North Korea Is Not Crazy

www.recordedfuture.com/north-korea-cyber-activity/

The Recorded Future Blog

by Insikt Group on June 15, 2017

Intent is critical to comprehending North Korean cyber activity.

Understanding North Korean national objectives, state organizations, and military strategy are key to, and often missing from, discussions about attributing North Korean cyber activity. Frequently, senior political leaders, cyber security professionals, and diplomats describe North Korean leaders or their respective actions as “crazy,” “erratic,” or “not rational.” This is not the case. When examined through the lens of North Korean military strategy, national goals, and security perceptions, cyber activities correspond to their larger approach.

Recorded Future research reveals that North Korean cyber actors are not crazy or irrational: they just have a wider operational scope than most other intelligence services.

This scope comprises a broad range of criminal and terrorist activity, including illegal drug manufacturing and selling, counterfeit currency production, bombings, assassination attempts, and more. The National Security Agency (NSA) has attributed the April WannaCry ransomware attacks to North Korea’s intelligence service, the Reconnaissance General Bureau (RGB). We assess that use of ransomware to raise funds for the state would fall under both North Korea’s asymmetric military strategy and ”self-financing” policy, and be within the broad operational remit of their intelligence services.

Background

The Democratic People's Republic of Korea (DPRK or North Korea) is a hereditary, Asian monarchy with state, party, and military organizations dedicated to preserving the leadership of the Kim family. North Korea is organized around its communist party, the Korean Worker's Party (KWP), and the military, the Korean People's Army (KPA).

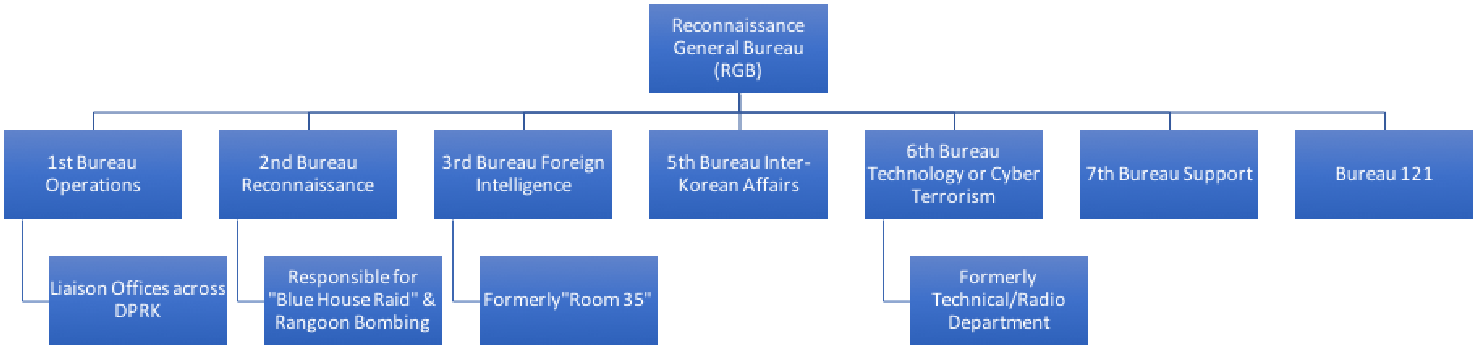
The Reconnaissance General Bureau (RGB), also known as "Unit 586," was formed in 2009 after a large restructure of several state, military, and party intelligence elements. Subordinate to the KPA, it has since emerged as not just the dominant North Korean foreign intelligence service, but also the center for clandestine operations. The RGB and its predecessor organizations are believed responsible for a series of bombings, assassination attempts, hijackings, and kidnappings commencing in the late 1950s, as well as a litany of criminal activities, including drug smuggling and manufacturing, counterfeiting, destructive cyber attacks, and more.

Satellite Image of the RGB Southern Operations Building in Pyongyang. (Source)

As North Korea's lead for clandestine operations, the RGB is also likely the primary cyber operations organization as well. As described by the Center for Strategic and International Studies in 2015 report:

The RGB is a hub of North Korean intelligence, commando, and sabotage operations. The RGB history of its leadership and component parts paints a picture of a one-stop shop for illegal and clandestine activity conducted outside the DPRK. The RGB and, prior to 2009 its component parts, have been involved in everything from maritime-inserted commando raids to abductions and spying. For the RGB to be in control of cyber assets indicates that the DPRK intends to use these assets for provocative purposes.

The RGB probably consists of seven bureaus; six original bureaus and a new seventh (Bureau 121) that was likely added sometime after 2013.


Reconnaissance General Bureau (RGB)
1st Bureau Operations
Liaison Offices across DPRK
2nd Bureau Reconnaissance
Responsible for "Blue House Raid" & Rangoon Bombing
3rd Bureau Foreign Intelligence
Formerly"Room 35"
5th Bureau Inter-Korean Affairs
6th Bureau Technology or Cyber Terrorism
Formerly Technical/Radio Department
7th Bureau Support
Bureau 121

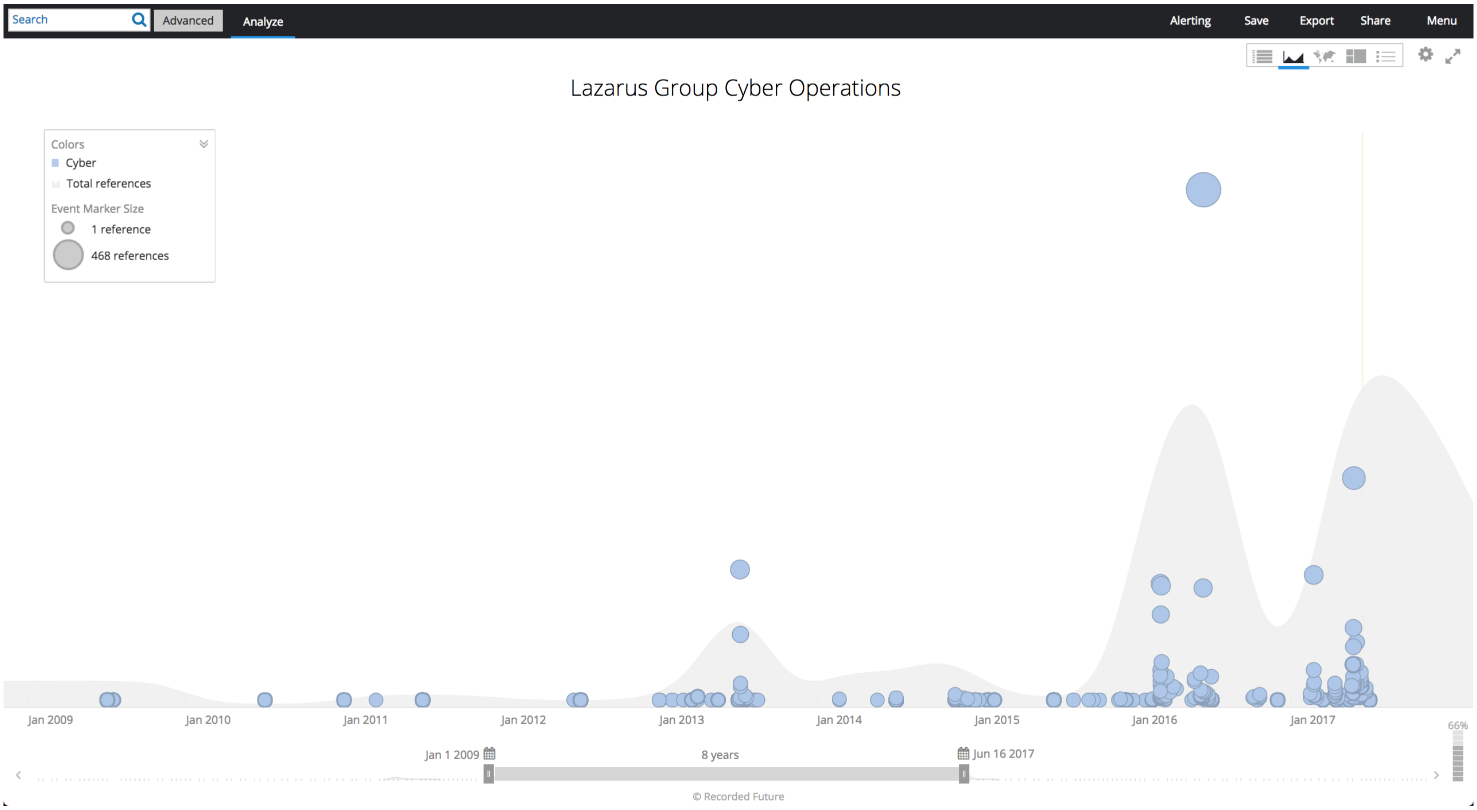
RGB organizational chart, compiled with information from The Korea Herald, 38 North, and CSIS.

Bureau 121 is probably North Korea's primary cyber operations unit, but there are other units within the KPA and KWP that may also conduct cyber operations.

