The American
Foreign Policy Council
Defense Technology Program Brief

May 2018 | Washington, D.C. | No. 17

Understanding North Korea's Cyber Strategy

By: Jenny Jun

Briefing Highlights

North Korea's acquisition of cyber capabilities is a natural extension of its existing national strategy. Current negotiations with North Korea should incorporate cyber dimensions.

• • •

During conflict, North Korea is likely to disrupt and degrade C4ISR capabilities, which renders enemy precision weapons less effective and boosts effectiveness of its own conventional forces.

• • •

North Korea will continue to use cyber operations for disruptive and coercive purposes below the threshold of war.

• • •

While North Korea may not be the most technically sophisticated actor, there are also less options to deter North Korea both in and out of cyberspace, giving them a unique asymmetric advantage.

• • •

Policymakers now involved in negotiations with North Korea regarding its nuclear and ballistic missile program should consider the associated cyber dimensions of their efforts. A denuclearization agreement is likely to change escalation dynamics in the event of a cyber attack, and the room for misunderstanding and miscalculation may increase without some mutual agreement about expected behavior in this domain.

How does North Korea use cyber means to achieve its political and military objectives?[1] Ever since the Korean War, North Korea's stated foreign policy goal has been to reunify the Korean peninsula under its rule. However, by the 1980s, winning a conventional war on the peninsula had become unrealistic, and the military balance between the North and South had started to shift in favor of the latter. With the end of the Cold War, Russian and Chinese patronage diminished, while the U.S.-ROK alliance grew stronger. In this strategic context, how does North Korea ensure regime security, deter foreign aggression, and achieve this objective without explicitly taking it by force?

North Korea's answer to this question has been to increasingly rely on asymmetric strategies and irregular operations, which include both the adoption of new capabilities as well as use of otherwise conventional means in ways that exploit asymmetric advantages. One obvious avenue embraced by the North was the establishment of a nuclear and ballistic missile program. Other, less discussed paths include North Korea's development of dedicated Special Operations Forces and its early interest in electronic warfare. Pyongyang's pursuit of cyber capabilities can likewise be explained in this context.

Cyberwarfare: Operation Orchard and Decision Styles

There are two possible ways in which the Korean People's Army (KPA) might incorporate cyber capabilities into its military strategy and doctrine.

First, it may try to disrupt or degrade enemy C4ISR, in an effort to "level the playing field" vis-à-vis the U.S.-ROK alliance. At this time, the KPA simply cannot match the U.S. and ROK in conventional military terms. Yet it must try not to fall too far behind an enemy equipped with state-of-the-art precision weapons and C4ISR capabilities. The next best option for North Korea is thus to disrupt or degrade either enemy systems/networks or the information passing through them. Thus, a leaked 2005 KPA publication, entitled "Electronic Warfare Reference Guide," states: "If one disrupts the GPS systems of US's precision-strike weapons, one can degrade its precision and lead it to strike another area," and "We can defend our troops and assets against electronically

Jenny Jun, *a Junior Fellow at the American Foreign Policy Council, is a Ph.D. student at Columbia University and a co-author of the CSIS report* North Korea's Cyber Operations: Strategy and Responses.

guided weapons if one knows how it works and develops appropriate defensive measures."[2] There is reason to believe that this sort of strategic thinking extends to cyber warfare as well.

Such efforts to disrupt and degrade enemy C4ISR have the added benefit of boosting the effectiveness of one's own (otherwise inferior) weapons systems. For example, during Operation Orchard, a 2007 Israeli operation to strike Syria's Al-Khibar nuclear reactor, the Israelis used a combination of cyber and electronic warfare to not only disable Syrian air defense radars but also to manipulate their screens, so that the Israeli fighter jets, which were not stealth aircraft, were able to enter Syrian airspace unimpeded. While not all air defense networks can be compromised as easily, such an operation is certainly a more cost-effective alternative than investing in stealth capabilities.

