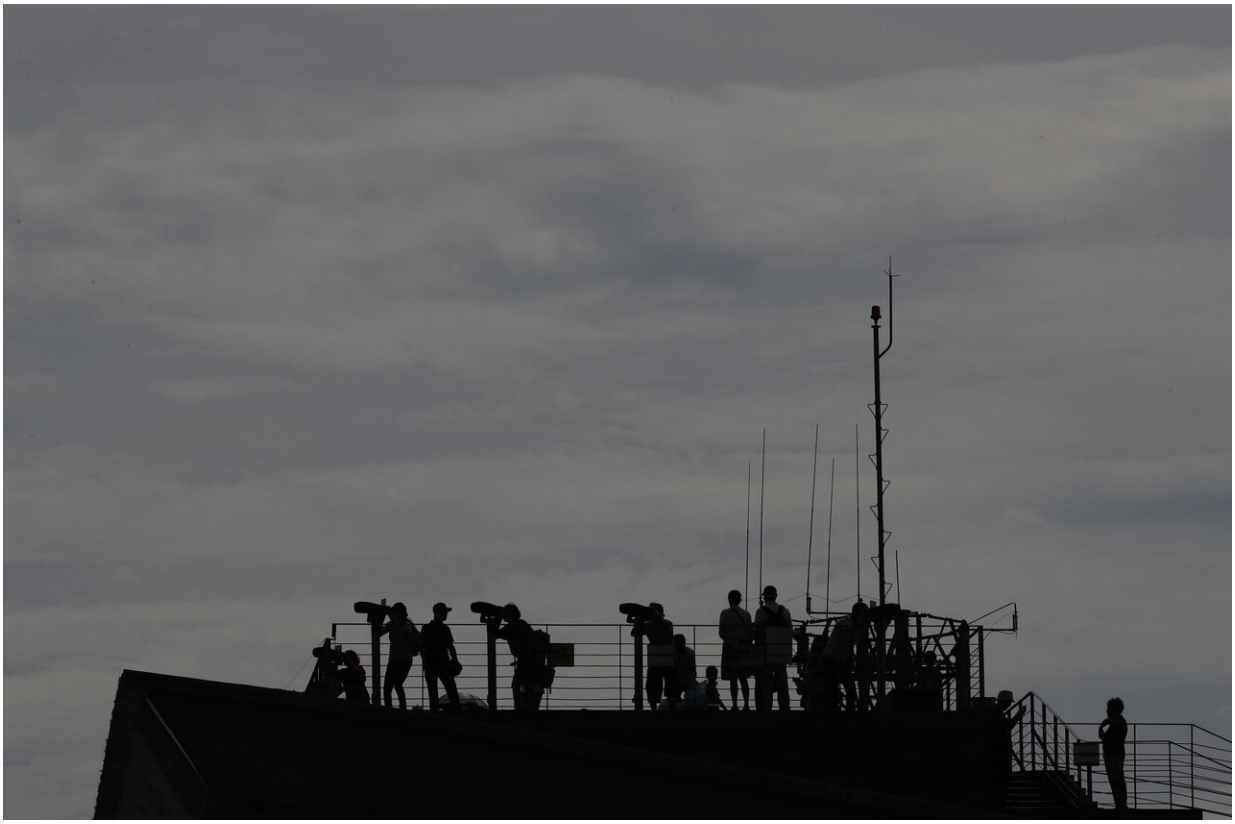
UN probing 35 North Korean cyberattacks in 17 countries

August 13 2019, by Edith M. Lederer



In this Sunday, Aug. 11, 2019, file photo, visitors watch the North side from the Imjingak Pavilion in Paju, South Korea. U.N. experts say they are investigating at least 35 instances in 17 countries of North Koreans using cyberattacks to illegally raise money for its nuclear program, and they are calling for sanctions against ships providing gasoline and diesel to the country. (AP Photo/Lee Jin-man, File)

U.N. experts say they are investigating at least 35 instances in 17 countries of North Koreans using cyberattacks to illegally raise money for weapons of mass destruction programs—and they are calling for sanctions against ships providing gasoline and diesel to the country.

Last week, The Associated Press quoted a summary of a report from the experts which said that North Korea illegally acquired as much as $2 billion from its increasingly sophisticated cyber activities against financial institutions and cryptocurrency exchanges.

