in North Korea." Center for Strategic and International Studies. December 18, 2014. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/141218_Cyber_Operations_North_Korea.pdf.

Keon, Michael. Korean Phoenix: A Nation from the Ashes. Prentice-Hall International. 1977. https://archive.org/details/koreanphoenixnat00keon.

Kim, Chong Woo and Carolina Polito. "The Evolution of North Korean Cyber Threats." The Asian Institute for Policy Studies. February 23, 2022. https://en.asaninst.org/contents/the-evolution-of-north-korean-cyber-threats/.

Kim, Il-Gi and Ho-hong Kim, "김정은 시대 북한의 정보기구" [North Korean Intelligence Organizations in the Kim Jong-un Era]. Institute for National Security Strategy. December 31, 2020. https://inss.re.kr/publication/bbs/rr_view.do?nttId=409818.

Kim, Kwang-jin. "North Korea's Terror Organizations and Their Possible Provocation." *Korean Studies Information Service System*. (북한의 대남테러 조직 및 테러전망). https://kiss.kstudy.com/DetailOa/Ar?key=50168279.

Kim, Pil-jae. "북한의 사이버 남침" (North Korea's Cyber Invasion of the South). Korean Journal of Public Security Association. Vol. 29, No. 4 (2020). https://www.kci.go.kr/kciportal/landing/article.kci?arti_id=ART002637515.

Maxwell, David. Personal Communication with Author. December 2022.

"Module 1: Introduction to International Terrorism. In Education for Justice University Module Series." United Nations Office on Drugs and Crime. https://www.unodc.org/documents/e4j/18-04932_CT_Mod_01_ebook_FINALpdf.pdf.

Narushige, Michishita. North Korea's Military-Diplomatic Campaigns, 1966-2008. New York: Routledge, 2010. https://www.tandfonline.com/doi/abs/10.1080/10163270409464070.

National Committee on North Korea. "Bylaws of the Korean Workers Party." National Committee on North Korea. May 9, 2016.

"North Korea Designations; Global Magnitsky Designation." U.S. Department of the Treasury. September 13, 2019. https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20190913.

"North Korean Miliary and Political Schools." Central Intelligence Agency. September 22, 1952. https://www.cia.gov/readingroom/docs/CIA-RDP82-00457R013900350003-1.pdf.

North Korean Tactics (ATP 7-100.2). Department of the Army. Washington, D.C. July 2020.

O, Tara. "North Korea Hacks South Korea's National Election Commission." East Asia Research Center. May 11, 2023. https://eastasiaresearch.org/2023/05/11/north-korea-hacks-south-koreas-national-election-commission/.

O, Tara. "How North Korea Launders Money Using Cryptocurrency to Evade Sanctions." East Asia Research. October 8, 2022. https://eastasiaresearch.org/2022/10/08/how-north-korea-launders-money-using-cryptocurrency-to-evade-sanctions/.

Oberdorfer, Don. The Two Koreas: A Contemporary History. Reading: Addison-Wesley. 1997. https://archive.org/details/twokoreascontemp00ober.

"『오중흡 7연대 모범 따라배우기』 궐기모임 진행" ['Learn from O Jung-hup's 7th Regiment Model' Campaign in Progress]. North Korea Information Portal. January 31, 1996.

Operations Department Defector interviewed by Robert Collins. 1993. Seoul, South Korea.

"Report of the detailed findings of the commission of inquiry on human rights in the Democratic People's Republic of Korea." UN OHCHR. February 7, 2014. https://documents.un.org/doc/undoc/gen/g14/108/71/pdf/g1410871.pdf.

ROK Defense White Paper. The Ministry of National Defense the Republic of Korea. 1990. https://books.google.com/books?id=BCjfAAAAMAAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

Sokolin, Anton and Shreyas Reddy, "North Korean, Russian cybercriminals join forces for first time," NKNews, November 24, 2025. https://www.nknews.org/2025/11/north-korean-russian-cybercriminals-join-forces-for-first-time-report/.

"Treasury designates DPRK Weapons Representatives." U.S. Department of the Treasury. November 8, 2022. https://home.treasury.gov/news/press-releases/jy1087.

"U.S., ROK Agencies Alert: DPRK Cyber Actors Impersonating Targets to Collect Intelligence." National Security Agency. June 1, 2023. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3413621/us-ROK-agencies-alert-dprk-cyber-actors-impersonating-targets-to-collect-intell/.

Voo, Julia, Irfan Hemani, and Daniel Cassidy. "National Cyber Power Index 2022." Harvard Belfer Center. September 2022. https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf.

Yamamoto, Yoshi. "Taken! North Korea's Criminal Abduction of Citizens of Other Countries." HRNK. 2011. https://www.hrnk.org/uploads/pdfs/Taken_LQ.pdf.

Yang, Jeong Yoon, So Jeong Kim, and Il Seok Oh. "Analysis on South Korean Cybersecurity Readiness Regarding North Korean Cyber Capabilities." Information Security Applications. August 2016. https://www.researchgate.net/publication/315858994_Analysis_on_South_Korean_Cybersecurity_Readiness_Regarding_North_Korean_Cyber_Capabilities.