Along the same lines, if North Korea is able to compromise portions of South Korea's air defense or missile defense systems, it may be able to make greater use of its otherwise severely outdated air force, artillery, and missiles. In fact, North Korea has already demonstrated that it is capable of conducting a combined operation incorporating electronic warfare elements. During the infamous shelling of Yeonpyong Island in November 2010, North Korea jammed ROK's AN/TPQ-37 radar before opening fire. As a result, the ROK military had to rely on preexisting coordinates when returning fire, resulting in 35 out of 50 rounds falling into the sea. This provided the North Korean side with enough time to fire a second round of attacks. And this occurred despite the ROK military's 2005 assessment that North Korea's EW capabilities were not a threat, because the South Korean side already possessed various countermeasures and encryptions. Thus, degrading and disrupting enemy C4ISR using cyber means can provide North Korea with immense asymmetric advantages by rendering enemy precision weapons less effective and boosting the effectiveness of its own conventional forces.

Second, North Korea may try to use cyber operations as part of a broader attempt to extend adversary decision cycles in the context of Blitzkrieg-style maneuver warfare. Though unrealistic today, historically North Korea has wanted to fight a blitzkrieg-style war supported by special operations forces and irregular operations.[3] This kind of warfighting relies heavily on maneuver warfare, where mechanized forces quickly penetrate enemy defenses, race to the rear, then isolate and destroy defending forces while irregular and light infantry infiltrate and disrupt enemy rear areas. By having a faster decision cycle than the adversary, fast-moving mechanized forces can maneuver more quickly than the defense is able to confront and destroy the threat.

Before the Information Age, North Korea's military strategy tried to slow down decision cycles through rear operations by special operations forces and light infantry units. Today, this can be done more effectively and rapidly by using a combination of cyber and EW capabilities, as long as North Korea has conducted significant operational preparation of the environment beforehand. If the KPA still engages in strategic planning for potential war on the Korean peninsula, as is widely believed, then it has most assuredly moved in this direction.

Thus, especially because the U.S.-ROK alliance as well as broader American operational capabilities in the Asia-Pacific rely heavily on various systems and networks for C4ISR, the DPRK is likely to focus on these information flows in a warfighting scenario. This focus, in turn, could have significant strategic consequences for U.S. capabilities on the peninsula and beyond.

Cyber Operations in Peacetime: Disruption and Coercion

Below the threshold of war, North Korea has been engaging in almost a decade of malicious peacetime cyber operations ranging from the attempted blackmail of a civilian nuclear reactor to the hacking of cryptocurrency exchanges. Setting aside for the moment Pyongyang's efforts to generate foreign cash through cyber crime, these politically motivated activities can be broadly characterized as either disruptive or coercive.

First, North Korea's disruptive cyber attacks are rooted in an old tradition of launching limited provocations aimed at undermining and destabilizing South Korean society or the U.S.-ROK alliance without risking general war. Since 2009, North Korea's cyber attacks have evolved from rudimentary DDoS attacks and website defacements to more sophisticated operations (such as the 2013 coordinated wiper malware campaigns on South Korean

banks and news media organizations) which demonstrate a significant investment of resources and organizational capacity. It is important to note that these cyber attacks are planned and executed by the Reconnaissance General Bureau (RGB), an agency formed around 2009 in an effort to consolidate a wide range of the regime's intelligence, commando, sabotage operations. Units that have since been incorporated into the RGB are responsible for assassination attempts such as the 1968 Blue House raid and the 1983 Rangoon bombing, and more recent incidents such as the 2010 sinking of the ROK navy corvette Cheonan and the 2015 DMZ mine crisis. The fact that North Korea's disruptive cyber operations are spearheaded by an organization that has a track record of a wide range of covert operations indicate that, as seen from Pyongyng, North Korea's cyber capabilities represent a tool that serves the regime's broad strategic interests.

Second, North Korea may in the future attempt to make greater use of cyber means for coercing its adversaries, especially for issuing compellent threats. When considering how it might get the U.S. or ROK to do what they otherwise would not want to, North Korea's options have been limited thus far. Thus, the North's positioning of artillery vis-à-vis Seoul or its missile and nuclear program may be useful for deterring invasion, but it is less so for prompting South Korea or the United States to take a particular action.

With cyber means, however, North Korea is exploring new ways to compel the U.S. and ROK to meet its demands. So far, these attempts – including the 2014 Sony Pictures hack and the blackmail of a South Korean civilian nuclear reactor in the same year – have yielded only mixed results. Some scholars have argued that it is generally difficult to compel an adversary using cyber means, due to the fact that many cyber operations rely on secrecy and surprise.[4] However, such assessments may need to be qualified in the future, as cyber capabilities evolve. Already, there are signs that tactics such as ransomware and doxing have been harnessed by North Korea for the purposes of extortion, and such capabilities could be used in the future for political ends –against private actors, NGOs or even foreign governments.

