The Incredible Rise of North Korea's Hacking Army

By Ed Caesar

Published: 2021-04-16 · Archived: 2026-04-05 21:11:47 UTC

The country's cyber forces have raked in billions of dollars for the regime by pulling off schemes ranging from A.T.M. heists to cryptocurrency thefts. Can they be stopped?

April 19, 2021

North Korea, whose government is the only one on earth known to conduct nakedly criminal hacking for monetary gain, has run schemes in some hundred and fifty nations.Illustration by Anuj Shrestha

Shimomura was a member of the Yamaguchi-gumi, the largest yakuza crime family in Japan. When one of his superiors asked him if he wanted to make a pile of fast money, he naturally said yes. It was May 14, 2016, and Shimomura was living in the city of Nagoya. Thirty-two years old and skinny, with expressive eyes, he took pride in his appearance, often wearing a suit and mirror-shined loafers. But he was a minor figure in the organization: a collector of debts, a performer of odd jobs.

The superior assured him that the scheme was low risk, and instructed him to attend a meeting that evening at a bar in Nagoya. (Shimomura, who has since left the Yamaguchi-gumi, asked to be referred to only by his surname.) When Shimomura showed up, he found three other gangsters, none of whom he knew. Like many yakuza, he is of Korean descent, and two of the others were also Korean-Japanese; for a while, they spoke in Korean. The superior finally arrived, and the five men moved into a private room. Each volunteer was given a plain white credit card. There was no chip on the card, no numbers, no name—just a magnetic strip.

The superior read instructions from a thin manual: early the next morning, a Sunday, they should go to any 7-Eleven and use their white card at the store's A.T.M. They could not use a regular bank A.T.M., or one in another convenience store. The gangsters should each withdraw a hundred thousand yen at a time (about nine hundred dollars) but make no more than nineteen transactions per machine. If anybody made twenty withdrawals from a single A.T.M., his card would be blocked. Withdrawals could start at 5 *a.m.* and continue until 8 *a.m.* The volunteers were told to choose the Japanese language when prompted—an indication, Shimomura realized, that the cards were foreign. After making nineteen withdrawals, they should wait an hour before visiting another 7-Eleven. They could keep ten per cent of the cash. The rest would go to the bosses. Finally, each volunteer was told to memorize a *PIN*.

On Sunday morning, Shimomura rose early, and dressed in jeans, sunglasses, a baseball cap, and an old T-shirt. He walked to a 7-Eleven, where he bought a rice ball and a Coke, to settle himself. He inserted the card into the A.T.M. When the screen asked him which language he preferred, he felt a tremor of nerves while selecting "Japanese." He withdrew a hundred thousand yen, then another, and then another. There was nobody else in the store apart from the guy at the register, who didn't seem interested in him.

After making the first withdrawal, Shimomura printed a receipt. He saw a foreign name on the paper—he couldn't tell what nationality the name was, but he knew it wasn't Japanese—then stuffed the receipt in his pocket. Around 8 *a.m.*, having completed a total of thirty-eight withdrawals at several A.T.M.s in the area, he headed home, waddling because of his bulging pockets: 3.8 million yen is a lot of cash. Shimomura took his ten per cent—about thirty-five hundred dollars—and stashed it in a drawer in his apartment. At 3 *p.m.*, he met his superior to deliver the remaining money. (Later, he discovered that one of the other gangsters had absconded with the money and the card.)

The superior told Shimomura that he would retain five per cent of what his volunteers brought in and send the rest of the cash to his bosses. When Shimomura handed over his money, he sensed that the superior had enlisted many others. He was right. As the newspapers soon reported, more than sixteen million dollars was withdrawn from roughly seventeen hundred 7-Eleven A.T.M.s across Japan that morning, using data stolen from South Africa's

Standard Bank. The newspapers surmised that 7-Elevens had been targeted because they were the only convenience stores in Japan whose cash terminals all accepted foreign cards. Soon after the raids, the withdrawal limit for many A.T.M.s in the country was reduced to fifty thousand yen.

Shimomura deduced that he had been at the bottom of the food chain in the scam. The real money-makers were much higher up. What he did not know, until an interview with this magazine last year, was the identity of the villains at the top of the chain. Shortly after the A.T.M. thefts, according to Japanese police, the ringleader of the 7-Eleven operation crossed from China into North Korea. Shimomura had unwittingly been collecting money for the Korean People's Army, as part of a racket that became known as FASTCash.

In satellite images of East Asia at night, lights blare almost everywhere, except in one inky patch between the Yellow Sea and the Sea of Japan, and between the thirty-eighth and the forty-third parallels: North Korea. Only Pyongyang, the capital, emits a recognizably modern glow. The dark country is one of the last nominally Communist nations in the world—a Stalinist personality cult centered on Kim Jong Un, the peevish, ruthless scion of the dynasty that has ruled North Korea since 1948, after the peninsula was divided. The D.P.R.K. purports to be a socialist autarky founded on the principle of *juche*, or self-reliance. Its borders are closed and its people sequestered. Foreigners find it profoundly difficult to understand what is happening inside North Korea, but it is even harder for ordinary North Korean citizens to learn about the outside world. A tiny fraction of one per cent of North Koreans has access to the Internet.

Yet, paradoxically, the North Korean government has produced some of the world's most proficient hackers. At first glance, the situation is perverse, even comical—like Jamaica winning an Olympic gold in bobsledding—but the cyber threat from North Korea is real and growing. Like many countries, including the United States, North Korea has equipped its military with offensive and intelligence-gathering cyber weapons. In 2016, for instance, military coders from Pyongyang stole more than two hundred gigabytes of South Korean Army data, which included documents known as Operational Plan 5015—a detailed analysis of how a war with the country's northern neighbor might proceed, and, notably, a plot to "decapitate" North Korea by assassinating Kim Jong Un. The breach was so egregious that Kim Tae-woo, a former president of the Korea Institute for National Unification, a think tank in Seoul, told the *Financial Times*, "Part of my mind hopes the South Korean military intentionally leaked the classified documents to the North with the intention of having a second strategy."

“We’ve got ways of making you stop talking.”

Cartoon by Benjamin Schwartz

North Korea, moreover, is the only nation in the world whose government is known to conduct nakedly criminal hacking for monetary gain. Units of its military-intelligence division, the Reconnaissance General Bureau, are trained specifically for this purpose. In 2013, Kim Jong Un described the men who worked in the “brave R.G.B.” as his “warriors . . . for the construction of a strong and prosperous nation.”

North Korea’s cybercrime program is hydra-headed, with tactics ranging from bank heists to the deployment of ransomware and the theft of cryptocurrency from online exchanges. It is difficult to quantify how successful Pyongyang’s hackers have been. Unlike terrorist groups, North Korea’s cybercriminals do not claim responsibility when they strike, and the government issues reflexive denials. As a result, even seasoned observers sometimes disagree when attributing individual attacks to North Korea. Nevertheless, in 2019, a United Nations panel of experts on sanctions against North Korea issued a report estimating that the country had raised two billion dollars through cybercrime. Since the report was written, there has been bountiful evidence to indicate that the pace and the ingenuity of North Korea’s online threat have accelerated.

According to the U.N., many of the funds stolen by North Korean hackers are spent on the Korean People’s Army’s weapons program, including its development of nuclear missiles. The cybercrime spree has also been a cheap and effective way of circumventing the harsh sanctions that have long been imposed on the country. In February, John C. Demers, the Assistant Attorney General for the National Security Division of the Justice

Department, declared that North Korea, “using keyboards rather than guns,” had become a “criminal syndicate with a flag.”

North Korea’s leaders have been attuned to the nefarious opportunities of a connected world since at least the early nineteen-nineties. A 2019 paper on the regime, written by scholars at Korea University, in Seoul, notes that Kim Jong Il, having watched the United States’ military engagement in the two Gulf conflicts, concluded that “modern war is decided by one’s conduct of electronic warfare.” (Among other tactics, American planes jammed Iraqi radar systems.) In 2005, a Korean People’s Army book quoted Kim as saying, “If the Internet is like a gun, cyberattacks are like atomic bombs.” His son Kim Jong Un came to power in 2012 and saw the commercial potential of the technology, noting that his army could “penetrate any sanctions.” Cyber prowess, he soon declared, was an “all-purpose sword that guarantees the North Korean People’s Armed Forces ruthless striking capability, along with nuclear weapons and missiles.” Yet the West didn’t really wake up to the danger posed by North Korea’s cyber forces until after the country executed three spectacular crimes, between 2014 and 2017.

The first was a hack of Sony Pictures. In June, 2014, Sony released a trailer for “The Interview,” a Seth Rogen and James Franco comedy about hapless journalists recruited by the C.I.A. to assassinate Kim Jong Un. A spokesperson for the regime called the film a “wanton act of terror” and promised a “merciless response” if the studio proceeded with releasing the film. Sony pressed ahead. (Rogen joked on Twitter, “People don’t usually wanna kill me for one of my movies until after they’ve paid 12 bucks for it.”)

That November, Sony employees reported that their computers had been hacked, by a group calling itself Guardians of Peace. After many of the company’s computers froze, Sony shut down the rest, stanching the bleed of data that was under way. For a few days, Sony Pictures operated without an electronic network, and in subsequent weeks the hackers leaked embarrassing—and, in some cases, damaging—e-mails, salaries, medical records, movies, and screenplays belonging to the company and its employees. Five upcoming Sony films were put online, as was the script of the next James Bond movie, “Spectre.” One of the studio heads, Amy Pascal, resigned after the hackers posted e-mails in which she joked with the producer Scott Rudin that at a meeting with President Barack Obama she’d be smart to bring up movies about slavery.

The F.B.I. soon attributed the attack to North Korean state actors. Pyongyang denied involvement but declared the hack a “righteous deed.” Obama promised to “respond proportionally” to what he called an act of “cyber vandalism.” Michael McCaul, who chaired the House Homeland Security Committee, later told reporters that the U.S. had launched a number of “cyber responses” to the Sony hack, not least a ten-hour Internet outage in North Korea in December, 2014.

If the attack on Sony had a cartoonish quality, the second major North Korean attack was like a caper. Around the time that the hackers were breaking into Sony’s network, members of the same gang—which became known as the Lazarus Group—began scoping out banks in Dhaka, Bangladesh. Accounts linked to the Lazarus Group sent e-mails to an array of targets at Bangladesh Bank and other financial institutions in Dhaka. The messages contained a link to malware that, if clicked, granted the North Koreans access to internal computer systems. In the first two months of 2015, at least three Bangladesh Bank employees were lured by these “spear-phishing” e-mails into downloading the infected attachment. By that March, the hackers had established a “backdoor” within the bank’s electronic communication system, allowing them to send messages to one another in a way that mimicked

the bank's encrypted-communication protocols, and did not alert security to their presence. The hidden hackers then spent ten months learning about Bangladesh Bank's operations from the inside.

Like many national banks in developing countries, Bangladesh Bank holds a foreign-currency account with the Federal Reserve bank in New York. On February 4, 2016, the Federal Reserve received instructions from Bangladesh Bank to make dozens of payments, totalling nearly a billion dollars, to various accounts, including one in Sri Lanka and four in the Philippines. The requests were made via the *swift* network—a global conduit for money transfers, based near Brussels. In fact, the Lazarus hackers had sent the requests, using stolen usernames and passwords that they had collected while roaming around Bangladesh Bank's network. In their fraudulent messages to the Federal Reserve, the Lazarus members had incorporated many details from genuine, previously executed *SWIFT* transfers, so that it would not be obvious their own requests were bogus. To further cover their tracks, the hackers had installed a network update that blocked *SWIFT* messages from being read at Bangladesh Bank—a piece of legerdemain that later impressed security experts. It was the equivalent of breaking into a bank's vault after disabling its surveillance cameras.

Priscilla Moriuchi, a fellow at Harvard's Belfer Center for Science and International Affairs who focusses on the North Korean cyber threat, worked at the National Security Agency for twelve years. She told me that the Bangladesh operation was "flashy." But the robbers not only showed technical finesse, she said; their patient work in the Dhaka heist "signalled a larger tactical and operational maturity."

The Federal Reserve granted the first five payment requests, a total of a hundred and one million dollars. The next thirty payments, which amounted to eight hundred and fifty million dollars, stalled only because of a stroke of luck. An automated alert system was activated after detecting, in the text of a transfer request, the word "Jupiter," which happened to be in the address of a Philippines bank branch. This alert was tripped because an unrelated business, Jupiter Seaways Shipping, in Athens, was on a sanctions-evasion watch list for its activities relating to Iran.

After this and another small irregularity were detected, freeze requests were placed on the recipient accounts. But—as the hackers had anticipated—because the heist was carried out on a holiday weekend in the Philippines the freeze requests weren't processed for another forty-eight hours. By that time, some eighty-one million dollars had been transferred into a different account. Most of this money was then withdrawn, converted into cash as Philippine pesos, and exchanged for casino chips. At the time, gambling establishments in the Philippines were exempt from anti-money-laundering regulations. It wasn't a billion dollars, but it was a huge haul.

By the time of North Korea's third major attack, nobody found the regime's cyber threat funny anymore. A 2017 ransomware scheme known as Wannacry 2.0 crippled networks in America, Europe, and Asia—including the computer systems of Boeing, Britain's National Health Service, and Germany's federal railway. The hackers encrypted computer after computer, then demanded payment, in bitcoin, to unfreeze the systems. North Koreans tailored some ransomware code and then propagated it from one device to the next by appropriating a dangerous piece of American code, known as EternalBlue, that a criminal group calling itself the Shadow Brokers had stolen from the N.S.A. and then posted online.

A twenty-two-year-old hacker and malware expert from England named Marcus Hutchins, who worked out of a bedroom in his parents' house, analyzed the Wannacry code and figured out how to direct much of the traffic that

it was generating into a “sinkhole”—a Web address where the malware would do no harm. After Hutchins realized that he had upended the hack, *Wired* reported, he went upstairs to tell his family. His mother, a nurse, was chopping onions. “Well done, sweetheart,” she said, before returning to her cooking.

The North Korean regime has long been considered a fundamentally criminal enterprise. Joseph Bermudez, Jr., a senior fellow at the Center for Strategic and International Studies, told me that the country’s survival has always been underpinned by a mafia-like “patronage system.” He explained that, even before the Korean War, smugglers and warlords had thrived in the region. Since the birth of the D.P.R.K., crime has been used to garner not only cash for the regime but also political and social capital. The Kims, Bermudez said, have fostered a “desire to produce revenue to secure pleasure with the leader.”

Until recently, North Korea’s most lucrative state-sponsored criminal operations included the smuggling of cigarettes, the creation of counterfeit money, the trading of endangered species, and the manufacture and distribution of laboratory-made illegal drugs such as methamphetamine. In the seventies, North Korean diplomats who were posted abroad often trafficked narcotics. In the eighties, North Korean counterfeiters created a remarkably plausible hundred-dollar “supernote.” (In 2006, the Secret Service estimated that it had removed fifty million dollars’ worth of fake notes from circulation; seven years later, the U.S. Treasury redesigned its hundred-dollar bill with extra security features.) Many traditional criminal revenue streams continue to flow back to Pyongyang, but in the past decade the state’s focus has pivoted to the Internet.

“You’re just lucky you don’t have your whole life looming in front of you.”

Cartoon by Barbara Smaller

The range and creativity of North Korea's digital crime spree caught many off guard. It wasn't just that Pyongyang's cyber warriors could compromise computer networks around the world; they showed real innovation in exploiting new technologies. Luke Dembosky, an attorney who advises companies on Internet-security issues, first confronted North Korea's cyber threat at the time of the Sony hack, when he was the Deputy Assistant Attorney General in the Justice Department's National Security Division. Then he witnessed the Bangladesh heist—a striking leap in sophistication. "It was stunning for someone like me, despite years in this business, to see a relatively isolated nation-state actor not simply copying someone else's methodology or scheme but actually breaking new ground," he said.

Priscilla Moriuchi, the Harvard analyst, told me that, in retrospect, the D.P.R.K.'s turn to cybercrime had been an organic development. "North Koreans understand criminality," she said. "They're integrated in many, many places with this criminal and gray underground world. And so it's natural to overlay this new technology, the Internet. It connects criminal organizations and smugglers with one another."

We discussed the Japanese A.T.M. scam of 2016. Shimomura may not have known his ultimate boss, but the yakuza had been smuggling illegal products out of North Korea for decades. Around the turn of the millennium, North Korea supplied about forty per cent of Japan's methamphetamines. So, if cyber scammers in Pyongyang needed boots on the ground to withdraw cash in Nagoya, they could make a request, and it would soon be answered.

Moriuchi also noted that, although the North Korean hackers were technically accomplished, their more important attribute was a felonious savoir-faire. In the Bangladesh Bank case, the robbers waited seventeen months after their first reconnaissance in Dhaka before they pulled off the heist. They had determined the ideal weekend and holiday to strike; they had planned how to move cash quickly out of recipient banks; and they had chosen institutions that had particularly lax know-your-customer protocols. Once they executed the theft, they used local contractors in the Philippines to launder their pesos, effectively hiding the money trail. Their success was predicated on knowing not only how computers work but how people do. "They're *smart*," Moriuchi told me. "It's this connection of the virtual world and the physical that's so impressive."

In most countries, hackers develop their skills by experimenting on computers at home when they are teen-agers. Marcus Hutchins, who dismantled Wannacry, was one such high-school recluse. But North Korea's talent in the cybercrime field is grown in a hothouse. Few families own computers, and the state jealously guards Internet access.

The process by which North Korean hackers are spotted and trained appears to be similar to the way Olympians were once cultivated in the former Soviet bloc. Martyn Williams, a fellow at the Stimson Center think tank who studies North Korea, explained that, whereas conventional warfare requires the expensive and onerous development of weaponry, a hacking program needs only intelligent people. And North Korea, despite lacking many other resources, "is not short of human capital."

The most promising students are encouraged to use computers at schools. Those who excel at mathematics are placed at specialized high schools. The best students can travel abroad, to compete in such events as the International Mathematical Olympiad. Many winners of the Fields Medal, the celebrated prize in mathematics, placed highly in the contest when they were teen-agers.

Students from North Korea often perform impressively at the I.M.O. (It is also the only country to have been disqualified for suspected cheating: the D.P.R.K. team was ejected twice from the competition, in 1991 and in 2010.) At the 2019 I.M.O., held in Bath, England, Kuk Song Hyon scored perfectly on the first five of six challenges, and was tied for first place with students from China, South Korea, Poland, and the U.S. until the final problem, when he received a low score.

Two colleges in Pyongyang, Kim Chaek University of Technology and Kim Il Sung University, vacuum up the most talented teen-agers from the specialized math and computer high schools and then teach them advanced code. These institutions often outperform American and Chinese colleges in the International Collegiate Programming Contest—a festival of unsurpassed and joyful nerdery. At the 2019 I.C.P.C. finals, held in Porto, Portugal, Kim Chaek University placed eighth, ahead of Oxford, Cambridge, Harvard, and Stanford.

Costin-Andrei Oncescu, who represented the University of Oxford at the 2019 I.C.P.C., and who began programming competitively in his native Romania at the age of ten, told me that the I.C.P.C. was not only fun and sociable but also a recruiting ground for big technology companies. Huawei sponsored the 2019 finals. Contestants, Oncescu said, have gone on to do impressive coding work. He mentioned Nikolai Durov, a member of the championship-winning St. Petersburg State University teams of 2000 and 2001, who subsequently co-founded the Russian social-media apps VK and Telegram.