Yoo, Dong-yol. "북한 정보기구의 변천과 현황 (North Korean Intelligence Organizations Change and Status). Vol. 11. No. 1 (2018). https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002354345.

Yu, Dong-yeol. "북한 정찰총국 분석 (Analysis of North Korea's Reconnaissance General Bureau)." Korea Institute of Liberal Democracy. January 16, 2015. http://kild.or.kr/bbs/board.php?bo_table=policy&wr_id=180.

"김영철 (Kim Yong-chol)." Ministry of Unification, Republic of Korea. https://nkinfo.unikorea.go.kr/nkp/search/search.do?eicode=P_945&query=%EA%B9%80%EC%98%81%EC%B2%A0.

북한/대남 도발. National Intelligence Service. https://www.nis.go.kr/AF/1_1_1.do.

"북한주요인사 (North Korean Key Personnel)," Republic of Korea Ministry of Unification.

"자유민주 사상전" (Liberal Democracy Ideological Warfare). Korea Institute of Liberal Democracy. July 26, 2019. https://www.kild.or.kr/.

2. Press and Online Articles

Ahn, Eui-geun. "유엔 대북제재위, 북한 정찰총국 '돈줄' 묶었다 (UN Sanctions Committee on North Korea Ties Up Reconnaissance General Bureau's 'Money Chain')." JTBC News. May 3, 2012. https://news.jtbc.joins.com/article/article.aspx?news_id=NB10103251.

Ahn, Sung-mi. "NK hackers stole $400m in cryptocurrency last year: report." The Korea Herald. March 20, 2022. http://www.koreaherald.com/view.php?ud=20220320000127&ACE_SEARCH=1.

Ahn, Sung-mi. "NK working with Russian cybercriminals: Sullivan," The Korea Herald. March 23, 2022. http://www.koreaherald.com/view.php?ud=20220323000619.

"AppleJeus: Analysis of North Korea's Cryptocurrency Malware." Cybersecurity and Infrastructure Security Agency. April 15, 2021. https://www.cisa.gov/uscert/ncas/alerts/aa21-048a.

"APT GROUP." Emagcon Security. April 9, 2015. https://emagcomsecurity.wordpress.com/2015/04/09/apt-advanced-persistent-threat-group/.

Bae, Jin-young. "북한 정찰총국, 가상화폐 거래소 해킹해 5억 7100만 달러 절취" [North Korea's Reconnaissance Bureau hacked cryptocurrency exchanges and stole $571 million]. Monthly Chosun. March 9, 2019. http://monthly.chosun.com/client/mdaily/daily_view.asp?Idx=6385&Newsnumb=2019036385.

Bajak, Frank and Hanna Arhirova. "Drone advances in Ukraine could bring new age of warfare." C4ISRNET. January 5, 2023. https://www.c4isrnet.com/battlefield-tech/2023/01/05/drone-advances-in-ukraine-could-bring-new-age-of-warfare/.

"BBC 출연 고위 탈북자 김국성의 대남공작 비화 "남파간첩 너무 많아 일시 중단… 청와대・국정원・국방부・국회가 활동무대 (BBC appearance Secret story of high-ranking North Korean refugee Kim Kook-song's spying on South Korea 'Temporarily suspended due to too many South Korean spies… The Blue House, National Intelligence Service, Ministry of National Defense, and the National Assembly are active

targets).” YouTube. December 16, 2021. https://www.youtube.com/watch?v=qFzDv66a-Soo.

Bermudez, Joseph Jr. “Special Report: A New Emphasis on Operations Against South Korea?” 38 North. June 11, 2010. http://38north.org/wp-content/uploads/2010/06/38north_SR_Bermudez2.pdf.

Bicker, Laura. “Drugs, arms, and terror: A high-profile defector on Kim’s North Korea.” BBC. October 11, 2021. https://www.bbc.com/news/world-asia-58838834.

Bremer, Ifang. “How a North Korean defector was coerced into spying for Pyongyang.” NK News. May 3, 2022. https://www.nknews.org/2022/05/how-a-north-korean-defector-was-coerced-into-spying-for-pyongyang/.

Bremer, Ifang. “Second North Korean defector this year found guilty of spying for Pyongyang.” NK News. May 13, 2022. https://www.nknews.org/2022/05/second-north-korean-defector-this-year-found-guilty-of-spying-for-pyongyang/.

Byun, Duk-kun. “N.Korea increasingly relies on cyber crimes to fund weapons programs: U.N. expert.” Yonhap. April 21, 2022. https://en.yna.co.kr/view/AEN20220421000200325?section=nk/nk.

Byun, Duk-kun. “White House highlights cryptocurrency risks, citing N.Korean cyber theft.” Yonhap. January 28, 2023. https://en.yna.co.kr/view/AEN20230128000200325?section=news.

Caesar, Ed. “The Incredible Rise of North Korea’s Hacking Army.” The New Yorker. April 19, 2021. https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army.

Cain, Geoffrey. “North Korea: How the Least-Wired Country Became a Hacking Superpower.” CNBC. May 27, 2013. https://www.cnbc.com/2013/05/26/north-korea-how-the-least-wired-country-became-a-hacking-superpower.html.

Chang, Dong-woo. “S.Korea slaps first sanctions on N.Korea over crypto theft, cyberattacks.” Yonhap. February 10, 2023. https://en.yna.co.kr/view/AEN20230210003300325?section=news.

Chawla,Vishal. “U.S. government warns that North Korea is targeting crypto firms.” The Block. April 19, 2022. https://www.theblockcrypto.com/post/142478/us-government-warns-that-north-korea-is-targeting-crypto-firms?utm_source=rss&utm_medium=rss.

Cho, Song-un. “김영철 ‘제재 많이 한다해도 우린 죽지 않는다’” [Kim Yong-chol: ‘Although There are Many Sanctions, We Will Not Die’]. Kukmin Ilbo. February 28, 2016. http://news.kmib.co.kr/article/view.asp?arcid=0923445004&code=11121400&cp=nv.

Choe, Sang Hun. "North Korean Hackers Stole U.S. South Korean Military Plans, Lawmaker Says." New York Times. October 10, 2017. https://www.nytimes.com/2017/10/10/world/asia/north-korea-hack-war-plans.htm.

Choi, Ha-young. "Korean-Chinese pastor-activist killed on North Korean border." NK News. May 2, 2016. https://www.nknews.org/2016/05/korean-chinese-pastor-activist-killed-on-north-korean-border/.

Choi, Ik-Jae and Jin-Kyu Kang. "Pyongyang Names New Spymaster." Korea JoongAng Daily. July 29, 2016. http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=3021915.

Choi, Seo-hee. "북한 사이버공격 '세계적 위협'..' 인터넷 연결 안돼도 해킹'" (North Korean cyber attack 'global threat'…"Hacking even without internet connection,)" Daum. February 21, 2018. https://news.v.daum.net/v/20180221033725718.

Choi, Seong. "Korea Computer Center – The Core of North Korea's IT Strategy." Korea IT Times. November 4, 2010. http://www.koreaittimes.com/news/articleView.html?idxno=11397.

Choi, Woo-suk. "정찰총국 해외정보국에서 김정남 암살" [Assassination of Kim Jong-nam by the Reconnaissance General Bureau's Overseas Intelligence Bureau]. Monthly Chosun. May 2017. http://monthly.chosun.com/client/news/viw.asp?ctcd=G&nNewsNumb=201705100040.

Cimpanu, Catalin. "U.S. Army report says many North Korean hackers operate from abroad." ZD Net. August 17, 2020. https://www.zdnet.com/article/us-army-report-says-many-north-korean-hackers-operate-from-abroad/.

"Circumstances of the Andariel Group Exploiting an Apache ActiveMQ Vulnerability." ASEC. November 17, 2023. https://asec.ahnlab.com/en/59318/.

Cook, James. Inside the Luxury Chinese Hotel Where North Korea Keeps Its Army of Hackers. December 2, 2014. https://www.businessinsider.com/photos-chinese-hotel-where-north-korea-keeps-hackers-2014-12.

Coppock, Mike. "The Korean War That Almost Was." History Net. Accessed February 23, 2022. https://www.historynet.com/the-korean-war-that-almost-was/?f.

Dark Reading Staff. "New Ransomware Variant Linked to North Korean Cyber Army." Dark Reading. May 5, 2022. https://www.darkreading.com/threat-intelligence/new-ransomware-variant-linked-to-north-korean-cyber-army.

"Database: North Korean Provocations." CSIS. December 20, 2019. https://beyondparallel.csis.org/database-north-korean-provocations/.

Fadilpašić, Sead. “Microsoft links Holy Ghost ransomware operation to North Korean hackers.” Tech Radar. July 15, 2022. https://www.techradar.com/uk/news/microsoft-links-holy-ghost-ransomware-operation-to-north-korean-hackers.

Getlen, Larry. “How North Korea’s dictator once kidnapped stars to make movies.” New York Post. January 18, 2015. https://nypost.com/2015/01/18/how-north-koreas-dictator-once-kidnapped-stars-to-make-movies/.

Groll, Elias. “Internal Emails Show Sony Struggling to Comprehend North Korea Threat.” Foreign Policy Magazine. June 25, 2025. https://fed.princeton.edu/cas/login?service=https%3A%2F%2Fidp.princeton.edu%2Fidp%2FAuthn%2FExternal%3Fconversation%3De1s1&entityId=http%3A%2F%2Fezproxy.princeton.edu.

Im, Tae-woo. “정보전사는 상위 0.001% 영재죠” (North Korean intelligence warriors are in the top 0.001% gifted). Maeil Business News. July 17, 2009. https://www.mk.co.kr/news/society/view/2009/07/389655/.