Attribution of specific cyber activity to the North Korean state or intelligence organizations is difficult, and up until recently, circumstantial. On June 12, US-CERT released a joint technical alert that summarized analysis conducted by the U.S. Department of Homeland Security (DHS) and FBI on the “tools and infrastructure *used by cyber actors of the North Korean government* to target the media, aerospace, financial, and critical infrastructure sectors in the United States and globally.”

This alert marked the first time the U.S. government linked threat actor groups and malware long-suspected to be utilized by North Korean state-sponsored actors with the with North Korean government itself. DHS and FBI explicitly identified two threat actor groups, Lazarus Group and Guardians of Peace, and three tools, Destover, Wild Positron/Duuzer, and Hangman, as used by the North Korean government. While the FBI and DHS identified many indicators of compromise, Yara rules, and network signatures, the report did not provide any evidence supporting the attribution to the North Korean government or details on which organization or unit might be responsible.

Lazarus Group, now known to be North Korean state-sponsored actors, have been conducting operations since at least 2009, with a DDoS attack on U.S. and South Korean websites using the MYDOOM worm. Until late 2015, Lazarus Group cyber activities primarily focused on South Korean and U.S. government and financial organizations, including destructive attacks on South Korean banking and media sectors in 2013 and highly publicized attack on Sony Pictures Entertainment in 2014.



Timeline of Lazarus Group cyber operations since 2009.

In early 2016, a new pattern of activity began to emerge in an unusual operation against the Bangladesh Central Bank. Actors obtained the legitimate Bangladesh Central Bank credentials for the SWIFT interbank messaging system and used them to attempt to transfer $951 million of the bank’s funds to accounts around the world. A few simple errors by the actors (and some pure luck) allowed central bankers to prevent the transfer of or recover most of the funds, but the attackers ended up getting away with nearly $81 million.

The National Security Agency (NSA) has attributed this attack on the Bangladesh Central Bank to the North Korean state, however, the investigation within the U.S. government is still ongoing. Threat analysts from numerous companies have attributed this attack and subsequent attacks on banks around the world through early 2017 to the

Lazarus Group (which DHS, FBI, and NSA have all linked to the North Korean government over the past three days).

According to a *Washington Post* report published on June 14, the NSA has compiled an intelligence assessment on the WannaCry campaign and has attributed the creation of the WannaCry worm to "cyber actors sponsored by" the RGB. This assessment, which was apparently issued internally last week, cited "moderate confidence" in the attribution and ascribed the April campaign as an "attempt to raise revenue for the regime."

The attacks on the Bangladesh Central Bank, additional banks around the world, and the WannaCry ransomware campaign represent a new phase in North Korean cyber operations, one that mirrors the phases of violence and criminality North Korea has passed through over the past 50 years. We will examine these phases later in this post.

The broad operational range of known and suspected North Korean cyber operations has for years raised questions about the rationality of North Korean leadership, possible motivations and benefits for the country from this type of cyber activity, and why North Korea would deny responsibility for these attacks. Recorded Future research addresses these questions by examining the whole picture and pairing geopolitical and strategic intelligence with threat intelligence.

Analysis

Digging into some of these past North Korean activities is important to add context to the cyber operations we have tracked since 2009. North Korea's engagement in a wide range of criminal and terrorist activities is part of its broad national strategy, which employs asymmetric operations and surprise attacks to overcome North Korea's conventional national power deficit.

According to an interview with a former U.S. State Department official, and North Korea expert, in *Vanity Fair*, "crime, in other words, has become an integral part of North Korea's economy. 'It not only pays, it plays to their strategy of undermining Western interests.[1]'"

It is critical to place North Korea's criminal and cyber activity in the context of its larger military and national security strategies which support two primary objectives:

1. Perpetuation of the Kim regime,
2. Unification of the Korean peninsula under North Korean leadership.

A 2016 University of Washington study succinctly summarizes North Korea's asymmetric military strategy:

Since the end of the Korean War, North Korea has developed an asymmetric military strategy, weapons, and strength because its conventional military power is far weaker than that of the U.S. and South Korea. Thus, North Korea has developed three military strategic pillars: surprise attack; quick decisive war; mixed tactics. First, its surprise attack strategy refers to attacking the enemy at an unexpected time and place. Second, its quick decisive war strategy is to defeat the South Korean military before the U.S. military or international community could intervene. Lastly, its mixed tactics strategy is to use multiple tactics at the same time to achieve its strategic goal.

Despite their near-constant tirade of bellicose rhetoric and professions of strength, North Korea fundamentally views the world from a position of weakness, and has developed a national strategy that utilizes its comparative strengths — complete control over a population of 25 million people and unflinching, amoral devotion to the Kim hereditary dynasty.