Oncescu added that the North Koreans had stayed in the same hotel as the other contestants in Porto. But he hadn't seen them socialize with students from other countries. He said that, although the competitions tested coding fluency, the true test was of a more general problem-solving capability. It often came down to pure math. To thrive, every team needed at least one "*very* math-oriented" person, Oncescu said. Students working in teams of three were asked to create code that provided a solution to an abstract puzzle, but only one team member at a time wrote the code.

The coding challenges at the 2019 I.C.P.C. were fiendishly difficult. An example: "Your university's board game club just hosted a checkers tournament, and you were assigned to take notes on the games. Unfortunately, while walking home, you dropped all of your papers into a puddle! Disaster! Much of what you wrote is now unreadable; all you have left are some lists of moves played in the middle of various games. Is there some way you can reconstruct what happened in those games?" The code that the students built needed to solve this problem in no more than a second. Oncescu said that, to win the competition, you had to work fast, collaboratively, and creatively. "The hardest part isn't the coding," he told me. "It's the *thinking*."

He added that there was a lot of overlap between contestants at these kinds of competitions and the "next generation" of top programmers and researchers. He could also imagine how such competitions might develop the skills of a criminal hacker, because "once you've found something weird about the way a system works, then it does become a mathematical problem in trying to take advantage of that." The coding and the analytical skills on display at such events were like the Force in the "Star Wars" movies: it could be used for the light side, or for the dark.

According to many estimates, about seven thousand North Koreans work in the country's cyber program. Employees are split between the General Staff Department of the military, which assists the Army's operations, and the Reconnaissance General Bureau, which is akin to the Office of the Director of National Intelligence in the

U.S. The 2019 Korea University paper featured an analysis of how hackers were divided within these silos. The General Staff Department has among its subgroups the chillingly named Enemy Collapse Sabotage Bureau, which is responsible for “information and psychological warfare.”

Most of the criminal work is performed by the Reconnaissance General Bureau. According to the Korea University researchers, a section of the R.G.B. known as Unit 180 is responsible for “conducting cyber operations to steal foreign money from outside North Korea.” The Lazarus Group is the best-known unit of North Korean commercial hackers, but this entity may include—or have been partially replaced by—other groups, which are known to Western law-enforcement and intelligence agencies by such names as the BeagleBoyz, *Hidden Cobra*, and *APT*38. (“*APT*” stands for “advanced persistent threat.”) Nobody seems to have a firm grasp on how many people work for each group or which group makes the most money.

Another tantalizing question is where, geographically, North Korea’s hackers do their work. Moriuchi, the Harvard fellow, has spent years tracking the metadata of North Korean Internet users. Between 2017 and 2020, she looked at North Korea’s tiny online footprint. At any moment, as few as a couple of hundred I.P. addresses in the country might be in use. From this and other clues, she concluded that most of the country’s coders were working outside North Korea, in China and parts of Southeast Asia. Certainly, Moriuchi said, most of North Korea’s new I.T. graduates appeared to spend a period of time abroad in such countries, where they learned valuable “real world” skills. These foreign units were, in essence, both profit generators and training grounds.

“He’s older and fatter, but that’s definitely the same guy in the painting.”

Cartoon by Frank Cotham

Recently, an American analyst showed me the digital footprint of a cell that, he ascertained, consisted of North Koreans working in the border town of Dandong, China. The unit's work was seemingly anodyne—there was no evidence that it engaged in malicious hacking. Communicating through the e-mail address bravemaster619@hotmail.com, the group solicited for freelance gigs on coder sites, in almost flawless English. Bravemaster619's profile on GitHub reads, "Wanna have your own website? Wanna add some features or customize the design of your existing system? Wanna improve your site to the next level? Hold my seasoned development skills!" The North Korean workers in Dandong did not advertise their nationality—presumably because of the sanction provisions—and appeared to charge competitive rates.

Last year, I spoke to Lee Hyun Seung, a thirty-five-year-old who defected from North Korea in 2014 and now lives in the United States. He had worked in a trading business owned by the D.P.R.K. government, and in that capacity he had lived for a time in Dalian, China. He said that he had no special knowledge of the hacking program, but that when he worked in Dalian he knew there were three teams of North Korean "I.T. workers" based in the city. Lee told me that he once visited a so-called hacker dorm in Dalian. The men there lived four to a room—sometimes six. The ten or so men who worked in one such unit told Lee that they spent most of their time making "big money" by designing mobile-phone video games for the Japanese, South Korean, and Chinese markets. A Chinese intermediary sold their products. Lee suggested that, though this coding work was mundane, the North Koreans he met rarely wanted to be promoted—because a promotion would mean returning to Pyongyang.

This anecdotal evidence was buttressed by another defector, who runs a South Korea-based clandestine radio network whose broadcast signal penetrated North Korea. He told me that he was familiar with the D.P.R.K.'s cyber program, and, as he understood it, the work performed by North Korean I.T. workers outside the country tended to be "low level." The stars of the program either were kept in Pyongyang or were returned there to do their most important government work—a tactic that prevented hackers engaged in high-priority operations from being caught while abroad. The defector told me that the best hackers in Pyongyang, who were involved in schemes that collected millions of dollars' worth of foreign currency, were rewarded with cars or comfortable houses, or with other material benefits known as Kim Jong Un's Special Gifts, which were impossible for ordinary citizens to obtain. This information, the defector said, came from a friend in North Korea whom he could "absolutely trust," but who could not speak with me without risking his life.

An American investigator of sanction breaches, who works at a prominent N.G.O. but was not authorized to talk on the record, was similarly convinced that the élite cadre of North Korean hackers was based in Pyongyang. Most likely, these operatives used foreign V.P.N.s—virtual private networks—to access the Internet from outside the country, thus masking their location.

John Demers, of the Justice Department, suspects that the Chinese state assists with North Korean cybercrime, because it "does not want North Korea to fail." The American investigator of sanction breaches noted that "North Korea is connected to the world through essentially Russian and Chinese infrastructure," adding, "There are strong indications that Russia and China are well aware of what's going on and actively have facilitated some of it." A certain amount of legal and illegal trade continues across North Korea's borders with Russia and China, both

of which have historically been allies. According to the U.S. Cybersecurity and Infrastructure Security Agency, no financial institution in Russia or China has been targeted by North Korean hackers.

The most common target of North Korea's cyber army is its sworn enemy, South Korea, which has suffered many hundreds of major attacks. Recently, I spoke to Simon Choi, a security-intelligence analyst who lives in Seoul. In 2008, while performing mandatory military service, he learned about North Korea waging a cyberattack on the South Korean Army—an unsuccessful attempt by the Reconnaissance General Bureau to deploy malware in order to steal highly classified weapons secrets. Choi became fascinated with the threat posed by North Korean hackers. "I realized the cyber war was *real*," he said.