In, Hyeon-woo. “도쿄신문 ‘북한 신임 정찰총국장에 장길성 임명’ [Tokyo Shimbun: ‘North Korea Appoints Jang Gil-sung as New Reconnaissance General Director’].” Hankook Ilbo. October 13, 2017. https://www.hankookilbo.com/News/Read/201710131796062755.

Jeong, Tae Joo. “Kim Jong Un orders creation of unified satellite intelligence command system.” Daily NK. October 3, 2025. https://www.dailynk.com/english/kim-jong-un-orders-creation-of-unified-satellite-intelligence-command-system/?tztc=1.

Jeong, Tae Joo. “Kim Son Il appointed as deputy director of Reconnaissance General Bureau.” Daily NK. September 21, 2020. https://www.dailynk.com/english/kim-son-il-appointed-deputy-director-reconnaissance-general-bureau/.

Jewell, Ethan. “North Korean hackers stole $620 million from Pokemon-like blockchain game: FBI.” NK News. April 15, 2022. https://www.nknews.org/pro/north-korean-hackers-stole-620-million-from-pokemon-like-blockchain-game-fbi/.

Jewell, Ethan. “North Korea hackers weaponize holiday cheer in latest cyberattack against Russia.” NK News. January 4, 2022. https://www.nknews.org/pro/north-korea-hackers-weaponize-holiday-cheer-in-latest-cyberattack-against-russia/.

Ji, Da-gyum. “Crypto hacking behind N.Korea’s renewed nuclear ambition.” The Korea Herald. December 6, 2022. http://www.koreaherald.com/view.php?ud=20221206000676&ACE_SEARCH=1.

Ji, Da-gyum. “Tale of North Korea’s cyberterrorists: How they break into ‘unbackable’ crypto platforms and cash out.” The Korea Herald. December 12, 2022. https://www.koreaherald.com/view.php?ud=20221212000714.

Ji, Seong-rim. “목함지뢰 도발 北림광일, 軍 작전총국장 승진 (Landmine Provocation – North’s Rim Kwang-il Promoted to Korean People’s Army Operations Bureau Director).” Yonhap. January 5, 2016. https://www.yna.co.kr/amp/view/AKR20160105118200038.

Ji, Seong-rim. “北, 대남공작・사이버전 강화 예고..정찰일꾼대회” [North Korea foretells strengthening of cyber operations and cyber warfare…Reconnaissance Workers Demand]. Yonhap TV. June 18, 2015. https://v.daum.net/v/20150618151731851?f=o.

Johnson, A.L. “SWIFT attacker’s malware linked to more financial attacks.” Broad Community. May 26, 2016. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8ae1ff71-e440-4b79-9943-199d0adb43fc&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

Kang, Jin-kyu. “베일에 쌓인 북한 정보산업성 (North Korea’s Ministry of Information Industry in Veil).” NK Economy. July 7, 2021. https://www.nkeconomy.com/news/articleView.html?idxno=4440.

Khomami, Nadia. “North Korea: Isolated State with a Long History of Assassinations.” The Guardian. February 15, 2017. https://www.theguardian.com/world/2017/feb/15/north-korea-isolated-state-with-a-long-history-of-assassinations.

Kim, Chae-hwan. “’南 탈북 가족 때문에’…김정일 정치군사대학 졸업생, 전투원 임명 배제” [‘Because of the North Korean refugee family in the South’… Graduates of Kim Jong-Il Political and Military University, excluded from appointment as combatants. Daily NK. January 25, 2022. https://www.dailynk.com/20220125-4/.

Kim, Hyo-kyung. “항공우주산업 내부시스템도 해킹 당해..방사청 ‘조사 중’” (The aerospace industry’s internal system was also hacked…Defense Acquisition Program Administration “Investigating”). Daum News. June 30, 2021. https://v.daum.net/v/20210630215208595?f=o.

Kim, In-soon. “North Korea’s cyber-terrorism capabilities.” Daum News. February 21, 2016. https://news.v.daum.net/v/20160221170027854.

Kim, Jeong-hwan. “북한225국 지령 받는 간첩단 왕재산 적발” [North Korea’s 225 Bureau Gives Orders to Spy Group’s Wangjaesan]. Nodongilbo. September 3, 2011. https://www.nodongilbo.com/news/articleView.html?idxno=7527.

Kim, Ju-hwan. “‘軍, 북한 사이버 도발 가능성 커’ [Military: High Probability of a North Korean Cyber Provocation“]. *YTN*. February 14, 2016. http://www.ytn.co.kr/_ln/0101_201602141700419216.

Kim, Pil-jae. "‘북한의 암살 전문가’ 양성조직: 김정일정치군사대학 (North Korea‘s Assassins Training Organization: Kim Jong-il Political College).“*New Daily*. January 25, 2013. https://www.newdaily.co.kr/site/data/html/2013/01/25/2013012500066.html.

Kim, Seong-min. "北, 對南 사이버테러요원 3000명… 댓글 다는 전문 요원 만 200여명" [3,000 North anti-South terrorist agents…200 experts who comment]. Chosun Ilbo. August 13, 2013. https://www.chosun.com/site/data/html_dir/2013/08/13/2013081300176.html.