Policy Considerations

A review of trends in North Korea's cyber operations indicates that the acquisition of cyber capabilities is a natural extension of its national strategy. The DPRK will continue to train and innovate its cyber forces, and seek new ways to achieve its goals using cyber means. In this context, the following policy questions can be asked:

- Is the U.S.-ROK alliance prepared to operate under a significantly degraded C4ISR environment on and beyond the Korean peninsula during a crisis?
- Given North Korea's attempts to gain/maintain access to key critical infrastructures, is the U.S. government working with relevant agency and private sector stakeholders to streamline incident response procedures and enhance resiliency?
- Can we improve cyber threat intelligence sharing between government and the private sector, among different industries, and with allies in the region?
- Given that North Korea is increasingly relying on cyber crime to fund further malicious activity, are there measures by which we can curb the profits from such operations?

Policymakers should keep in mind that while North Korea may arguably be less technically sophisticated in cyberspace than the U.S., Russia, or China, there are also less options to deter North Korea, both in and out of cyberspace. This means that Pyongyang may be particularly emboldened by the perception that its targets lack credible means to counter its cyber attacks. Cyber capabilities offer North Korea a sharp asymmetric advantage, and its threat to the U.S. and American interests abroad should not be taken lightly.

Finally, policymakers now involved in negotiations with North Korea regarding its nuclear and ballistic missile program should consider the associated cyber dimensions of their efforts. A denuclearization agreement is likely to change escalation dynamics in the event of a cyber attack, and the room for misunderstanding and miscalculation may increase without some mutual agreement about expected behavior in this domain. Also, if North Korea intends to use cyber capabilities for coercive purposes, failure to incorporate such a discussion into the agenda may leave a critical loophole even if progress on the nuclear and missile fronts is made. The current negotiations are, first and foremost, about North Korea's nuclear

and missile programs. Perhaps over time, however, the momentum and trust built from these talks could create an opportunity to discuss restraint in the cyber domain as well.

Endnotes

1. An earlier version of this article has been published under the name "Lessons from North Korea's Cuber Operations" in a paper serious on hybrid warfare by the Clingendael Institute.
2. The leaked document was cited in Nak-gyu Yang, "Electronic Warfare Tactics as Described in North Korea's Field Manual," Asia Economy, April 18, 2011, http://m.asiae.co.kr/view.htm?no=2011030709432824411#cb.
3. For more information on North Korea's military strategy, refer to Minnich, James M., The North Korean People's Army: Origins and Current Tactics (Annapolis, MD: Naval Institutie Press, 2005) and Bermudez Jr., Josoph S. The Armed Forces of North Korea. London: I. B. Tauris, 2001.
4. Lindsay, Jon, and Erik Gartzke. "Coercion through Cyberspace: The Stability-Instability Paradox Revisited." in Coercion: The Power to Hurt in International Politics, edited by Kelly M. Greenhill and Peter JP Krause. Oxford University Press, 2018.

DEFENSE TECHNOLOGY PROGRAM BRIEF

About The Defense Technology Program

A revolution is taking place in the nature of warfare. The proliferation of ballistic missiles and weapons of mass destruction has given rogue states and terrorist groups unprecedented access to potentially devastating capabilities, while space and cyberspace have emerged as distinct new arenas of strategic competition. The American Foreign Policy Council's (AFPC) work in these areas is aimed at helping U.S. offcials understand and respond to this new, and increasingly complex, threat environment.

For more information about the program, please contact Richard Harrison, Vice President of Operations and Director of Defense Technology Programs at Harrison@afpc.org.

About AFPC

For close to four decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies. AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.

AFPC Mission Statement

The American Foreign Policy Council seeks to advance the security and prosperity of the United States by:

- providing primary source information, as well as policy options, to persons and organizations who make or influence the national security and foreign policies of the United States;
- arranging meetings and facilitating dialogue between American Statesmen and their counterparts in other countries; and
- fostering the acceptance and development of representative institutions and free market economies throughout the world in a manner consistent with the Constitution, the national interest, and the values of the United States.

CONTACT AFPC

509 C Street NE
Washington, D.C. 20002
Telephone: 202.543.1006
Fax: 202.543.1007
www.afpc.org