After completing his military service, Choi took a job in online security. He also began to organize a team of volunteers in South Korea, called the IssueMakers Lab, which pores over malware attributed to the North Koreans, in order to understand it better. The group now numbers ten people, and includes men and women. Although the members are amateurs, not spies, their assessments are considered to be rigorous and acute. In his day job, Choi trawls the dark Web, investigating drug deals and other crimes on behalf of law-enforcement agencies; after hours, he thinks about hackers in Pyongyang.

Choi told me that about eleven hundred North Koreans have written malicious scripts. He showed me some malware code, written in 2016, that had been designed to cover the tracks of a North Korean bank heist. The malware consisted of rows of seemingly random letters and numbers flowing down a page, in pairs. In the margins were some recognizable English-language words—"Windows," "*everyone*"—connected by cryptic punctuation. Choi could fluently and sensitively parse all this. Chinese and American coders were the best in the world, he said, but Russians and North Koreans were tied for second. Of all the malware that Choi had examined, he reserved his greatest admiration for the Stuxnet worm, which had been used in a successful joint Israeli-American attack on Iran's nuclear centrifuges, in 2010. He spoke about the Stuxnet code in the way that an art historian might discuss "The Night Watch": it was "elegant," "precise," "sophisticated." Choi told me that North Korean code was "masculine" in its brute concision: "Very simple, very practical, and they always go straight for their aim and goal." He added, "The key to their success is their relentlessness—they just attack, endlessly."

Sometimes, he explained, coders embedded signatures or initials into their scripts. It was a form of tagging, or maybe even bragging. He had occasionally noticed the initials of former International Math Olympiad competitors in malware that he examined. Once, when examining code related to a 2013 spear-phishing attempt on I.C.I.C.I., an Indian bank, Choi noticed a tag, kut_rsc1994, belonging to a coder who had studied at Kim Chaek University. ("KUT" is an established tag for the school.) On further inspection, Choi came to believe that the coder was Ryu Song Chol, who had won a silver medal for North Korea at the I.M.O., in Amsterdam, in 2011. Later, Ryu posted this tag on a hacking Web site, seemingly confirming the link.

Choi was circumspect about attributing coding tags to real-life people: who could know for sure which person was behind which persona? The North Koreans could well have swapped identities. He felt confident, though, that he had never examined code written by a North Korean woman. I laughed when he told me this. How could he possibly know? "These are all guys," he repeated. North Korea, he said, remained a traditional, male-dominated society, and it was extremely unlikely that the Reconnaissance General Bureau would train women for such work.

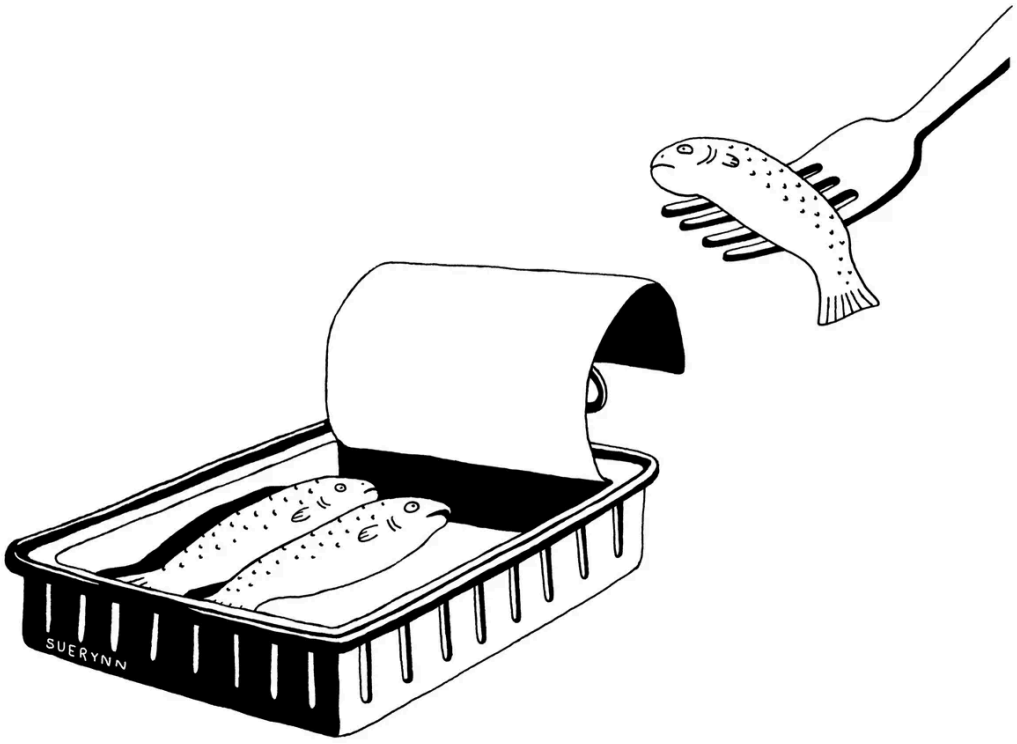
The IssueMakers often gave nicknames to the most accomplished North Korean hackers, although Choi wouldn't tell me the names of anybody currently working for Pyongyang. I wondered whether he had ever felt as if he understood these coders as people. "I think we have a mutual awareness," he told me. "They must see what we analyze as well, because we publish it. That's my feeling—that we are both aware of each other."

The Internet, to abuse John Donne, makes one little room an everywhere. North Korea's hackers have conducted operations in more than a hundred and fifty countries. In November, 2018, a programmer in Santiago, Chile, was recruited for a high-level position at a foreign firm. The programmer, who worked at Redbanc, a network that connects all the A.T.M.s in Chile, was invited via LinkedIn to apply for a position developing software at Global Processing Centre, a third-party-payment processor in St. John's, Antigua. The position was lucrative and part time: the programmer could supplement his income without impinging on his work for Redbanc.

Global Processing Centre's job offer came from someone purporting to be Justin Stuart-Young, the company's chief information officer. The Redbanc programmer was directed to a private e-mail address for Stuart-Young. The courtship progressed to a video interview, in which Stuart-Young interviewed the programmer in Spanish. After at least three more interviews, during which Stuart-Young said that he was looking forward to visiting Chile someday to meet in person, the Redbanc employee was asked to download and run a program that generated a PDF of a résumé. He did as instructed, but he never heard from Stuart-Young again. (The Redbanc programmer has since resigned, and the company would not identify him.)

While the programmer and Stuart-Young were corresponding, a cybersecurity professional named Juan Roa Salinas started in a new role at Redbanc. As he inspected the company's internal network, he saw signs that it had been compromised. There were unusual connections to Internet domain names that he would not have expected to see on the network.