The lengthier version of the report, recently seen by the AP, reveals that neighboring South Korea was hardest-hit, the victim of 10 North Korean cyberattacks, followed by India with three attacks, and Bangladesh and Chile with two each.

Thirteen countries suffered one attack—Costa Rica, Gambia, Guatemala, Kuwait, Liberia, Malaysia, Malta, Nigeria, Poland, Slovenia, South Africa, Tunisia and Vietnam, it said.

The experts said they are investigating the reported attacks as attempted violations of U.N. sanctions, which the panel monitors.

The report cites three main ways that North Korean cyber hackers operate:

—Attacks through the Society for Worldwide Interbank Financial Telecommunication or SWIFT system used to transfer money between banks, "with bank employee computers and infrastructure accessed to send fraudulent messages and destroy evidence."

—Theft of cryptocurrency "through attacks on both exchanges and users."

— And "mining of cryptocurrency as a source of funds for a professional branch of the military."

The experts stressed that implementing these increasingly sophisticated attacks "is low risk and high yield," often requiring just a laptop computer and access to the internet.

The report to the Security Council gives details on some of the North Korean cyberattacks as well as the country's successful efforts to evade sanctions on coal exports in addition to imports of refined petroleum products and luxury items including Mercedes Benz S-600 cars.

One Mercedes Maybach S-Class limousine and other S-600s, as well as a Toyota Land Cruiser, were transferred from North Korea to Vietnam for last February's summit between the country's leader Kim Jong Un and U.S. President Donald Trump, the experts said, adding that Vietnam said it asked for but was never provided a list of vehicles being brought into the country.

The panel also said it obtained information that the Taesong Department Store in Pyongyang, which reopened in April and is selling luxury goods, is part of the Taesong Group which includes two entities under U.N. sanctions and was previously linked to procurement for North Korea's ballistic missile programs.

The panel recommended sanctions against six North Korean vessels for evading sanctions and illegally carrying out ship-to-ship transfers of refined petroleum products.

Under U.N. sanctions, North Korea is limited to importing 500,000 barrels of such products annually including gasoline and diesel. The U.S. and 25 other countries said North Korea exceeded the limit in the first four months of 2019.

The panel also recommended sanctions against the captain, owner, and parent company of the North Korean-flagged Wise Honest, which was detained by Indonesia in April 2018 with an illegal shipment of coal.

As for North Korea's military cooperation with other countries, the experts said Iran rejected an unnamed country's allegation that two North Korean entities under sanctions maintained offices in Iran—the Korea Mining Development Trading Corporation known as KOMID, which is the country's primary arms dealer and main exporter of goods and equipment related to ballistic missiles and conventional weapons, and Saeng Pil Company.

The experts said they have requested information from Rwanda on a report that North Koreans are conducting special forces training at a military camp in Gabiro. And they said they are also waiting for a response from Uganda "to multiple inquires" about reports indicating specialized training is being conducted in the country, and KOMID and North Korean workers maintain a presence.

As examples of North Korean cyberattacks, the panel said hackers in one unnamed country accessed the infrastructure managing its entire ATM system and installed malware modifying the way transactions are processed. As a result, it forced 10,000 cash distributions to individuals working for or on behalf of North Korea "across more than 20 countries in five hours."

In Chile, the experts said, North Korean hackers demonstrated "increasing sophistication in social engineering," by using LinkedIn to offer a job to an employee of the Chilean interbank network Redbanc, which connects the ATMs of all the country's banks.

According to a report from one unnamed country cited by the experts, stolen funds following one cryptocurrency attack in 2018 "were

transferred through at least 5,000 separate transactions and further routed to multiple countries before eventual conversion" to currency that a government has declared legal money, "making it highly difficult to track the funds."

In South Korea, the experts said, North Korean cyber actors shifted focus in 2019 to targeting cryptocurrency exchanges, some repeatedly.

The panel said South Korea's Bithumb, one of the largest cryptocurrency exchanges in the world, was reportedly attacked at least four times. It said the first two attacks in February 2017 and July 2017 each resulted in losses of approximately $7 million, while a June 2018 attack led to a $31 million loss and a March 2019 attack to a $20 million loss.

The panel said it also investigated instances of "cryptojacking" in which malware is used to infect a computer to illicitly use its resources to generate cryptocurrency. It said one report analyzed a piece of malware designed to mine the cryptocurrency Monero "and send any mined currency to servers located at Kim Il Sung University in Pyongyang."