Celeste Bean

March 5, 2021

POL557A

Role of Cyber-Attacks in Security on the Korean Peninsula

Contents

Introduction to the Security Dynamic on the Korean Peninsula

Relations between North and South Korea have existed in a state of perpetual tension since the 1953 Korean Armistice Agreement, signed at the end of the Korean War, though the conflict never formally ended. Neither the Republic of Korea in the South nor the Democratic People's Republic of Korea in the North "recognize the other as a legitimate state," with each state's constitution claiming full control of the peninsula (Hewlett-Packard 8).

The power dynamics of the peninsula have evolved dramatically since the armistice. Although South Korea's GDP per capita was lower than North Korea's until 1973, South Korea firmly cemented its military, economic, and technological lead in the 21st century, owing in part to continued American support and North Korea's disastrous famine from 1994 to 1998 (Tudor, 26). An estimated 95 percent of South Korea's 50 million citizens regularly use the internet, contrasted with North Korea's estimated 50,000 users of a population of 25 million (Park 2016, 87).

In North Korea's efforts to exploit brinkmanship and maintain negotiating leverage against South Korea's military superiority, the dictatorship has "relied on various asymmetric and irregular means to sidestep the conventional military deadlock on the peninsula" (Jun, 14). Creating an atmosphere of conflict is clearly part of North Korea's military strategy, evidenced by North Korea's 26 military attacks and 221 violations of the armistice agreement from 1953 to 2015 (Jun 21). Asymmetric weapons, which allow "actors with limited financial and technical resources… to compromise high-value targets," are the only cost-effective way the impoverished North Korean government can hope "to express their political wills, create a favorable environment for negotiation," and mitigate South Korea's lead (Kshetri 184; Park 2015, 2).

In contrast, South Korea's primary goal, aided by its alliance with the United States, is to "[preserve] the freedom, safety and prosperity of their soldiers and citizens on the peninsula, and [reduce] to the greatest extent possible the risk of attacks" (Mount 39). As a well-integrated member of the international community, South Korea is also bound by international laws and norms of conduct requiring proportionality of response, which limits its retaliatory options. Typically, South Korea has allowed the United States to issue deterring threats while focusing on a defensive posture against North Korean provocations (Mount 41).

What Role Do Cyber Attacks Play in the Security Relationship on the Korean Peninsula?

Cyber-attacks have emerged as a natural and especially valuable addition to North Korea's arsenal of asymmetric weapons as "another means of exploiting U.S. and [South Korean] vulnerabilities at relatively low intensity while minimizing risk of retaliation or escalation" (Jun, 14). The late Kim Jong-Il publicly emphasized the importance of cyber capabilities, stating "the 20th century's war was a war of oil and bullets, but the 21st century's war is [an] intelligence war" (Boo 2017, 108). Estimates suggest North Korea is rapidly producing cyber experts and devotes between 10 and 20 percent of its military budget to cyberspace (Park 2015, 89).

By "launch[ing] low-intensity unconventional cyber-operations to disrupt the peaceful status quo without escalating the situation to a level [North Korea] cannot control or win," North Korea probes the conventional military deadlock on the peninsula and improves its negotiation positions, while South Korea is effectively relegated to a defensive posture to avoid escalation

(Jun 15). Cyber-attacks are especially effective against South Korea's "large cyber resources and dependency on digital culture" while also limiting retaliation in kind by virtue of North Korea's own technical unsophistication (Kshetri 185). In cyberwarfare, North Korea's disconnection from the global Internet and frequent power outages become an asset. This gives North Korea "has very much to gain and very little to lose from engaging in cyberwarfare activities" (Kshetri 191).

North Korea's Objectives through Cyberspace

Since 2004, North Korea's operations in cyberspace have pursued three main objectives: to project power and improve North Korea's negotiating position with low cost and low risk; to gain access to sensitive information about North Korea's adversaries; and to illicitly financing North Korea's government though cybercrime amidst international sanctions.