A voracious reader of tech news, Roa had been fascinated by the North Korean attack on Bangladesh Bank and had studied the activities of the Lazarus Group and *APT*38. He had learned about North Korea's FASTCash attacks, such as the one deployed in Japan. As he investigated the "strange behavior" in the Redbanc network, he and members of the company's response team concluded that the business was under attack from a nation-state actor, most likely from Pyongyang. Among other clues, a Redbanc terminal had inexplicably looked up an I.P. address in North Korea. Roa, judging that the threat was severe, recommended that Redbanc shut off its Internet for a week.



“Guess we better find a subletter by the end of the month.”

Cartoon by Suerynn Lee

Roa remembers that his bosses found his request “shocking,” but they complied. An internal inquiry after the shutdown revealed that the company had indeed been in the middle of an attempted FASTCash breach. Such assaults normally take several months to execute. The hackers had first used a third-party criminal group for “social engineering.” The social engineers had mimicked a job offer from a real company in Antigua, using fake but convincing e-mail addresses and even impersonating an executive, Justin Stuart-Young, using a Spanish-speaking actor who roughly fit his description. (When I spoke to the real Stuart-Young recently, it was the first time he had heard of the Chile attack, and of his identity being stolen.)

When the Redbanc programmer had run the infected program, it had activated a “dropper,” which granted hackers remote control of his computer. The hackers then made a series of lateral moves across other computers on the company’s network. Their goal was to compromise Microsoft’s Active Directory system at Redbanc, which connects users with resources. By the time Roa noticed the intrusion, the hackers had not yet achieved this objective. The next stage of the operation would have been to gain control of the mainframe at Redbanc, and then to initiate the FASTCash attack itself, which would use malware to conceal fraudulent withdrawal requests made at A.T.M.s. Roa purged the hackers from the Redbanc network before they could overtake the mainframe.

After the attempted raid, Redbanc did what many companies subjected to such threats do: it kept quiet and improved its security. The FASTCash attack at Redbanc became public only because Felipe Harboe, then a Chilean senator, heard about it at a meeting of security experts and decided to tweet the news. Harboe told me last fall that he had broken Redbanc’s silence because South American institutions were now under constant threat from North Korean and Russian hacking groups. Redbanc officials, he said, were “surprised and upset” that

Harboe had exposed their breach, but he felt that the problem required more transparency. There had been other A.T.M. attacks in Chile, and ransomware schemes—in which hackers take control of a computer network and demand a fee for returning systems to normal—were even more common. Many ransomware operations started like the one at Redbanc, relying on a single weak point of entry.

The North Koreans' failure at Redbanc was only a minor inconvenience. The hackers' strategy is to catch many fish by casting a wide net. The Cybersecurity and Infrastructure Security Agency has noted that, around the time of the attack on Redbanc, North Korean actors set in motion successful FASTCash assaults on dozens of banks in Asia and Africa, stealing tens of millions of dollars. In a single breach in 2017, money was simultaneously withdrawn from A.T.M.s in more than thirty countries.

Priscilla Moriuchi believes that in the past two years the aesthetic of North Korean cybercriminals has become subtler. In addition to targeting big financial institutions, they have developed a faster, less flamboyant "operational tempo." She explained, "They've managed to routinize financial fraud, attacks on smaller financial institutions and regular citizens. They're much more like a normal criminal group now."

A report published in March by the U.N. panel of experts noted that one new avenue for North Korean cybercriminals is the theft of military information, either to sell or to harvest for the country's weapons program. But the most reliable money-maker for North Korea has become the theft of cryptocurrency.

Jesse Spiro, who is in charge of policy initiatives at Chainalysis, a private company that investigates cryptocurrency-related crime, told me recently that North Korean hackers have stolen at least $1.75 billion in digital coins from trading exchanges. This revenue stream alone could cover about ten per cent of North Korea's total defense budget.

North Korea's crypto-exchange hacks have a relatively straightforward methodology. Exchanges that trade bitcoin and other types of cryptocurrency typically hold escrow accounts full of their customers' coins. These storage facilities are known as "hot wallets," because they are connected to the Internet. (A more secure but laborious method of storing coins is in an offline "cold wallet" containing, say, QR-code printouts that contain the keys to blockchain accounts.) Hackers from North Korea often gain access to an exchange's internal systems using the same types of manipulations involved in the failed attempt in Chile. Real-sounding people propose real-sounding schemes, then persuade a network user at a targeted company to download an infected document. Typically, one or two admin-level members at a cryptocurrency exchange have access to a hot wallet's private keys. If hackers can compromise a sufficiently senior figure, they can reach the wallet and steal its coins.

Tom Robinson, the chief scientist at the blockchain-analytics firm Elliptic, who tracks the proceeds of cryptocurrency hacks for governmental and private clients, told me that cryptocurrency trades have become attractive targets for North Korean hackers: "Once the funds have moved out of the exchange, you can't reverse those transactions, like you can maybe with a traditional bank payment. Once they're gone, they're gone. And there's no intermediary, there's no controller of bitcoin, who you can go to and say, 'Those funds are stolen. Give them back to me.' It's completely decentralized. It can also be fairly anonymous—you don't need to enact the scheme through accounts linked to your identity."

Robinson said that one of the most successful fake personas used by the Lazarus Group was Waliy Darwish—a man who supposedly worked for a cryptocurrency company, based in Michigan, called Celas L.L.C. The Lazarus

Group invented both Darwish and Celas. LinkedIn profiles and other pages related to the persona and to the company are still active. On LinkedIn, Darwish poses as a graduate of the Rotterdam University of Applied Sciences and says that his interests include Rolls-Royces. He also claims, ungrammatically but somewhat truthfully, to "know how to act the blockchain in cryptocurrency." In February, an F.B.I. indictment against three suspected North Korean hackers noted that some malicious software created by the Lazarus Group and purporting to be a cryptocurrency-trading program was called Celas Trade Pro.

In the spring of 2018, the Darwish-Celas mirage was convincing enough to bait employees of a cryptocurrency exchange in Hong Kong into downloading infected software. (An investigation into this operation continues, and investigators believe that confirming the identity of the exchange might damage an ongoing inquiry.) Within a few weeks of the malware's installation, the hackers had stolen about ten thousand eight hundred bitcoins from the exchange's hot wallet. The coins, then worth around ninety-four million dollars, would now be worth more than half a billion dollars.

The money-laundering patterns that typically follow such raids are dizzying. Elliptic has traced what happened to the coins from the Hong Kong-exchange hack. Robinson explained that all the stolen coins were forwarded to a wallet maintained by the hackers, then split into dozens of small amounts and sent, through different routes, to another exchange. Such an atomized transfer of money is known as a "peel chain." When Robinson showed me a diagram of the dispersal of coins, I was reminded of an airline-magazine route map in which several lines sprout from one dot and then converge on another.