Kim, Soo-yeon. "N.Korea to step up cyber-attacks against S. Korea next year: Seoul spy agency." Yonhap. December 22, 2022. https://en.yna.co.kr/view/AEN20221222005900325.

"Kim given gift of drones on Russian trip." Korea Times. September 17, 2023. https://www.koreatimes.co.kr/www/nation/2023/09/103_359387.html.

"Kim Yong Chol reportedly named as N.K.'s United Front Department chief." DongaIlbo. January 19, 2016. http://english.donga.com/List/3/01/26/520636/1.

Knowles, Catherine. "Kaspersky uncovers details about active cyber-espionage campaign." IT Brief. September 13, 2022. https://itbrief.co.nz/story/kaspersky-uncovers-details-about-active-cyber-espionage-campaign.

Ko, Dong-hwan. "North Korea hacked 892 foreign policy experts." The Korea Times. December 25, 2022. https://www.koreatimes.co.kr/www/nation/2022/12/113_342329.html.

Kyodo. "Kim Jong-nam, half-brother of North Korean leader, met with suspected U.S. spy days before he was killed, court hears." SCMP. January 29, 2018. https://www.scmp.com/news/asia/east-asia/article/2131104/kim-jong-nam-half-brother-north-korean-leader-met-suspected-us.

Lakshmanan, Ravie. "Lazarus Group Exploits Zero-Day Vulnerability to Hack South Korean Financial Entity." The Hacker News. March 8, 2023. https://thehackernews.com/2023/03/lazarus-group-exploits-zero-day.html.

Lee, Hyun-ki. "북한 정찰총국의 실체" [Status of North Korea's Reconnaissance General Bureau]. Radio Free Asia. February 25, 2021. https://www.rfa.org/korean/weekly_program/c548cc2cc77c-bc15c0acc758-c8fcac04c9c4b2e8-1/weeklydiagnosis-02252021090845.html.

Lee, Jung-seok. "미외교협회 "북한 사이버 공격 위협적"…' 군사 역량 보고서' 평가 (U.S. Council on Foreign Relations: North Korea threatens cyberattacks…Evaluation of 'Military Capability Report')." Liberty Korea Post News. December 27, 2021. http://www.lkp.news/news/articleView.html?idxno=18434.

Lee, Michael. "North's hackers cash in on cryptocurrency." Korea JoongAng Daily. February 17, 2022. https://koreajoongangdaily.joins.com/2022/02/17/national/northKorea/blockchain-cryptocurrency-North-Korea/20220217175935352.html.

Lee, Seung-hyun. "북, '정면돌파전' 위한 당·정·군 지도부 인사개편" [North Korea Reshuffles Party, Government, and Military Leadership for 'Frontal Breakthrough']. Tongil News. January 1, 2020. https://www.tongilnews.com/news/articleView.html?idxno=130908.

Lee, Yong-gol and Byong-kwan Han. "북한 리영길 '화려한 부활' 배경과 의미 (The Background and Meaning of North Korea's Ri Yong-gil's Revival)." Ilyo Newspaper. November 18, 2016. https://ilyo.co.kr/?ac=article_view&entry_id=214567.

Lorenzo, Franceschi Bicchierai. "North Korean hackers exploited Chrome zero-day to steal crypto." Tech Crunch. August 30, 2024. https://techcrunch.com/2024/08/30/north-korean-hackers-exploited-chrome-zero-day-to-steal-crypto/.

Martin, Jack. "UN Report: South Korea Hardest Hit By North Korean Cyber Attacks." Coin Telegraph. August 13, 2019. https://cointelegraph.com/news/un-report-south-korea-hardest-hit-by-north-korean-cyber-attacks.

Mok, Yong-jae. "김정은 집권 이후 신설된 북 해킹조직 6개 (Six New North Korean Hacking Organizations Created Since Kim Jong-un's Rise to Power)." Radio Free Asia. November 22, 2017. https://www.rfa.org/korean/in_focus/ne-my-11222017102238.html.

Moon, Dong-hee. "정찰총국 인사조치에 對南 사이버공격 우려…어떤 부서길래" [Concerns about reinforcing cyberattacks in South Korea in response to personnel measures by the Reconnaissance General... What kind of department]. Daily NK. September 23, 2020. https://www.dailynk.com/%EC%A0%95%EC%B0%B0%EC%B4%9D%EA%B5%AD-%EC%9D%B8%EC%82%AC%EC%A1%B0%EC%B9%98%EC%97%90-%E5%B0%8D%E5%8D%97-%EC%82%AC%EC%9D%B4%EB%B2%84%EA%B3%B5%EA%B2%A9-%EC%9A%B0%EB%A0%A4-%EC%96%B4%EB%96%A4-%EB%B6%80/.

Mun, Dong Hui. "Hackers use S.Korean internet security agency as a disguise to mount cyberattacks." Daily NK. November 14, 2022. https://www.dailynk.com/english/hackers-use-south-korean-internet-security-agency-as-disguise-mount-cyberattacks/.