North Korea uses cyber-attacks "to achieve the government's political objectives as well as send propaganda and make armed provocations against South Korea" (Park 2015, 30). The attacks systematically "erode confidence in key commercial sectors" without warranting a full military response in retaliation (Jun 16), and North Korea has attacked myriad South Korean institutions, ranging from nuclear power plants to transportation infrastructure to publications like Free North Korea Radio (Jun 40). Analysis suggests "North Korea's cyber-attacks have certain patterns in timing and political issues" with especially large spikes around significant holidays, such as the end of the Korean War or America's Independence Day (Cisnero 38). Coordinating around symbolic dates allows North Korea to undermine South Koreans' faith in their government as well as more effectively disseminate misinformation and propaganda (Boo 2017, 104).

Secondly, collecting cyber intelligence "increases [North Korea's] comparative advantage in classified information, diplomatic negotiating positions, or future policy changes" (Geers 9). Attacks on South Korea spike each March, when the United States and South Korea conduct joint military exercises, and analysis of attacks in 2015 and 2016 clearly indicates they were launched from Chinese IP addresses known to be leased to North Korea (Park 2016, 48). Various malwares uncovered in South Korean networks explicitly searched for Korean-language military terms, indicating the adversaries were targeting South Korean command, control, communications,

computers, intelligence, surveillance, and reconnaissance assets (Jun 15). Evidence suggests North Korea has used its gathered intelligence to prepare for diplomatic missions and anticipate South Korean military operations (Park 2016, 95).

Lastly, cybercrime offers a lucrative means of financing the dictatorship despite international sanctions against North Korea's nuclear operations and "[has] brought financial gain and inserted this small and isolated country further into international political discourse" (Fei 35). North Korean hackers frequently target South Korean financial institutions and companies with identity theft and phishing emails (Park 2015, 6). A South Korean institute estimates North Korea earns "1 billion dollars per year through cyber activities," which is exceptional given North Korea's official trade volume of 10 billion dollars (Boo 2017, 109).

South Korea's Response in Cyberspace

Given North Korea's antagonism strategically operates below a threshold warranting military response, South Korea focuses on defensively responding to North Korea's attacks. South Korea first established "a cyber command in January 2010 and a cyber-protection policy team at the Defense Ministry in March 2011" in response to North Korean antagonism but did not publish an official cybersecurity strategy until 2019 (Kshetri 195). While the policy describes provisions for "actively [responding] to all cyber-attacks that infringe upon national security and national interests by concentrating national capabilities," the majority of the document focuses on defensive aspects such as "[strengthening] preventive capacity by building a system that efficiently collects, manages, and eliminates vulnerabilities in cyberspace" and "[acquiring] practical capabilities to analyze causes of cyber-attacks and identify the culprits" (Cheong Wa Dae). The South Korean government also works closely with its sophisticated domestic private sector to create public-private partnerships and improve its responses.

Conclusion

Cyberspace represents the newest and most sensitive realm for the 80-year conflict on the Korean peninsula. North Korea has adopted cyber-attacks as low-cost, high-yield provocations to maintain tension with South Korea and advance its political agenda without warranting escalatory military responses. Further south on the peninsula, South Korea has

relegated itself to a defense cyber security posture in the interest of maintaining a mostly peaceful status quo. Unless South Korea wants to dramatically upset the tenuous balance on the peninsula, South Korea must continue to develop its cyber defensive responses.

References

Boo, Hyeong-wook and Lee, Kang-Kyu. "Cyber War and Policy Suggestions for South Korean Planners." *International Journal of Korean Unification Studies*. Vol. 21, No. 2, 2012, 85–106.

Boo, Hyeong-wook and Choi, Seuon. "Crisis Pattern Change and Its Implication for National Crisis Management System." *Journal of Defense Policy Studies*. Vol. 30, no. 1, 2014.

Boo, Hyeong-wook. "AN ASSESSMENT OF NORTH KOREAN CYBER THREATS." *The Journal of East Asian Affairs*, vol. 31, no. 1, 2017, pp. 97–117. JSTOR, www.jstor.org/stable/44321274. Accessed 14 Feb. 2021.