A peel chain is designed to outwit automatic alerts, which search for the transit of a precise volume of cryptocurrency. The stolen coins were sent to two Chinese men, Tian Yinyin and Li Jiadong, who had opened accounts on other exchanges, including one in the U.S., using fake pictures and fake names. They then cashed out the coins and transferred the money to Chinese banks. According to the U.S. Treasury, several financial institutions in China offer accounts to North Koreans, or to front companies that have relationships with Pyongyang. Last year, Tian and Li were indicted in the United States for allegedly laundering "over a hundred million dollars' worth of stolen cryptocurrency to obscure transactions for the benefit of actors in North Korea" between 2017 and 2019. They remain at large.

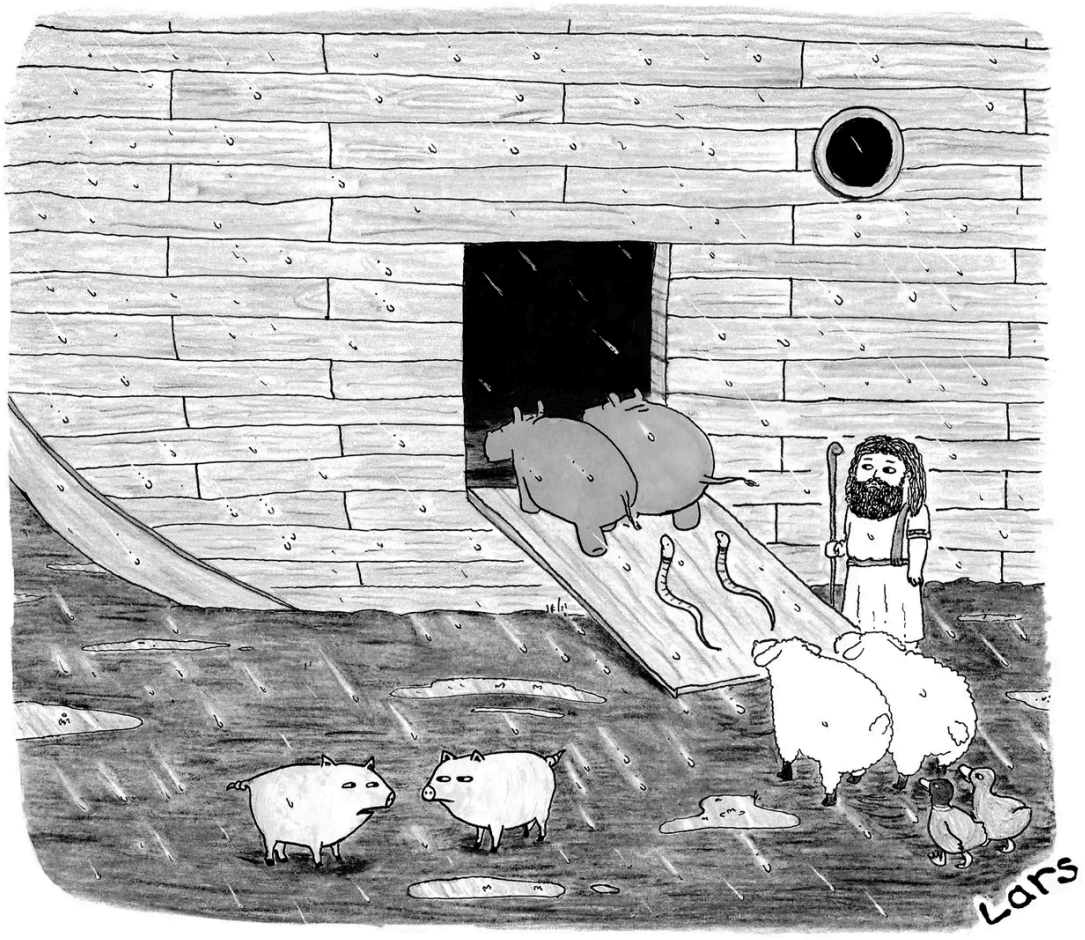
In 2019, the U.N. listed dozens of cryptocurrency exchanges that had been hacked by the North Koreans. One exchange in Seoul, Bithumb, was successfully raided four times—a tremendous failure of security. Since the U.N. report was published, the refinement of the attacks has only deepened, as has the skill with which the proceeds of crime are laundered. According to Jesse Spiro, of Chainalysis, fifteen cryptocurrency heists have been reported so far this year. It is too early to say how many will be attributed to North Korea.

Spiro noted that the authorities were increasingly on the lookout for such schemes. Awareness of peel chains, for example, has become widespread; the tactic is "relatively easy to trace if you have blockchain forensics or analysis capabilities," he said. But new obfuscation techniques have emerged. Professional money launderers offer such services as CoinJoin, which mixes stolen and non-stolen coins to confuse forensic analysts.

If one compared the industry and the manpower that went into planning and executing the Bangladesh heist with the almost casual way in which digital tokens are often stolen, it would be evident why the North Koreans have come to favor such exchange heists. Spiro told me that private forensics firms and law-enforcement agencies were

finally addressing the problem with the seriousness it deserved. Understanding how to track cryptocurrency is an increasingly important skill, not least because North Korean hackers, and members of many criminal gangs, accept ransomware payments in digital currency. Between 2019 and 2020, according to Chainalysis, ransomware incidents rose by more than three hundred per cent.

Even if other laundering techniques become well known and stolen coins could be readily flagged, the key to making such heists unprofitable is to stop thieves from cashing out. This is unlikely anytime soon, Spiro said, because of the lax practices of certain Chinese, Eastern European, and Southeast Asian exchanges. At a press conference to announce the February indictments against the three North Korean hackers, John Demers, of the Justice Department, made a pointed reference to such facilitators, saying that it was past time "for Russia and China, as well as any other countries whose entities or nationals play a role in the D.P.R.K. revenue-generation efforts, to take action."



"I just don't know if I'm ready to take mass transit yet."

Cartoon by Lars Kenseth

What good will such statements do? The U.S. has failed for a decade to find an effective response to the North Korean cyber threat. Luke Dembosky, the former Deputy Assistant Attorney General, worked with Sony throughout the 2014 crisis. At the time, some security experts doubted that North Korea was capable of such an attack. Dembosky told me that "we would not have sent Obama to the podium lightly," but when the President did

speak it was in measured terms. North Korea was accused of “vandalism” instead of a more serious crime. David Maxwell, a former Special Forces colonel who is now a senior fellow at the Foundation for Defense of Democracies, a conservative think tank, told me that it was hard to know what to do about a country behaving like a gang: “North Korea often operates below the threshold of a strategic response. Something like the Sony hack—that was an attack on a company. It wasn’t something that our government *defended* against.”