"N.Korea Honors Brass Behind DMZ Box Mine Attack." Chosunilbo. November 25, 2015. http://english.chosun.com/site/data/html_dir/2015/11/25/2015112501590.html.

"N.Korea's Vast Cyber Warfare Army." The Chosun Daily. August 13, 2013. http://english.chosun.com/site/data/html_dir/2013/08/13/2013081300891.html.

Nam, Young-woong. "1992.10.06: 남한조선노동당 중부지역당 사건 (역사) (October 6, 1992: South Korea Workers' Party Central District Party Incident (History)." Naver. June 14, 2022. https://blog.naver.com/heronam78/222772941492.

Nelson, Nate. “North Korea’s Top APT Swindled $1B From Crypto Investors in 2022.” Dark Reading. January 25, 2023. https://www.darkreading.com/remote-workforce/north-korea-apt-swindled-1b-crypto-investors-2022.

Newman, Lily Hay. “Good Luck Not Accidentally Hiring a North Korean Scammer.” Wired. May 30, 2022. https://www.wired.com/story/north-korean-it-scammer-alert/.

“North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High.” Chain Analysis. January 13, 2022. https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/.

“North Korean hackers stole $400m in digital assets last year, says report.” The Guardian. January 14, 2022. https://www.theguardian.com/world/2022/jan/14/north-korean-hackers-stole-400m-in-digital-assets-last-year-says-report.

“NSA ‘워너크라이 공격 배후 北 정찰총국’ 최종 확인 중국 내 북한 정찰총국 IP 발견” (NSA “North Korea Reconnaissance General Bureau behind WannaCry attack final confirmation North Korean Reconnaissance General Administration IP found in China). Clien. June 16, 2017. https://www.clien.net/service/board/park/10869637.

“One American Hacker Took Down North Korea’s Internet for Revenge.” Crossing Borders. February 23, 2022. https://www.crossingbordersnk.org/blog/one-american-hacker-took-down-north-koreas-internet-for-revenge/2022/2/23.

Oshin, Olafimihan. “Cyberattack suspected in North Korean internet outag.” The Hill. January 26, 2022. https://thehill.com/policy/international/asia-pacific/591473-cyberattack-suspected-in-north-korean-internet-outage.

Pak, Dong-hyeon. “<간첩협의 목사> 북한의 225국에 직접 연계 적발은 최초” [Spy Pastor: The first direct link to North Korea’s 225th Bureau]. PE News. November 24, 2015. https://www.penews.co.kr/news/articleView.html?idxno=110.

Pak, Hong-hwang. “북무인기 韓 등 6개국 부품 사용… 정찰총국 소행” [North Korean drones use parts from six countries, including South Korea…Conducted by the Reconnaissance General Bureau]. Seoul Shinmun. June 21, 2017. https://www.seoul.co.kr/news/politics/diplomacy/2017/06/22/20170622002009.

Park, Jaewoo and Hyung Jun. “Interview: U.S. cyber crime czar discusses readiness to stop North Korean threats.” Radio Free Asia. January 18, 2023. https://www.rfa.org/english/news/korea/fick-01182023163022.html.

Park, Yong-Han and Michael Lee. “Documents on South’s naval vessels hacked.” Korea JoongAng Daily. June 21, 2021. https://koreajoongangdaily.joins.com/2021/06/21/national/defense/submarine-nuclear-hacking/20210621182100321.html.

Pernet, Cedric. “North Korean cyberespionage actor Lazarus targets energy providers with new malware.” Tech Republic. September 14, 2022. https://www.techrepublic.com/article/lazarus-targets-energy-providers/.

Pernet, Cedric. “North Korean threat actors target news outlets and fintechs with a Google Chrome vulnerability.” Tech Republic. March 30, 2022. https://www.techrepublic.com/article/north-korean-threat-actors-target-news-outlets-fintechs-google-chrome-vulnerability/.

Raska, Michael. “North Korea’s Evolving Cyber Strategies: Continuity and Change.” De Gruyter. September 8, 2020. https://www.degruyter.com/document/doi/10.1515/sirius-2020-3030/html?lang=de.

Reddy, Shreyas. “Explainer: How North Korea is developing drones into weapons of war.” NK News. December 29, 2022. https://www.nknews.org/2022/12/explainer-how-north-korea-is-developing-drones-into-weapons-of-war/.

“S.Korea launches jets, fires shots after North flies drones.” National Public Radio. December 26, 2022. https://www.npr.org/2022/12/26/1145530094/s-korea-launches-jets-fires-shots-after-north-flies-drones#:~:text=The%20military%20responded%20by%20firing,according%20to%20the%20Defense%20Ministry.

Sanger, David E., David D. Kirkpatrick, and Nicole Perlroth. “The World Once Laughed at North Korean Cyberpower. No More.” New York Times. October 15, 2017. Accessed January 1, 2022. https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

Silver, Stephen. “North Korea’s Spy Strategy: Pose as Defectors.” National Interest. January 22, 2022. https://nationalinterest.org/blog/reboot/north-koreas-spy-strategy-pose-defectors-199480.

