Testimony before the House Committee on Foreign Affairs

Subcommittee on Indo-Pacific

"Illicit IT: Bankrolling Kim Jong Un"

Jean H. Lee

Journalist

Host of the Lazarus Heist podcast, BBC World Service

Former Korea director, Woodrow Wilson International Center for Scholars

Former AP Pyongyang/AP Seoul bureau chief

July 27, 2023

U.S. Capitol, 2200 Rayburn House Office Building

Chairwoman Kim, Ranking Member Bera, distinguished Members of the Subcommittee: Thank you for inviting me to testify at today's hearing on "Illicit IT: Bankrolling Kim Jong Un."

I am honored to be here on the Hill on this day, of all days, the 70th anniversary of the armistice that brought the Korean War to a halt. It was on this day 70 years ago that my father received the best birthday gift that a child of the war could wish for: a cease-fire. He turned 13 that day. Unfortunately, that truce never became a peace treaty, and 70 years later, the war that Kim Il Sung started in 1950 with tanks and rifles is being carried on by his grandson Kim Jong Un. But the grandson's weapons of choice are not rifles but ballistic missiles and nuclear bombs, weapons that take the conflict well beyond the confines of the Korean Peninsula.

Today, there is a new battleground that did not exist in the grandfather's era: cyberspace. Infantrymen are not Kim Jong Un's prized soldiers; his star warriors are nuclear scientists and computer hackers who are using science and technology to fight and steal on their leader's behalf. And unless we include this new battleground in the strategy to counter North Korea, there is little chance of constraining a weapons program that is growing more threatening and more destabilizing by the day.

New leader, new threats

North Korea today is more isolated than ever. The borders remain closed to most trade and traffic, and international sanctions remain in place. And yet, Kim Jong Un has the resources to conduct an unprecedented, accelerated campaign of illicit weapons testing. This year's highlight was the test launch two weeks ago of the centerpiece of his arsenal: the Hwasong-18, a solid-fuel intercontinental ballistic missile designed to carry multiple warheads with the range to strike us here in Capitol Hill.

We are aware of the threats these weapons pose. But what can be done to stop North Korea at a time when nuclear negotiations and diplomacy remain stalled?

I believe the key to building a counter strategy lies in understanding who Kim Jong Un is, what drives him, how he sees the world, and how he is seeking to build his legacy, at home and abroad. It requires understanding how he is using science and technology to build loyalty among the next generation. It requires understanding how he has incorporated computers and technology into the Kim family tactics for illicit financing and asymmetric. It requires understanding that Kim has put cyber tactics at the center of his strategic thinking, and that he is circumventing traditional measures, such as sanctions, by waging a hidden war in cyberspace through cyber warfare, cyber espionage and cyber theft.

My colleagues here today are deeply knowledgeable about nuclear proliferation, illicit financing, human rights, and cybersecurity. My testimony seeks to complement their expertise by sharing observations and analysis based on years of watching North Korea, not just from Washington as an analyst but also up close, on the ground in Pyongyang, as a journalist. My observations and analysis are solely my own.

From 2008 to 2017, I made extensive visits to North Korea, where I became the first American journalist allowed to join the foreign press corps in Pyongyang. I was there for the last few years of Kim Jong Il, the succession period to prepare Kim Jong Un to succeed him, and the early years of Kim Jong Un's rule when I opened an AP news bureau in Pyongyang.

One thing that caught my eye was the strategy of using science and technology to build up this young new leader's profile in a country where he was a stranger to his people. The goal was to paint him as the reincarnation of his revered grandfather — but a modern version, a visionary who would use computers to take his analog country into the 21st century.

I spent a lot of time in computer labs at North Korea's top universities, in conversation with students and professors. It was apparent that a targeted investment was being made in some students, at some well-outfitted facilities, to train them to be very skilled at computing. I wondered if there was another purpose. The North Koreans are efficient; they think several steps ahead. There is almost no spontaneity in a country as rigid as North Korea. And there is always more than one purpose for every policy directive, including computers.

These suspicions were confirmed with the Sony Pictures hack in 2014, a cyberattack in which hackers not only took not only took down the company's network, locking employees out of their computers and offices, but also stole private communications and unreleased films. The theft included a comedy called "The Interview" that portrayed the assassination of Kim Jong Un. The cyberattack, threats and humiliating revelations that ensued were an act of revenge and disruption -- and a chance for the suspected hackers to plant a flag about their cyber capabilities. President Obama named North Korea as the culprit.

From there, the hackers set their sights on theft, and nearly succeeded in stealing $1 billion from the Bangladesh Bank in 2016. Then, in 2017, hackers took more than 300,000 computers in 150 countries hostage in exchange for ransom in what is known as the WannaCry attack.

