World News

How North Korean Hackers Became the World's Greatest Bank Robbers

The Reconnaissance General Bureau, North Korea's equivalent to the CIA, has trained up the world's greatest bank-robbing crews. In just the past few years, RGB hackers have struck more than 100 banks and cryptocurrency exchanges around the world, pilfering more than $650 million. That we know of.

Students at Mangyongdae Revolutionary School, a prestigious academy in Pyongyang. North Korea's elite hackers are often deployed to countries with faster internet speeds to target banks around the world. In the US, they've gone after Wells Fargo, Citibank and the New York Federal Reserve. (Credit: KCNA)

It was among the greatest heists against a United States bank in history and the thieves never even set foot on American soil.

Nor did they target some ordinary bank. They struck an account managed by the Federal Reserve Bank of New York, an institution renowned for its security.

In vaults 80 feet below the streets of Manhattan, the bank holds the world's largest repository of gold. Many of these gold bars belong to foreign governments, which feel safer storing their gold inside well-defended bunkers in America than at home.

By the same token, overseas governments also store cash with the Fed. But this is cash in the 21st-century sense: all ones and zeroes, not smudgy bills. The bank holds vast foreign wealth on humming servers wired up to the internet.

That's what the thieves went after in February 2016: nearly $1 billion, sitting in a Fed-run account. This particular account happened to belong to Bangladesh. Having already hacked into the servers of the Bangladesh Central Bank, the criminals waited until a Friday a day off in many Muslim-majority nations, Bangladesh included. Then they started draining the account. Posing as Bangladesh Central Bank staff, the hackers sent a flurry of phony transfer requests to the Fed totaling nearly $1 billion. The Fed started zapping cash into accounts managed by the thieves overseas, most of them in the Philippines. Much of the money was quickly pulled out as cash or laundered through casinos.

From there, the trail goes cold.

The hackers didn't get the full billion they desired. Most of the bogus requests were caught and canceled by suspicious personnel. But they did end up with an amazing score: $81 million.

The culprits of this heist are loyal to one of the most impressive organized crime syndicates in the world. They don't work for the Triads, nor the Sinaloa Cartel, nor Sicily's Cosa Nostra. They are agents of the Reconnaissance General Bureau (or RGB), which is headquartered in Pyongyang. This is North Korea's equivalent to the CIA.

Like the CIA, North Korea's RGB is steeped in clandestine overseas plots: assassinations, abductions and lots of spying. But it is perhaps better understood as a mash-up between the CIA, the KGB and the Yakuza.

What distinguishes the bureau is its entrepreneurial streak one with a distinctly criminal bent. For decades, North Korea has been beleaguered by Western sanctions and barred from global markets. This has prodded the regime to seek revenue in darker realms that are beyond the law. These black-market enterprises have included heroin production, printing bogus $100 bills and counterfeiting name-brand cigarettes.

But all of those rackets have now been totally eclipsed by hacking. The bureau has trained up the world's greatest bank-robbing crews, a constellation of hacking units that pull massive online heists.

These thieves also have one distinct advantage over other syndicates: They are absolutely confident that they'll never be charged. So it goes when your own country sponsors your criminal mischief.

This is a new phenomenon, according to US intelligence officials. "A nation state robbing banks … that's a big deal. This is different," says Richard Ledgett. He was, until his recent retirement, the deputy director of the National Security Agency.

In recent years, North Korea has launched hacks against more than 100 banks and online exchanges in a total of 30 countries. The RGB appears to have successfully pilfered $650 million. That we know of.

And yet they are chronically overlooked—at least in the American media, where talk of online subterfuge is dominated by Russian political hacks. If you weren't aware that North Korea pulled a heist on the Federal Reserve, note that the caper went down in February 2016, when the media spotlight was fixed on the US presidential race at the expense of, well, almost everything else.

Not so long ago, North Korea spoke of smiting the US with its "treasured nuclear sword of justice." Now it offers grand gestures of warmth. Kim Jong-un has released American prisoners. He has giddily stepped into South Korea if only for a moment and he is now readying peace talks with President Donald Trump, a man who has threatened the young autocrat's life via Twitter.