“S Korea considering buying Israeli drone detection system: source.” Yonhap News. January 8, 2023. https://en.yna.co.kr/view/AEN20230108000900325?section=nk/nk.

Smith, Josh. “Crypto hacks stole record $3.8 billion in 2022, led by North Korea groups – report.” Reuters. February 7, 2023. https://www.reuters.com/technology/crypto-hacks-stole-record-38-billion-2022-led-by-north-korea-groups-report-2023-02-01/.

Song, Jong-seok. “Cybersecurity emerges as top priority.” Korea JoongAng Daily. June 2, 2022. https://koreajoongangdaily.joins.com/2022/06/02/opinion/columns/cybersecurity-military/20220602195420736.html.

Specia, Megan. “Built for Invasion, North Korean Tunnels Now Flow With Tourists.” New York Times. November 4, 2017. https://www.nytimes.com/2017/11/04/world/asia/north-korea-south-korea-demilitarized-zone-tunnel-tourism.html.

SPN News Seoul Pyongyang News Editorial Team. "유럽연합, '북한 미사일 발사 관련 유엔 결의 반영해 14명 추가 제재' [EU 'Imposed Additional Sanctions on 14 People in Response to UN Resolution Regarding North Korean Missile Launches']." SPN News. June 9, 2017.

Stahie, Silviu. "North Korea Responsible for 30% of All Cryptocurrency Stolen Since 2017." Bitdefender. May 18, 2023. https://www.bitdefender.com/blog/hotforsecurity/north-korea-responsible-for-30-of-all-cryptocurrency-stolen-since-2017/.

Sun-young Park. "A Lethal Trail to the Blue House." Korea JoongAng Daily. March 29, 2009. https://koreajoongangdaily.joins.com/2009/03/29/features/A-lethal-trail-to-the-Blue-House/2902872.html.

Tarabay, Jamie. "Korean Cybersecurity Experts Play Cat-and-Mouse with the North's Hackers." Bloomberg. September 2, 2022. https://www.bloomberg.com/news/articles/2022-08-31/north-korea-hackers-sometimes-leave-k-pop-clues-in-code?sref=hhjZtX76.

"Targeted attacks by Andariel Threat Group, a Subgroup of the Lazarus." Ahn Lab, June 23, 2018.

Tassev, Lubomir. "Cryptocurrency Theft Remains Key Revenue Source for North Korea, UN Report Says." Bitcoin. February 6, 2022. https://news.bitcoin.com/cryptocurrency-theft-remains-key-revenue-source-for-north-korea-un-report-says/.

Taylor, David. "Study reveals North Korean cyber-espionage has reached new heights." The Guardian. February 20, 2018. https://www.theguardian.com/world/2018/feb/20/north-korea-cyber-war-spying-study-fire-eye.

"The General Bureau is the 'headquarters of operations against South Korea' that integrates the Party Operations Department and the Military Reconnaissance Bureau."〔출처:중앙일보〕Korea JoongAng Daily. April, 4, 2010. https://www.joongang.co.kr/article/4121510.

Weisensee, Nils. "Hackers likely helped North Korea build hypersonic missile: United Nations report." NK News. February 8, 2022. https://www.nknews.org/2022/02/hackers-likely-helped-north-korea-build-hypersonic-missile-un-report/.

Williams, Martyn. "North Korea Gets a New PDA." North Korea Tech. November 5, 2010. https://www.northkoreatech.org/2010/11/05/north-korea-gets-a-new-pda/.

Yang, Man-soo. "황장엽 암살기도 지령내린 북한 정찰총국은 " [The North Korean Reconnaissance General Bureau, which ordered the assassination of Hwang Jang-yop]. Today Korea. April 14, 2021. http://www.todaykorea.co.kr/news/articleView.html?idxno=107567.

Yoo, Dong-yol. "대남간첩공작 본산, 정찰총국 [Headquarters of Anti-South Korean Espionage, Reconnaissance General Bureau]." Monthly North Korea. No. 524 (August 2015).

Ministry of Unification, Republic of Korea. https://www.unikorea.go.kr/books/monthly/northkorea/?boardId=bbs_0000000000000045&mode=view&cntId=45744.

Yoo, Cheong-mo. "N.K. hacking group monitored ex-ministers' emails for months: police." Yonhap. June 7, 2023. https://en.yna.co.kr/view/AEN20230607006200315?section=nk/nk.

Yoo, Cheong-mo. "N.Korea massacred over 1,100 Christians, Catholics during Korean War: report." Yonhap. February 22, 2022. https://en.yna.co.kr/view/AEN20220222002800315?section=search.

Yoo, Dong-yol. "북한 정찰총국 해부 (Analyzing North Korea's Reconnaissance General Bureau)." kild.or.kr. July 26, 2019. https://www.kild.or.kr/bbs/board.php?bo_table=activity_08&wr_id=30.