In this context, criminality, terrorism, and destructive cyber attacks all fit within the North Korean asymmetric military strategy which emphasizes surprise attacks and mixed tactics. The criminality and cyber attacks also have the added bonus of enabling North Korea to undermine the very international economic and political systems that constrain and punish it.

Evidence is mounting that sanctions, international pressure, and possibly increased enforcement by China are beginning to take their toll on the North Korean economy and in particular, North Korea intelligence agent's ability to procure goods for regime leadership. A May 2017 report from the Korea Development Institute concluded that North Korea's black market had helped the nation endure the impacts of the international sanctions last year.

Detailed below are numerous non-cyber operations that have been conducted by the predecessor organizations of the RGB. The violence, destruction, and criminal breadth of these operations reveal the broad operational scope of these intelligence services and the context in which they are conducted.

This data further reveals a history of denials by North Korea of responsibility for operations dating back to the 1960s, putting into context the current leadership's denials of cyber operations.

Note

The activities detailed below are intended to be illustrative, not an exhaustive list, of the broad operational remit for North Korean operations.

"Blue House Raid"

One of the first major attacks on South Korea since the armistice was declared after the Korean War in 1953 occurred in 1968. The so-called "Blue House Raid" was an assassination attempt on then-President Park Chung Hee by 31 North Korean special operations soldiers on the night of January 20, 1968. The 31 North Korean soldiers crossed the DeMilitarized Zone (DMZ) on foot and managed to get within a half mile of the President's residence (the so-called "Blue House") before being exposed. Upon discovery the North Korean soldiers engaged in a series of firefights with South Korean forces; 68 South Koreans and three U.S. soldiers were killed. Most of the North Korean soldiers were killed in the eight days after the raid; two made it back across the DMZ and one was captured.

The captured North Korean soldier claimed during a press conference that they had come to "cut Park Chung Hee's throat." That account was disputed during a secret meeting in 1972 between a South Korean intelligence official and the then-Premier Kim Il-sung. Kim claimed his government had nothing to do with the raid and "did not even know about it at the time."

A captured North Korean soldier after the Blue House Raid. (Source)

1983 Rangoon Bombing

On October 9, 1983, three North Korean soldiers attempted to assassinate then-South Korean President Chun Doo Hwan while on a trip to Myanmar. A bomb at a mausoleum the President was scheduled to visit detonated early, killing 21 people, including the Korean Foreign Minister and Deputy Prime Minister.

During the trial for the bombers, testimony revealed that the North Korean agents used a North Korean trading vessel to travel to Myanmar and the home of a North Korean diplomat to prepare the bombs. In a classified report (report was declassified in 2000) ten days after the bombing, CIA analysts laid out a strong case that North Korea was responsible for the attack despite official denials of involvement from the official North Korean news agency. North Korean state media even accused President Chun of using the attack to increase tensions on the peninsula.

South Korean officials wait at the mausoleum in Rangoon minutes
before the bomb detonated. (Source)

Korean Air Flight 858 Bombing

On November 29, 1987, two North Korean intelligence agents boarded and placed a bomb on a Korean Air flight from Baghdad, Iraq to Seoul. During a layover in Abu Dhabi, the two agents de-planed but left the bomb (disguised as a radio) onboard. The bomb detonated and the plane crashed in the jungle on the Thai-Burma border and killed all 115 people on board.

One of the North Korean intelligence agents, who was captured alive, later revealed that the bombing was meant to "discourage foreign participation in the 1988 Olympic Games in Seoul and create unrest" in South Korea. The agent also confessed that the order to bomb the plane had come directly from then North Korean leader Kim Il-Sung or his son, later leader Kim Jong-il.

Transition to Criminality

By the mid-1990s, North Korea had generally shifted from acts of terrorism to criminality. While North Korea had held a policy of "self-financing,[2]" in which embassies and diplomatic outposts were forced to earn money for their own operations typically via engaging in illicit activity such as smuggling, since the late 1970s, it was during the 1990s that this criminality became a business of the entire state and not just the diplomatic establishment. A number of factors affected this shift, including the end of the Cold War and the withdrawal of crucial aid from benefactors (like the Soviet Union and China), a crippling famine, a leadership transition, and years of international condemnation and punitive actions.

A 2015 report from the Committee for Human Rights in North Korea characterizes North Korea's involvement in "illicit economic activities" into three separate phases. First, from the origins of North Korea state involvement in the 1970s through mid-1990s, from the mid-90s through the mid-2000s, and approximately 2005 to today. The RGB, its predecessor organizations, and other military and intelligence services support these illicit activities.

