PACNET

KEEP AN EYE ON NORTH KOREAN CYBER-CRIME AS THE COVID-19 SPREADS

BY TODD WIESEL

Todd Wiesel (tjw2144@columbia.edu) is a student at Columbia University completing his bachelor's in Political Science and East Asian Studies. He is also an MBA candidate at London Metropolitan University, where his research focuses on the impact and effects of corporate social responsibility on capital markets. He previously earned a master's degree in Innovation, Leadership and Business Management from Oxademy Business School, and is a former Kim Koo Fellow at the Korea Society, focusing his research on the inter-Korean negotiation process. Before enrolling in Columbia, he worked as the managing director of The Negotiation Institute. Prior to his tenure at TNI he served as an urban warfare and counter-terror specialist in the Israel Defense Forces.

The Covid-19 outbreak continues to cause tumult in the global economy, with countries like South Korea and Italy reporting a rapid increase in diagnoses and many companies requesting that employees work from home to keep the virus from spreading.

In North Korea's case, it has had its Chinese borders closed for over a month, long before the rest of the world began to react to the virus. Even if it were, as its state media claims, coronavirus-free, how long could their economy sustain total global isolation? By sealing their border with their largest economic partner, North Korea has effectively placed itself at the mercy of UN sanctions.

Kim Jong-un knows that his country cannot last like this for very long, and with so much of his power stemming from the support of Pyongyang's elite, we must prepare ourselves for their reaction. Learning from the DPRK's past behavior, national security leaders should be less concerned about military action and focus their attention on shoring up their cyber defenses.

Jonathan Corrado, policy director for the Korea Society, noted in a recent article the extreme lengths North Korea has gone to prevent the spread of coronavirus in the country. These border closures, although necessary to reduce the chance of viral contagion, will have a lasting impact on their already minuscule economy.

Even prior to the closures, UN Security Council sanctions already heavily impacted North Korean exports. Yet, despite the cuts to the DPRK's exports, World Bank data indicates that North Korea's GDP has been slowly rising since 2015. This financial discrepancy can be explained primarily through North Korea's burgeoning international crime economy.

According to the 2017 Global Initiative against Transnational Organized Crime's 30-page report entitled Diplomats and Deceit: North Korea's Criminal Activities in Africa, North Korean diplomats travel "regularly to Pyongyang and Beijing in China with diplomatic bags filled with contraband." These members of diplomatic missions to countries on the African content would smuggle illegal items such as diamonds, gold, and ivory back to the DPRK and China, where they sell for exorbitant prices.

In 2016, Angolan leaders had been meeting with North Korean liaisons to collaborate on national security projects. This collaboration did not come as a surprise—Angola has long been militarily linked to North Korea. A 2015 *Washington Times* article identified a number of UN sanctions that Angola had violated by engaging in business with the DPRK. Angola was found to be purchasing military training, weapons, and over 4.5 tons of ship engines and parts, to service the naval boats they had purchased from Pyongyang in 2011. North Korean arms are also believed to be regularly supplied to Ethiopia, where they have been providing and manufacturing weapons since the mid-80s.

North Korea has not limited its illegal activities to Africa. DPRK embassies have long been (correctly) accused of facilitating the international trade of crystal

meth, taking advantage of the high premiums their products can garner and abusing diplomatic channels to smuggle the drug into foreign countries.

However, thanks to Covid-19, protecting the elites of Pyongyang has become such a priority that the state has sent all Chinese diplomats back to China, while simultaneously suspending all flights, trains, and travel with the outside world. The shutdown means North Korea will no longer be able to rely on its diplomats returning from trips abroad to produce the much-needed cash for the economy.

To ensure that their country can continue to function while they weather the global crisis, North Korea may very likely double down on cybercrime. While smuggling and other forms of illicit trading require the physical moving of goods and/or services, cybercrime can be committed from anywhere, even a sealed North Korea.

North Korea has already proven itself adept at infiltrating computer systems around the world. Bureau 121, an elite cyber warfare agency in North Korea, has been named the leading suspect for many famous cyber-attacks, including the Sony hack in 2014, the SWIFT banking hack in 2015, and the Bangladesh Bank Robbery in 2016. All together, these operations are estimated to have cost over $100 million in stolen funds, and billions of dollars in cybersecurity damages.

The most alarming of North Korea's alleged cyberattacks is the 2017 WannaCry ransomware attack. This ransomware—which locked 200,000 devices in a single day and demanded ransom payments in bitcoin—caused severe disruptions among businesses around the globe. But WannaCry did not just target private corporations. The attack also infected the National Health Service (NHS) in England and Scotland, causing NHS services to divert ambulances and turn away patients.

Fortunately, May 2017 was not a time of global health panic. However, as the Covid-19 continues to spread, the DPRK's vice minister of public health declared that the Chinese border will remain shut indefinitely until a cure is completely ready. We must prepare ourselves for attempts to disrupt healthcare systems. An economically strangled North Korea has much to gain from global disruptions, and we must brace ourselves and develop our cyber defenses accordingly.