Young, Benjamin R. "The Emerging North Korean-Russian Cybercrime Partnership." National Interest. March 21, 2022. https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/emerging-north-korean-russian.

"北오극렬 국방위 부위원장은 누구" [Who Is North Korea's New Vice Chairman of the National Defense Commission, O Kuk-ryol?]." Daily NK. February 20, 2009. https://www.dailynk.com/%E5%8C%97%EC%98%A4%EA%B7%B9%EB%A0%AC-%EA%B5%AD%EB%B0%A9%EC%9C%84-%EB%B6%80%EC%9C%84%EC%9B%90%EC%9E%A5%EC%9D%80-%EB%88%84%EA%B5%AC/.

"' 북한 정찰총국, 대규모 자금세탁 배후' 美 연방검찰" (North Korea's Reconnaissance General Bureau Behind Massive Money Laundering, Say U.S. Federal Prosecutors). Cheonji Ilbo. July 25, 2020.

업데이트, '北 직접남파 간첩' 현정부 첫 체포." Donga News. September 29, 2009. https://www.donga.com/news/Politics/article/all/20060822/8342386/1.

"탈북자 '90년대초 청와대에 남파간첩 근무'…국정원 '사실무근'" [North Korean Refugee 'Working as a South Korean spy at the Blue House in the early 1990s'...NIS 'groundless'). YouTube. October 11, 2021. https://www.youtube.com/watch?v=Q9w0G-CfPDTE&list=PLG0wy_ZMVm9Ybr8asUTmSG3OJ28KpcVBT&index=10.

Figure Bibliography

Figure 1, Source: Joseph Bermudez, "38 NORTH SPECIAL REPORT: A NEW EMPHASIS ON OPERATIONS AGAINST SOUTH KOREA?" 38 North, June 11, 2010. https://www.38north.org/wp-content/uploads/2010/06/38north_SR_Bermudez2.pdf.

Figure 2, Source: Joseph Bermudez, "38 NORTH SPECIAL REPORT: A NEW EMPHASIS ON OPERATIONS AGAINST SOUTH KOREA?" 38 North, June 11, 2010. https://www.38north.org/wp-content/uploads/2010/06/38north_SR_Bermudez2.pdf.

Figure 3, Source: Dagyum Ji, “Seoul to mass produce air defense radars to counter N. Korean drones”, NK News, July 14, 2017, https://www.nknews.org/2017/07/seoul-to-mass-produce-air-defense-radars-to-counter-n-korean-drones/.

Figures 4 and 5, Source: Park Sun-yeong, “N. Korea threatens use of weapons to control border with China,” Korea Joongang Daily, March 29, 2009. https://koreajoongangdaily.joins.com/2009/03/29/features/A-lethal-trail-to-the-Blue-House/2902872.html.

Figure 6, Source: North and South Development, [Special Feature on National Liberation Day of Korea], North and South Development, August 16, 2024. https://sand.or.kr/kr/opinion/opinion.php?bgu=view&idx=23358&ckattempt=1.

Figure 7, Source: Kim Chae Hwan “南탈북 가족 때문에” …김정일정치군사대학 졸업생, 전투원 임명 배제”, Daily NK, January 25, 2022. https://www.dailynk.com/20220125-4/.

Figure 8, Source: Dagyum Ji, “Tale of North Korea’s cyberterrorists: How they break into ‘unhackable’ crypto platforms and cash out”, Korea Herald, December 12, 2022. https://www.koreaherald.com/article/3017774.

Figure 9, Source: Dagyum Ji, “Tale of North Korea’s cyberterrorists: How they break into ‘unhackable’ crypto platforms and cash out”, Korea Herald, December 12, 2022. https://www.koreaherald.com/article/3017774.

Figure 10, Source: U.S. Department of Treasury, “GUIDANCE ON THE DEMOCRATIC PEOPLE’S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS” U.S. Department of Treasury, May 16, 2022. https://ofac.treasury.gov/media/923126/download?inline.

Figure 11, Source: Dagyum Ji, “Crypto hacking behind N. Korea’s renewed nuclear ambition”, Korea Herald, December 6, 2022. https://www.koreaherald.com/article/3015095.

Figure 12, Source: Emagcom Security. “APT (Advanced Persistent Threat) Group”https://emagcomsecurity.wordpress.com/2015/04/09/apt-advanced-persistent-threat-group/.

Figure 13, Source: Michael Raska, “North Korea’s Evolving Cyber Strategies: Continuity and Change”, De Gruyter Brill, September 8, 2020. https://www.degruyterbrill.com/document/doi/10.1515/sirius-2020-3030/html?lang=de.

Figure 14, Source: Eric Tucker, “US charges North Korean computer programmers in global hacks”, AP News, February 17, 2021. https://apnews.com/article/us-charges-north-korea-global-hacks-3c8145431462830e8f80e1576f731577.

Figure 15, Source: Credit to Lilli Duberstein, “RGB Action: Rights Violated”, June 17, 2025.

The Committee for
Human Rights in North Korea
북한인권위원회