Some of these cyberattacks may ring a bell. But it is easy to underestimate cyberattacks from hackers who hail from a country disconnected from the Internet. There is a tendency to overlook North Korean hackers as a serious threat.

In 2020, I joined the BBC to carry out investigative reporting and research that allowed me to revisit these cyberattacks in greater detail as well as explore more recent cryptocurrency thefts. The goal was to explain the attacks in simple, straightforward terms, investigate how North Korean hackers operate, and to put the cyberattacks into political context. The podcast series is called the Lazarus Heist, a name that highlights how these hackers operate as modern-day bank robbers. The name comes from the nickname the Lazarus Group, given to them by a private cybersecurity firm, after the Biblical figure who comes back from the dead.

Hacking as a form of patriotism

Relying on illicit sources of funding is nothing new for North Korea. North Korea's economic struggles deepened following the collapse of the Soviet Union in 1991 and the loss of the safety net that the Eastern bloc provided. Shifting geopolitics compelled Kim Il Sung to reconsider his foreign policy, and he began to see ballistic missiles and nuclear weapons as a path to guaranteeing North Korea's relevance and security — and his family's hold on power.

That investment in ballistic missiles and nuclear weapons has drawn sanctions ever since. North Korea has adapted to life with sanctions by becoming creative with its methods for illicit financing. Under Kim Jong Il, that included supernotes, counterfeit cigarettes, methamphetamines, and smuggled luxury to keep his power base happy, according to the FBI, which embarked on elaborate ruses to trap North Korea and its partners.

Kim Jong Un, born in the mid-1980s, is a millennial who was educated in Switzerland and could see how computers were changing the world. He was in his early 20s when his father suffered a stroke in 2008, hastening his appointment as heir apparent. The inner circle now faced the challenge of how to engineer a transition of leadership to a young man, particularly the peers who would be his power base.

Science and technology became the platform for building loyalty. My North Korean staff, like my South Korean staff, loved all tech gadgets. Cellphones, Bluetooth headsets and laptops became status symbols as the regime doled out electronics as political prizes. The message was clear around us: Propaganda posters promoted computers and mathematics, linking them to ballistic missiles and nuclear weapons. A TV drama I analyzed for the Korea Economic Institute encouraged students to serve their country through science and technology.

Students who showed promise in math were given special access to resources, and placed under enormous pressure to perform. The best were sent abroad to compete for North Korea in international Math Olympiads. The next step, according to one former Math Olympiad winner who defected during a competition in Hong Kong, told me would be to apply their skills in the military as "cyber warriors."

Hackers were sent abroad to China, Southeast Asia and the Middle East to learn how we live, bank and socialize online in the rest of the world. Many were on legitimate visas as IT workers.

In June 2018, the FBI filed a 179-page criminal complaint charging a North Korean identified as Park Jin Hyok with conspiracy to commit computer fraud and abuse, and conspiracy to commit wire fraud, between September 2014 and August 2017. Park has not been arrested. But the complaint, unsealed in September 2018, helped to paint a portrait of one of the key suspects behind the cyberattacks on Sony Pictures, the Bangladesh Bank and the networks targeted by WannaCry.

The FBI described Park as a computer programmer who graduated from a top university in Pyongyang before being dispatched to Dalian, China, as early as 2002 to work for a North Korean company to create gaming and gambling programs for global clients. By day, he was a programmer. By night, he was a hacker, according to the FBI. Agents followed him online as he set up an email address, drafted a resume and proceeded to use social media to lay the groundwork for the attacks that would unfold in 2014, 2016 and 2017.

Each of the attacks outlined by the FBI, and brought to life in the Lazarus Heist, was meticulously and methodically planned. Each cyberattack targeted different elements of computing networks and financial systems. They may have started with the seizure of Sony's private network but with WannaCry, the intrusion was global.

With the Bangladesh Bank heist, the hackers managed to gain access to the global SWIFT banking system. The goal was to steal $1 billion dollars. The heist sped along until one small detail happened to trigger a check in the Fed. Most of the payment were stopped but five transactions went through. Eventually, the North Koreans are believed to have pocketed $81 million, much of the cash laundered at a casino in the Philippines.

The final haul from the Bangladesh theft may have been relatively small but the scope and scale of the attempt revealed an ambitious campaign on the part of the suspected hackers as well as a vast network of middlemen and money launderers across Asia.