But those with deep knowledge of North Korea's RGB also tend to believe that North Korea has pulled off another stunning technological feat: amassing one of the most skilled hacking syndicates in the world.

Moreover, these bank heists are linked to the state's nuclear arsenal. Missile tests provoke sanctions. Sanctions dry up North Korea's foreign cash reserves. Pyongyang is then left scrambling to find alternate revenue streams in the underworld. None of these criminal enterprises are as lucrative as hacking—and none poses a greater threat to the US-dominated global financial system.

To make sense of North Korea's hacking feats, I sought out Kim Heung-Kwang, a bespectacled 58-year-old computer scientist living in Seoul. Kim is familiar with the thinking of tech-savvy servants of the regime in Pyongyang.

After agreeing to meet, Kim sends directions by text. Following them leads my co-producer, Sona Jo, and me into a drab cement structure on the outskirts of Seoul, far from the capital's glitzy shopping promenades. Outside, it's snowing softly and a chill pervades the unheated building. Reaching Kim's chambers requires a steep climb up a freezing stairwell.

Kim has come a long way since he emerged scared, soaking wet and nearly possessionless from the Tumen River in 2003. That was the year he sneaked to the banks of the river, which divides his homeland from China, and bribed a North Korean guard. The soldier looked away as Kim swam through freezing waters toward China. But as he swam, Kim says, he was shot at by a second guard whom he'd neglected to bribe.

Ultimately, he made it to the far shore unscathed and, from China, made his way to South Korea. Today, he heads an alliance of highly educated North Korean defectors.

He keeps busy by running this alliance called North Korea Intellectuals Solidarity which comprises escaped North Korean lawyers, doctors, engineers, academics and programmers. The intel he has gathered from these associates suggests to him that North Korea's hackers are "an absolute treasure to Kim Jong-un," he says. "Because it is becoming clear that North Korean hackers are the best in the world."

Kim is a computer scientist himself. He specializes in digital networks and claims he took part in early modem communication between Pyongyang and Hamhung, North Korea's second-largest city and Kim's hometown.

That's also where he spent years as a university professor, teaching soldiers-to-be about online networks. Many of his students, he says, were swept into the RGB to fulfill their ultimate mission: infiltrating the networks of enemies overseas.

Kim believes this background, plus his access to intel shared among hundreds of highly placed defectors, qualifies him as an authority on North Korean hackers. They are, he says, profoundly underestimated on the world stage.

"They're the geniuses of North Korea," Kim says. "Let's make this simple. You want to rank countries when it comes to government hacking? Well, most people will say America is No. 1, Russia is No. 2, China is No. 3and so on."

"But tell me, honestly. Is anyone pulling off as many successful hacking operations as North Korea?"

Let's review some of North Korea's greatest hacks.

In 2014, North Korean agents crept into the digital infrastructure of Sony Pictures, which was preparing to release "The Interview," a screwball comedy about assassinating Kim Jong-un. Pyongyang's agents wiped data and leaked embarrassing emails until Sony caved and canceled the film's mainstream release.

In 2017, North Korean hackers seized Microsoft computers worldwide with a worm known as WannaCry. Devices were rendered useless unless the owner paid a ransom in Bitcoin—the price of unfreezing the computer. More than 200,000 computers in 150 countries were affected.

And in the last three years alone, North Korean hackers have targeted banks and cryptocurrency exchanges in the following countries: South Korea, Thailand, India, the Philippines, Poland, Peru, Vietnam, Nigeria, Australia, Mexico, Japan and Singapore. In the US, they've gone after Wells Fargo, Citibank and, of course, the New York Federal Reserve.

All told, these heists have pulled in an estimated $650 million in just a few years.

"So even just from reading the news," Kim says, "everyone should start to wonder if maybe North Korean hackers are now the very best in the world."

The $650 million figure comes from Simon Choi, among the more authoritative sources on North Korean hackers. At 34, he has spent much of his young life chasing their digital trail. He is a consultant to South Korea's National Intelligence Service—formerly titled the Korean CIA—as well as the military's cyberwarfare division.