Cheong Wa Dae National Security Office, "National Cybersecurity Strategy," April 2019.

Cisneros, M. (2015). *Cyber-Warfare: Jus Post Bellum*. Master's thesis, Naval Postgraduate School, Monterey, CA.

FEI, SU. Military Developments in Artificial Intelligence and Their Impact on the Korean Peninsula. Edited by LORA SAALMAN, Stockholm International Peace Research Institute, 2019, pp. 33–38, The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: Volume II East Asian Perspectives, www.jstor.org/stable/resrep24532.12. Accessed 18 Feb. 2021.

Geers, K., Kindlund, D., Moran, N. and Rachwald, R. (2013) "World War C: Understanding Nation-State Motives behind Today's Advanced Cyber-attacks," retrieved from www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf.

ICT Cyber Desk. Case Study. International Institute for Counter-Terrorism (ICT), 2013, pp. 24–29, *Cyber-Terrorism Activities Report No. 3*, www.jstor.org/stable/resrep09470.5. Accessed 18 Feb. 2021.

Jun, Jenny, et al. North Korea's Cyber Operations: Strategy and Responses. Center for Strategic and International Studies, 2016.

Kramer, Franklin D., et al. CYBER, EXTENDED DETERRENCE, AND FORWARD THEATERS. Atlantic Council, 2017, pp. 18–21, CYBER AND DETERRENCE: The Military-Civil Nexus in High-End Conflict, www.jstor.org/stable/resrep03691.8. Accessed 18 Feb. 2021.

Kshetri, Nir. "Cyberwarfare in the Korean Peninsula: Asymmetries and Strategic Responses." *s*, vol. 31, no. 3, Sept. 2014, pp. 183–201. EBSCOhost, doi:10.1007/s12140-014-9215-1.

Mount, Adam, and Mira Rapp-Hooper. "Nuclear Stability on the Korean Peninsula." *Survival (00396338)*, vol. 62, no. 1, Feb. 2020, pp. 39–46. *EBSCOhost*, doi:10.1080/00396338.2020.1715063.

Park, J. (2015) *Finding Effective Responses against Cyber Attacks for Divided Nations*, M.S. thesis, U.S. Naval Postgraduate School, Monterey, CA, US, December.

Park, J, et al. “South Korea’s Options in Responding to North Korean Cyber-attacks.” *Journal of Information Warfare*, vol. 15, no. 4, 2016, pp. 86–99. JSTOR, www.jstor.org/stable/26487553. Accessed 18 Feb. 2021.

Platte, James E. “Defending Forward on the Korean Peninsula: Cyber Deterrence in the U.S.-ROK Alliance.” *The Cyber Defense Review*, vol. 5, no. 1, 2020, pp. 75–94. JSTOR, www.jstor.org/stable/26902664. Accessed 14 Feb. 2021.

Sangsuvan, Kitsuron. “Resolving the Conflict on the Korean Peninsula by Preventive Diplomacy.” *International Journal on World Peace*, vol. 37, no. 4, Dec. 2020, pp. 27–57. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=asn&AN=147695166&site=ehost-live.

Siers, Rhea. “North Korea: The Cyber Wild Card 2.0.” *Journal of Law & Cyber Warfare*, vol. 6, no. 1, 2017, pp. 155–165. JSTOR, www.jstor.org/stable/26441283. Accessed 18 Feb. 2021.

Tudor, Daniel, and James Pearson. *North Korea Confidential: Private Markets, Fashion Trends, Prison Camps, Dissenters and Defectors*. , 2015. Print.

Turell, Johan, et al. “Lessons from Past Cyber Incidents and Country Studies.” Stockholm International Peace Research Institute, 2020, pp. 32–42, Cyber-Incident Management: Identifying and Dealing with the Risk of Escalation, www.jstor.org/stable/resrep26199.11. Accessed 18 Feb. 2021.