In 2016 and 2017, the UN Security Council sought to stop the flow of financing with tough sanctions supported by China and Russia. Member nations were to send North Korean workers home by December 2019. However, many IT workers are believed to remain abroad, as outlined in the most recent UN Panel of Experts report.

It is important to note that after ramping up testing in 2017, Kim Jong Un declared himself satisfied with his nuclear program and shifted to a phase of diplomacy. However, the

cyberattacks did not cease during the season of diplomacy in 2018 and 2019. In Season 2 of the Lazarus Heist, we weave a spate of cyberattacks in with the timeline for diplomacy to show how the North Koreans may have been looking to shore up funds as a contingency even as Kim was negotiating a nuclear deal. Those negotiations failed, and North Korea retreated into isolation in late 2019.

Meanwhile, the cyberattacks, the missile tests, and the cat-and-mouse chase have continued.

In February 2021, the Department of Justice announced new charges against three North Koreans accused in attacks that yielded $1.3 billion from cyber and cryptocurrency thefts. In March 2022, the Lazarus Group was accused of stealing nearly $620 million in cryptocurrency from an online video game called Axie Infinity that runs on the Ethereum blockchain in what the US government called the largest virtual currency heist to date. In June 2022, the blockchain company Harmony Bridge reported a theft of $100 million; the FBI named the Lazarus Group as suspects.

Where is that money going? In May, Deputy National Security Advisor for Cyber & Emerging Tech Anne Neuberger estimated that half of the funding for North Korea's nuclear weapons may be coming from cyber theft.

Conclusion

The FBI and Department of Justice have been relentless in their pursuit of North Korean hackers. In addition to the indictments against three North Koreans, the FBI has been working with partners at home and abroad to target the middlemen allegedly hired by North Koreans. They include the 2021 arrests of the Nigerian social media influencer Ramon Abbas, aka Hushuppi, and Ghaleb Alaumary, known online as Big Boss.

But the challenge is multiplying. While illicit financing during the Kim Jong Il years might be characterized as a game of cat and mouse, the chase in the Kim Jong Un era is now more like whack-a-mole due to the nature of the Internet.

UN Security Council sanctions are only effective when enforced by member nations; that is not happening. Strategic competition between the United States and China, and geopolitical divisions between the West and Russia over the Ukraine war, make further attempts to bring Russia and China on board with new, tightened UN sanctions difficult.

The U.S. Treasury has been aggressive in targeting specific companies and individuals, as well as technology utilized by hackers. In May 2022, Treasury sanctioned the virtual currency mixer Blender, allegedly used to launder stolen cryptocurrency from the Axie Infinity heist. In August

2022, they added the mixer Tornado Cash, linked to the Harmony Bridge theft. An advisory issued by the State Department, Treasury and FBI warned against hiring North Korean IT workers.

Cybersecurity firms such as Mandiant and Chainalysis have been aggressive in tracking suspected hackers.

However, policymaking has been slow to keep up. North Korean cyberattacks must not be limited to discussions about cybersecurity but must be woven into discussions about sanctions, diplomacy, the military, the economy and Kim Jong Un's strategic thinking. Further investment must be made to bring the worlds of law enforcement, cybersecurity and policy together. This effort should include partners and allies, including South Korea, which has been a target of North Korean cyberattacks for far longer than the United States. Political interests — in both the United States and South Korea — must not overshadow the shared urgency of addressing North Korea's cyber ambitions.

It may be hard to fathom how North Korea — one of the poorest countries in the world, a country disconnected from the global Internet, a nation so bereft of electricity that it appears like a black hole from space — could possibly produce some of the world's most successful hackers. But where they fall short in sophistication, the North Koreans make up for in sheer persistence, patience and motivation. It is that very desperation that drives the hackers' ambitions. They are clever and resourceful, and spend enough time on their mission to identify weaknesses in new technologies, particularly in regulation when it comes to cryptocurrency. Cyber theft is a low-cost, high-yield tactic. Cyberspace and the difficulty of attribution provide a convenient cloak.

I am grateful for the Committee's attention to this issue. This is a matter of national and global security. Unchecked, North Korea's campaign of cyber theft will continue to have destabilizing consequences by contributing to the nuclear threat. Financial gain through cyber will give Kim Jong Un more space and motivation to shut out the world, dimming prospects for diplomacy. That isolation and defiance threaten to jeopardize the peace and stability of a region important to the United States and its allies. And finally, I would like to make a plea on behalf of the 26 million people of North Korea who pay the ultimate price when resources are focused on nuclear weapons, not basic necessities, and when their leader chooses a path of isolation that keeps them locked in a repressive, anachronistic existence while the rest of the region flourishes around them.

Thank you for your attention to this issue. I look forward to your questions.