"I think we're only able to uncover about 30 percent of their total hacking," Choi tells me. "This is just a portion of their activity." When I asked Choi to rank North Korea's hackers, he tells me that "their skill has come a long way. They are now No. 1 in the world in terms of hacking."

This is no fluke, Kim says. Under the reign of Kim Jong-un—the regime's first millennial dictator—the RGB has continually restructured itself to emphasize cybercrime. It now oversees an estimated 3,000 to 6,000 hackers.

"A nation state robbing banks … that's a big deal. This is different."

The bureau was created in 2009, during the last years of Kim Jong-il's rule. It was comprised of a variety of units devoted to spycraft, overseas killings, psychological warfare and cyberwarfare—all of them pulled under one roof. According to Kim, once Kim Jong-un ascended to the throne, and took over the RGB, he lavished even more resources on its elite hacking units.

Two of those units stand out as exemplary.

One is known as Unit 121—sometimes called "Lazarus" or "Hidden Cobra" by outside spy agencies—which pulled off both the Sony Pictures and the Federal Reserve hacks, Choi says. (The FBI has actually looked into filing charges against North Korea for the Fed heist.)

The other is Unit 110, which, according to Choi, began as a specialty unit targeting rival nations' military intelligence. It has since devoted more energy, Choi says, to bilking credit card systems, ATM networks and, more recently, online stores of cryptocurrency.

Such online finesse begs the question: How is this impoverished state launching so many successful attacks from its home soil—especially given its constant power outages and primitive digital infrastructure?

It isn't, Kim says. The bureau simply deploys hacker cells to live abroad—many of them in China—where online speeds are much faster. There, North Korean agents may feign jobs as traders or importers but run operations at night.

Other digital clues left by North Korean hackers suggest they're located in India, Malaysia, Nepal, Indonesia and as far away as Mozambique. Recorded Future, a firm monitoring cyberthreats worldwide, claims North Korean agents look at Amazon, Baidu (China's Google equivalent), a fair amount of porn and, more embarrassing still, their own AOL accounts. They also use iPads and iPhones. (Kim Jong-un himself has been spotted using Apple computers.)

Kim Jong-un and his iMac. (Credit: KCNA)

Climbing this professional ladder was a gauntlet, each step bringing ferocious competition from other young men. For tech-related positions, either academic of professional, he says that "100 openings will attract thousands of applicants."

He worked alongside hackers both in college and at the bureau. Those with brains would always rise fast, he says. "In North Korea, there are now very strong incentives to become engineers or IT specialists. Because if you become a cyberexpert, you can become a senior manager within the Communist Party," he says. "Boys and men dream of pursuing this path."

Hacking has a special cachet in North Korea, Jang says, because it affords a life grander than a rice farmer could ever imagine. The most skilled programmers are allowed to move their entire families from hardscrabble provinces into the capital of Pyongyang, a privilege denied to common servants of the state.

But the very best cyberwarriors are deployed abroad and, by necessity, given free access to the internet. Of course, the web is a space seething with information the Kim dynasty hides from the general population. "So these people do learn about North Korea's reputation as a dictatorship," Jang says. "They know what they do is considered criminal."

But all evidence indicates they're not just targeting their traditional "enemy": those wicked Americans and, as Pyongyang's apparatchiks see it, their quasi-colony in South Korea. They're hitting banks all across the world, especially poorly defended institutions in Southeast Asia.

Jang breaks down the mental gymnastics: "In North Korea, we learn that America doesn't just militarily invade countries around the world. It also manipulates the world using its dollar regime—the global financial system."

In other words: Any one institution participating in the global banking network is fair game. The fact that US-imposed sanctions prevent North Korea from accessing these very networks only sweetens the justification, Jang says. "Through hacking, they feel they're lifting those sanctions," he says, and thus making up lost revenue.

For North Korean hackers, the alternative to maintaining this worldview—drifting into some fantasy of revolt—is almost unthinkable, he says. They have too much to lose: an unfiltered view of the web, relief from hunger and want, parents and siblings living cozily in Pyongyang.