Several government agencies—including the F.B.I., the N.S.A., and the Secret Service—are now working aggressively to address the threat. The F.B.I.’s indictments against hackers from the Lazarus Group outline the unit’s alleged crimes in detail. One indictment noted that the hackers had “attempted to steal or extort more than $1.3 billion” from “entertainment companies, financial institutions, cryptocurrency companies, online casinos, cleared defense contractors, energy utilities, and individuals.” The F.B.I. also recently arrested and charged a Canadian-American man who allegedly laundered money for the North Koreans.

Similarly, an American blockchain expert named Virgil Griffith was indicted in January, 2020, in the Southern District of New York, for contravening U.S. sanctions against North Korea. Griffith had travelled to Pyongyang in 2019 to give a speech at a cryptocurrency conference. The complaint against Griffith alleges that he was instructed by his North Korean hosts to focus his presentation on “the potential money laundering and sanction evasion applications of cryptocurrency and blockchain technology.” Griffith has pleaded not guilty.

The unsealed indictments are a boon to journalists and researchers, but the chances of any North Korean hacker being prosecuted successfully are vanishingly slim. There is, however, a growing recognition in America of the threat presented by cybercriminals. President Joe Biden has secured ten billion dollars for federal agencies dealing with the issue of cybercrime. A government adviser told me that one major remedy being considered is the establishment of new protocols that will allow agencies to work much more closely with private security companies, which often perform the best cybercrime forensic work.

The national-security threat posed by North Korean hackers is less obvious than the one posed by Russian hackers, who have notoriously interfered in U.S. elections. The Obama Administration’s special adviser on cybersecurity, Michael Daniel, is now the president and C.E.O. of the Cyber Threat Alliance, a nonprofit organization dedicated to improving the sharing of intelligence about the threats posed by online crime. He told me that North Korea presented unique difficulties for law-enforcement agencies, not only because its criminal activity was mixed up with its intelligence-gathering capabilities but also because its gangsterism now interferes with crucial networks in other countries, such as health-care operations. “When you get ransomware hitting medical systems during a pandemic, that’s no longer just a monetary threat,” Daniel said.

North Korea’s cybercrime perpetrators often seem like faceless, amoral criminals. They also seem like victims. Costin-Andrei Oncescu, the Oxford programmer, was saddened to think of brilliant young North Korean minds being wasted in schemes to rob banks and install ransomware. But it is almost impossible to learn the stories of people from the program. David Maxwell, the former Special Forces colonel, told me that the few defectors from the Reconnaissance General Bureau’s cyber units had generally immigrated to South Korea, where they had immediately fallen under the supervision of the country’s intelligence services. Occasionally, however, it is possible to glimpse the path imposed on Kim Jong Un’s “brave warriors.”

Ri Jong Yol was a mathematics prodigy. He was born into an academic family outside Pyongyang in 1998. By the time he entered first grade, at the age of seven, he had been studying daily with a private tutor, and had already mastered the entire elementary-school syllabus. In middle school, he entered and won a national mathematics competition, and he was selected to attend a high school for gifted children. At fifteen, he was the youngest member of North Korea's team at the 2013 International Math Olympiad, in Santa Marta, Colombia.

Ri was a tall, gregarious, good-looking boy who liked playing volleyball and Ping-Pong. Unlike his teammates at the I.M.O., he enjoyed meeting the kids from other countries. He saw foreign teen-agers accessing the Internet in their spare time and wondered if he might give it a try. He had never been online. (The few computer terminals that he'd seen in village schools weren't connected to the Internet, and he'd never even seen the machines turned on, because the schools rarely had electricity.) In the end, Ri did not submit to temptation. He knew that he would be severely punished if he was caught.

Ri won a silver medal at his first I.M.O.—an exceptional result for such a young contestant. In 2014 and 2015, he made the team again, travelling to Cape Town, South Africa, and then to Chiang Mai, Thailand. He won silver medals at both events. Ri remembers how happy he was seeing other contestants who returned year after year. He also struck up friendships with South Korea's team members, with whom he shared a language. They were meant to be his enemies, but Ri couldn't see the harm in talking to them.

After he returned from the 2015 I.M.O., an acquaintance who worked at a local Workers' Party office told him that senior figures from a secretive government agency were interviewing Ri's friends and relatives. He instantly knew what was about to happen: the state would harness his talent for numbers by giving him a job as a hacker, or as a functionary in the nuclear program. Apparently, the state had decided that he didn't need to go to college before he began a career of secretive labor. The prospect filled him with dread. Working in the most guarded sections of the military meant that you were cut off from society. He would have no freedom whatsoever. He also realized that if he were instructed to join such an agency he could not refuse.

Ri knew that he could compete in the I.M.O. until he was eighteen, which meant that he could participate in one more competition before being recruited: an event at the Hong Kong University of Science and Technology. The North Korean mathletes were not heavily supervised at the competition, and Ri was on friendly terms with the teachers who accompanied the team. After winning another silver medal, Ri took his chance. He walked out of the dorm where he was staying and hailed a cab to the airport, where—with the help of a friendly airline worker—he found the address of the South Korean consulate. He took another taxi there and told a South Korean diplomat that he wished to defect. He then spent seventy days in Hong Kong, waiting nervously while the South Korean delegation negotiated his safe passage to Seoul. (After Ri's defection, North Korea suspended its I.M.O. program for two years, and now sends a government agent with the team, to insure that nobody escapes.)

Ri is now twenty-three and goes by a South Korean name. He is studying mathematics at Seoul National University. He has not seen his parents since he defected. In a recent conversation, he told me that he had developed his escape plan without any outside help, but he may have been protecting his loved ones. In North Korea, the families of defectors often meet grim fates. Ri said that he had no regrets about leaving his native country. Since his escape, he has considered how his talent would have been squandered had he stayed in Pyongyang. In Seoul, he saw only possibilities. He told me, with excitement, that he was hoping to spend a year in the United States, on an exchange program.

One of the first things that Ri did after he landed in South Korea in 2016 was go online. With the help of a mentor, he set up a Gmail account. The mentor then encouraged him to make his first Google search. He was momentarily at a loss. In North Korea, where information was strictly controlled, Ri's curiosity had been insatiable. But now, with the world seemingly at his fingertips, he felt overwhelmed by choice. There was so much to know. Ri opened a search box and typed "북한/北韓": "North Korea." ♦

An early printing of this story misstated the approximate latitude of the border between North and South Korea. An earlier version misstated the name of the think tank the Foundation for Defense of Democracies.