Illegal Drug Manufacturing and Smuggling

North Korea has had a state-sponsored drug smuggling (and later manufacturing as well) program since the mid-1970s. This vast enterprise has been supported by the military, intelligence services, and diplomats and has often included working with criminal organizations such as the Taiwanese gang United Bamboo, Philippine criminal syndicates, and Japanese organized crime.[3]

Academic research indicates that North Korea has developed extensive covert smuggling networks and capabilities primarily to provide a means of hard currency for the Kim regime.

The North Korean state actively cultivates opium poppy and produces as much as 50 metric tons of raw opium per year. To put that in context, the United Nations estimates that Afghanistan produced 6,400 tons of raw opium in 2014, which makes North Korea a minor producer in comparison. According to a Congressional Research Service report, government processing labs have the capacity to process twice that amount into opium or heroin each year. Experts estimate that North Korea brings in as much as $550 million to $1 billion annually from illicit economic activities.

Counterfeiting

One of the more widely reported North Korean criminal enterprises has been the production of counterfeit American $100 (and $50) bills, or so-called "supernotes." In a 2006 Congressional testimony, the U.S. Secret Service made a definitive link between the production of the "supernote" and the North Korean state.

According to interviews in a 2006 *New York Times Magazine* article, North Korean state support for counterfeiting U.S. currency dates back to a directive issued by Kim Jong-il in the mid-1970s. Original counterfeiting involved bleaching $1 bills and reprinting them as $100 notes and evolved over time as North Korea's international isolation grew and its economy collapsed.

“Supernote” and a real $100 bill. (Source)

Distribution and production of the supernotes followed a similar pattern to North Korean-produced narcotics, utilizing global criminal syndicates, state and intelligence officials, and legitimate businesses. North Korea has repeatedly denied involvement in counterfeiting or any illegal operations.

A History of Denial

As outlined above, North Korea has a history of denying responsibility for their violent, illicit, and destructive operations. This includes denying involvement in the Blue House Raid, the Rangoon Bombing, all criminal and illicit activity including counterfeiting U.S. dollars, the Sony Pictures Entertainment attack, and the Bangladesh Central Bank robbery. Some scholars argue that acts such as counterfeiting a nation’s currency constitutes a *casus belli*, an action or event that justifies war, and others argue that “international legal norms and constructs do not adequately address what constitutes casus belli in the cyber domain.”

Both of these arguments, as well as an understanding of North Korea’s asymmetric military strategy, underscore why North Korea would not want to claim responsibility for many of these destructive and violent acts. Acknowledging state responsibility could provide the United States or South Korea with a valid *casus belli*, resulting in a war that North Korea would most certainly lose. Even if the evidence is strong, official government denials create uncertainty and give North Korea space to continue operations.

Impact

What has been missing from the discussion about whether North Korea is responsible for the WannaCry campaign and the bank heists has been the why — the geopolitical and strategic intelligence that give CSOs, security professionals, and threat analysts context for the activity they are seeing.

As of last week the NSA and several companies, including Symantec and Kaspersky, have linked the recent WannaCry ransomware campaign to North Korea; Recorded Future assesses that this type of cyber activity would fall within both North Korea’s “self-financing” policy and asymmetric military strategy.

In this context, as a nation that is under immense international financial and political pressure and one that employs these types of policies and strategies, Recorded Future believes that North Korean cyber operations (with the goal of acquiring hard currency) will continue for at least the short to medium term (one to three years). Additionally, destructive cyber operations against the South Korean government and commercial entities will persist over this same term and likely expand to Japanese or Western organizations if U.S. and North Korea tensions remain high.

The cyber threat environment and military strategy framed above indicate that companies in several major economic sectors should increase monitoring of North Korean cyber activity. Financial services firms must remain constantly vigilant to exploitation of their SWIFT connections and credentials, possible destructive malware attacks and DDoS, and threats to customer accounts and data. Companies in the government contracting and defense sectors, especially companies that support the Terminal High Altitude Area Defense (THAAD) system deployment as well as U.S. or South Korean operations on peninsula, should be aware of the heightened threat environment to their networks and operations on the Korean peninsula.

Energy and media companies, particularly those located in or that support these sectors in South Korea, should be alert to a wide range of cyber activity from North Korea, including DDoS, destructive malware, and ransomware attacks. Broadly, organizations in all sectors should continue to be aware of the adaptability of ransomware and modify their cyber security strategies as the threat evolves.

This is part one of a two-part series on North Korea. In part two, we will examine patterns of behavior and internet activity from North Korea, including the widespread use of virtual private servers (VPS) and virtual private networks (VPN) to obfuscate browsing, internet transactions, and other, possibly malicious, activity.