RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 136 – 30 December 2022

Mapping North Korean Cyber Strategies

By Michael Raska

SYNOPSIS

The impact of the COVID-19 pandemic together with stricter international sanctions have altered the direction, character, and modus of North Korea's cyber operations. It increased the internal pressure on the cyber units to generate financial resources to sustain the Kim-Jong un regime and its strategic weapons programmes, by raising the relative sophistication and creativity of hacking methods.

COMMENTARY

In the recently published IISS report, *Cyber Capabilities and National Power: A Net Assessment*, North Korea is ranked in the third-tier category of cyber powers, an assessment based on strengths or potential strengths in some capability indicators such as offensive cyber operations and on significant weaknesses in others such as sophisticated cyber-intelligence capability.

Indeed, compared to leading cyber powers such as the United States, China, and Russia, North Korea has limitations in the use of cyberspace for coercive political purposes. However, North Korea is unique in its ability to offset its strategic inferiority in conventional military capabilities, gain access to foreign science and technology intelligence, and evade diverse sanctions.

Decentralised Cyber Operations

Over the past decade, North Korea's cyber teams have gradually developed resources, malware arsenals, and coding capabilities based on their experiences and lessons learned from attacking different targets worldwide, and by sharing networking infrastructure, and social engineering skills. The net result has been a progressive adaptability, creativity, and sophistication of North Korean hacker groups.

North Korean hacker groups have been geographically dispersed in China, Russia, Southeast Asia, and even Europe, acting independently or mutually supporting each other based on their specific cyber missions: from cyber espionage and information manipulation (APT 37, Kimsuky, Sun Team); ransomware and financial extortion (APT 38, Andariel); to various disruptive and destructive cyber operations (Lazarus Group).

At the same time, Pyongyang has been able to protect its critical infrastructure from potential reprisals, limiting its online access, dependencies, and network vulnerabilities by relying on China and Russia's networks. This has allowed North Korea's hacker groups to exploit vulnerabilities in critical infrastructures globally, including transportation networks, telecommunications, electric and nuclear power grids, aviation systems, finance, and media.

Impact of Sanctions and COVID-19 Pandemic

Since 2016, North Korea has coped with progressive waves of UN and US economic sanctions imposed as a response to its nuclear and ballistic missile tests. These sanctions have precluded Pyongyang from accessing global financial markets, imposed strict import and export controls, and essentially banned foreign banks, companies, and individuals from conducting economic activities with North Korea.

These tailored financial and economic sanctions coupled with the COVID-19 pandemic and resulting border closures have also likely increased pressure on North Korea's cyber units to generate financial resources for the Kim Jong-un regime and its military research and development.

While the sanctions have had an adverse impact on North Korea's economy, evident in project delays and resource constraints, they have failed to deter or to change North Korea's development of its nuclear weapons programmes. Indeed, North Korea has showcased its military-technological developments over the past five years, mainly an expanding catalogue of increasingly capable strategic ballistic missiles.

In December 2022, South Korea's main spy agency, the National Intelligence Service (NIS), revealed that North Korean hacker groups had illegally extracted an estimated $1.2 billion in cryptocurrency and other virtual assets since 2017, with more than half of it in 2022 alone. And in 2020, North Korea's *Lazarus Group* had been attributed with a major cryptocurrency theft, involving the extraction of about $275 million worth of cryptocurrency from the Singapore-based exchange, KuCoin. While KuCoin recovered about $204 million of the stolen funds, the crypto hack showed the creative ways in which North Korea's Lazarus Group exploited novel financial platforms such as decentralized finance (DeFi) to launder a portion of the stolen funds.

Searching for Novel Attack Vectors

The second major shift in North Korean cyber operations during the COVID-19 pandemic has focused on the expansion of cyber espionage operations to obtain research data and intelligence on vaccine and treatment technologies. In January 2021, before the Eighth Party Congress, North Korea reportedly established a new elite hacking group, Bureau 325, tasked with obtaining research data on vaccine technology related to COVID-19. A month later, South Korea's NIS reported that North

Korean cyber groups attempted to hack the servers of US drug manufacturer Pfizer and South Korean companies developing coronavirus vaccines and treatments.

The Bureau 325 can be seen as a next generation of North Korean cyber force, composed of elite members of existing hacking groups, and newly hired top university graduates in computer science, biochemistry, mathematics, and related fields from top colleges such as the Kim Chaek University of Technology and Kim Il-Sung University.

The newly-formed teams point toward a new trend that may characterise the next phase of North Korean cyber operations and strategies, i.e., external collaborations with select hacker groups from overseas, working synergistically together to amplify diverse cyber skills and proficiencies. In 2019, for example, the Russian APT 28, Fancy Bear, had reportedly linked up with two of North Korea's hacker groups, Lazarus and an obscure group Cerium, to jointly target seven leading pharmaceutical companies involved in COVID-19 research in the United States, Canada, France, India, and South Korea. Evidence shows the Cerium group used targeted spear-phishing emails, and masqueraded as representatives from the World Health Organization coordinating efforts to contain the COVID-19 pandemic.

As the cyber defences of major cyber powers become more sophisticated with the use of emerging technologies such as artificial intelligence, North Korean cyber units must also enhance their technical sophistication, operational security, and funding. The use of novel attack vectors may propel them to work together or in selective alliances with other state-sponsored hacking groups.

Limitations of International Responses

International cooperation on detecting, protecting, and responding to North Korean cyber operations has been constrained by varying threat perceptions and interests. China and Russia, for example, have consistently denied providing a haven for North Korean hacker groups.

Meanwhile, the United States and South Korea have held biannual meetings on cyber policy issues since 2012, working on ways to strengthen bilateral cooperation in tackling cyber challenges and implementing measures to protect critical government infrastructure and online security. However, the US-ROK alliance has not clarified joint strategy, obligations, and appropriate responses to major disruptive or destructive cyberattacks.

The US-ROK alliance's ability to deter and effectively respond to North Korean cyber threats is also constrained by political considerations on the future of the alliance and the US military presence in Korea. One of the main impediments is the question over the interpretation of a potential destructive cyber-attack as an "armed attack" in the context of the 1953 Mutual Defence Treaty, which would trigger a US military response such as, for example, assuming wartime operational command and control of South Korean forces.

As a result, North Korea can use its cyber capabilities along with its advancing nuclear and ballistic missile programmes as a form of hybrid warfare in which cyber-enabled Weapons of Mass Effectiveness complement its Weapons of Mass Destruction in a

unified political strategy to impose a decision on the United States and the international community to recognise the sovereignty and legitimacy of North Korea under Kim Jong-un.

Michael Raska is Assistant Professor and Coordinator of the Military Transformations Programme at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg