CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Executive Summary

NORTH KOREA'S CYBER OPERATIONS: STRATEGY AND RESPONSES

Center for Strategic and International Studies
Office of the Korea Chair

PROJECT AUTHORS
Jenny Jun, Scott LaFoy, Ethan Sohn

SENIOR ADVISERS
Dr. James A. Lewis
Director & Senior Fellow,
Strategic Technologies Program, CSIS

Dr. Victor D. Cha
Senior Advisor and Korea Chair, CSIS

EXECUTIVE SUMMARY

North Korea is emerging as a significant actor in cyberspace with both its military and clandestine organizations gaining the ability to conduct cyber operations. However, there is no comprehensive standard literature about North Korea's cyber capabilities that takes an integrated view of the topic. Existing research is fragmented in pockets of strategic, technical, and policy pieces, though no individual study reaches far enough to create a standard reference document about North Korea's cyber capabilities. This report aims to fill this void, integrating Korean and English language information sources, existing work in each respective field, and creating a foundation for future deeper research.

Cyber attacks in South Korea and the United States have recently been associated with North Korea. The U.S. and ROK governments attribute recent incidents, including the 2014 attack against Sony Pictures Entertainment and the March 2013 attacks against South Korean banks and media agencies, respectively, to North Korea. These attacks have shown that the country is capable of conducting damaging and disruptive cyber attacks during peacetime. North Korea seems heavily invested in growing and developing its cyber capabilities for both political and military purposes.

These attacks raise important policy questions. Existing research does not comprehensively answer questions about why North Korea conducted these and similar attacks, how the government has been able to launch these attacks, and what this implies for U.S. strategy and policy. This report attempts to answer these questions with a top-down view of North Korea's motivations, government, and military organizational structure. It also provides analysis on how these factors affect North Korean behavior in cyberspace. We hope that this will give decision-makers a better understanding of North Korean patterns of behavior as well as allow them to anticipate and respond to future incidents.

THE STRATEGIC CONTEXT OF DPRK'S CYBER OPERATIONS

This section builds a contextual foundation upon which current and future North Korean cyber operations can be better understood. Historically, North Korea has relied on asymmetric and irregular means to sidestep the conventional military deadlock on the peninsula while also preparing these means for use should a war break out. Cyber capabilities provide another means of exploiting U.S. and ROK vulnerabilities at relatively low-intensity while minimizing risk of retaliation or escalation. In this context, cyber capabilities are logical extensions of both North Korea's peacetime and wartime unconventional operations.

1. **North Korea's Strategic Context**: North Korean strategy emphasizes asymmetric and irregular operations in both peacetime and wartime to counter the conventional military strength of the U.S. and ROK. North Korea's national strategy has always been defined by the fact that the Korean Peninsula is entrenched in a conventional military deadlock. As a result, North Korea's modern peacetime strategy is to launch low-intensity unconventional operations to disrupt the peaceful status quo without escalating the situation into something the DPRK cannot control or win. However, should a war ever actually break out, the Korean People's Army (KPA)'s wartime strategy is to launch extensive irregular operations that exploit U.S. and ROK vulnerabilities and support its regular military operations.

2. **Cyber Capabilities and Asymmetric Strategy**: North Korea sees cyber operations as a relatively low-cost and low-risk means of targeting the vulnerabilities of a state that relies heavily on cyberspace for national and military activity. Disruptive or destructive cyber attacks allow for direct power projection against a distant adversary without physical infiltration or attack. Cyber capabilities are also an effective means to severely disrupt or neutralize the benefits of having a networked military. Issues of attribution and the lack of firmly established norms make it hard for the defender to communicate red lines and threats.

3. **North Korea's Cyber Strategy**: Cyber operations should be thought of as an extension of North Korea's broader national strategy. During peacetime, cyber capabilities allow the DPRK to upset the status quo with little risk of retaliation or immediate operational risk. During wartime, the DPRK would target U.S. and ROK C4ISR in support of the DPRK's 'Quick War, Quick End' strategy. North Korean cyber doctrine, if one exists, may be premised on the idea that an extensively networked military is vulnerable to cyber capabilities.

THE ORGANIZATION OF DPRK'S CYBER OPERATIONS

North Korea's cyber operations are not ad-hoc, isolated incidents. They are the result of deliberate and organized efforts under the direction of preexisting organizations with established goals and missions that directly support the country's national strategy. Knowing which North Korean organizations plan and execute cyber operations is important because North Korea does not publish its own cyber strategy or doctrine. Examining an organization's historic goals and missions as well as analyzing their known patterns of behavior are the next best option for predicting how North Korea will operationalize cyber capabilities. This section will provide a top-down perspective on North Korea's cyber operations and establish that the organizations that conduct cyber operations strongly influence the purpose of the operations. The Reconnaissance General Bureau and the General Staff Department of the KPA generally control most of North Korea's known cyber capabilities. These two organizations are responsible for peacetime provocations and wartime disruptive operations, respectively.

1. **The Reconnaissance General Bureau (RGB)**: The RGB is the primary intelligence and clandestine operations organ known within the North Korean government and is historically associated with peacetime commando raids, infiltrations, disruptions, and other clandestine operations, including the 2014 Sony Pictures Entertainment attack. The RGB controls the bulk of known DPRK cyber capabilities, mainly under Bureau 121 or its potential successor, the Cyber Warfare Guidance Bureau. There may be a recent or ongoing reorganization within the RGB that promoted Bureau 121 to a higher rank or even established it as the centralized entity for cyber operations. RGB cyber capabilities are likely to be in direct support of the RGB's aforementioned missions. In peacetime, it is also likely to be the more important or active of the two main organizations with cyber capabilities in the DPRK.

2. **The General Staff Department (GSD)**: The General Staff Department of the KPA oversees military operations and units, including the DPRK's growing conventional military cyber capabilities. It is tasked with operational planning and ensuring the readiness of the KPA should war break out on the Korean Peninsula. It is not currently associated with direct cyber provocations in the same way that the RGB is, but its cyber units may be tasked with preparing disruptive attacks and cyber operations in support of conventional military operations. North Korea's emphasis on combined arms and joint operations suggests that cyber units will be incorporated as elements within larger conventional military formations.

3. **North Korea's Tech Base**: The DPRK maintains an information technology base that can serve as general research and development foundation for computer technology and programming. The existence of a software and computer industry means the DPRK's technical industries are not as primitive as many think.

FUTURE THREAT TRENDS FROM DPRK'S CYBER OPERATIONS

1. **Future Threats**: Left unchecked and barring any unpredictable power shift, North Korea is likely to continue to place strategic value in its cyber capabilities. Future North Korean cyber attacks are likely to fall along a spectrum, with one end being continued low intensity attacks and the other end characterized by high intensity attacks from an emboldened North Korea. Concurrently, the DPRK will likely deepen the integration of its cyber elements into its conventional military forces. Although North Korea's history of low-intensity provocations makes it more likely that they will continue on the lower end of the spectrum, the U.S. and ROK should remain wary of the latter possibilities and plan and prepare accordingly.

    a. At one end of the spectrum is a continuation of low-intensity disruptive cyber attacks, possibly with increased frequency. This may not result in any extensive damage or casualties, but an increase in the frequency of disruptions may result in a general erosion of confidence in key commercial sectors.

    b. At the other end is an emboldened North Korea moving toward higher intensity attacks, possibly crossing a "use of force" threshold. North Korea may be emboldened, either from past success or a miscalculation of its capabilities and adversary resolve, and elevate the intensity of its cyber attacks. This could lead to crossing of the "use of force" threshold and an escalation of conflict with the U.S. and ROK.

    c. Cyber capabilities are likely to be increasingly integrated with other operational elements of the DPRK's military. North Korea has a well-established tradition of irregular operations, provocative behavior, and the integration of these operations with conventional military means. Policymakers should expect a potential combination of cyber operations with diplomatic offensives, psychological operations, military exercises, missile tests, or other provocative behaviors.

    d. Contingency Planning for a range of scenarios is necessary. Although the majority of North Korea's provocations are relatively low intensity, there have also been occasional spikes in intensity, such as the shelling of Yeonpyeong Island and sinking of the Cheonan. These examples mean that contingency plans for high intensity cyber attacks or a conventional provocation aided by cyber capabilities must also be formulated to mitigate the damage that will likely emerge from an unpredicted escalation.

RECOMMENDATIONS FOR POLICY

1. **Policy Objectives**:
   There are four main policy objectives for managing the emerging North Korean threat in cyberspace, none of which should be pursued exclusively. The following section makes more specific policy recommendations for the U.S. and the U.S.-ROK alliance. The recommendations are made with these general objectives in mind.

   a. Prepare a graduated series of direct responses targeting North Korea's cyber organizations.

   b. Curb North Korea's operational freedom in cyberspace.

   c. Identify and leverage North Korea's vulnerabilities to maintain strategic balance.

   d. Adopt damage mitigation and resiliency measures to ensure that critical systems and networks maintain operational continuity despite suffering an attack.

2. **Recommendations for the United States**:

   a. **Consider developing a declared policy on the U.S. range of countermeasures for low-intensity cyber attacks qualifying as internationally wrongful acts.** In response to the cyber attack against Sony in November 2014, policymakers did not have an established menu of proportional response options, which hindered the ability of the U.S. to respond quickly and send a clear signal. Establishing a declared policy allows for more timely responses and may have, deterrent effects. The positives outweigh the negatives of potentially binding one's hands, so long as the government is willing and able to execute its own policy. Measures such as Executive Order 13694 announced on April 1, 2015 have prepared the groundwork for such a policy, but further explicit responses should be set so that U.S. entities are prepared to respond quickly in future crises. As these response measures would address low-intensity cyber attacks, policy should distinguish countermeasures, such as sanctions, from peacetime reprisals, which would be applicable for attacks that cross the threshold of "use of force" or "armed attack."

   b. **Further implement Executive Order 13687 and 13694 against specific DPRK individuals and/or entities that have engaged in cyber attacks that pose a threat to national security.** The U.S. now has a basis for sanctioning individuals and entities that engage in or materially support disruptive or destructive cyber operations. The U.S. should utilize Executive Order 13687 and Executive Order 13694 to further identify and implement sanctions against specific North Korean individuals and entities. This would continue to build a basis for limiting their operational freedom.

   c. **Strengthen the international legal and normative base in order to curb North Korea's current operational freedom with a wider range of policy options.** Currently, the international legal and normative basis on state responsibility in cyberspace is weak. Although the UN Group of Government Experts (GGE) agreed in 2013 and 2015 that states should seek to ensure that their territory is not knowingly being used for international wrongful acts using cyber capabilities, this is far from being practically applied by states. Greater acceptance of this norm, however, could help curb any overseas North Korean activity in support of cyber operations by encouraging states to refrain from knowingly hosting them, and taking appropriate measures once notified of the fact.

d. **International cooperation is imperative for implementation.** Unilateral action is less effective in this case than deep and broad international cooperation, unless the objective is to purely send a message. The U.S. will need strong working relationships with other states for both greater enforcement of U.S. sanctions against North Korean individuals and entities and to impose limitations on North Korea's operational freedom. In order to achieve this, the U.S. should work with existing allies and partners with an existing common understanding regarding international norms applicable to cyberspace and work jointly to promote their greater adoption at the regional and global level.

3. Recommendations for the U.S.-ROK Alliance:

a. **The U.S. and ROK should develop contingency plans and a menu of corresponding response options for a range of scenarios affected by North Korea's cyber operations.** These scenarios should not be necessarily limited exclusively to cyber operations, as North Korea may launch joint provocations in the future. A range of options from declaratory statements to operations aimed at degrading North Korean assets should be assessed. Wargaming and continued preparation for future crises will continue to be vital. The scope of contingencies considered should go beyond the Korean Peninsula and should incorporate the impact on other regional U.S. allies such as Japan, and other important strategic assets in the region such as early warning networks. The Cyber Cooperation Working Group, as the current key bilateral cyber defense dialogue, remains a good mechanism for further concrete discussions on this topic.

b. **Consider exploiting North Korea's vulnerability to outside information.** One realistic response option to North Korea's cyber attacks may be to leverage the regime's obsession with tight control on information within the country. This could be considered one of North Korea's largest asymmetric vulnerabilities. Targeting this may be an efficient means of directly influencing North Korean behavior. The continuous introduction of unwanted information into North Korea would create pressure that could be utilized, possibly in conjunction with sanctions or countermeasures, to compel North Korea to end an illicit cyber operation. The recent crisis on the Korean Peninsula in August 2015 over South Korean loudspeakers at the DMZ has shown that the North Korean regime is highly vulnerable to this measure.

c. **Review the possibility that North Korea's growing cyber power may affect the current strategic balance on the Korean Peninsula.** The alliance should discuss in a subsequent high-level strategic dialogue whether and how North Korea's cyber power may affect the alliance's peacetime and wartime strategic balance. In the case that North Korea's cyber capabilities become increasingly integrated as a supporting element into its conventional military operational planning, the alliance needs to consider how such a situation might augment North Korea's existing military capabilities and how alliance assets might be adversely affected. Examples of possibly affected functions are military command and control, the alliance's air defense networks, and any future missile defense arrangements.

d. **Vulnerabilities in interoperability arising from the current hub-and-spokes alliance structure should be actively mitigated.** If North Korea's cyber capabilities are increasingly integrated with its conventional military elements, the alliance needs to mitigate its inherent vulnerabilities. Alliance networks, military units, and early warning sys-

tems must be interoperable and hardened against disruptive cyber operations. South Korea and Japan, even if not directly allied, must cooperate with each other and the U.S. to track and protect network-dependent assets, such as early warning systems, against cyber attacks. Cyber units in each country must be capable of efficiently communicating and working together to manage threats that stretch beyond just the Korean Peninsula.

e. **Encourage greater information sharing arrangements beyond intelligence and government agencies.** Information sharing is critical in helping each defender gain a more comprehensive picture of the threat and to reduce vulnerabilities accordingly. A more comprehensive knowledge base about North Korea's tactics, techniques, and procedures (TTPs), allows defenders to detect malicious activity at the initial exploitation phase and gives the defender enough time to stop an attack. It also has an added benefit of forcing North Korea to change their TTPs more frequently, thus increasing both the expense and risk of each operation. Beyond intelligence sharing between just intelligence and government agencies, arrangements for sharing more incident response data between CERT/CSIRTs are a valuable option. Additionally, finding mechanisms that incentivize private sector participation is important. Information sharing mechanisms should also not necessarily be limited to the alliance but seek to incorporate a wider cooperative network.

f. **The U.S. and ROK should continue to engage in regional confidence building measures (CBMs) and capacity building efforts to create more common ground on cyber issues in the Asia-Pacific, especially with China.** Both the U.S. and ROK have been engaged in efforts to implement greater CBMs and capacity building in the Asia-Pacific. The ROK has hosted the Seoul Global Conference on Cyberspace in

2013 and has been active on this issue in regional forums such as the ASEAN Regional Forum (ARF) and Asia-Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group (TEL). CBMs provide a basis for increasing transparency and trust, and serve as a starting point for further functional cooperation despite other disagreements. They help buttress the efforts such as the Korea-Japan-China trilateral consultations. Capacity building is closely related to CBMs in that greater domestic technical, legal, and bureaucratic capacity to respond to cyber incidents enables further functional international cooperation. The ROK government's current Northeast Asia Peace and Cooperation Initiative (NAPCI), which seeks to increase cooperation in the region by focusing on issue-specific dialogues, could further focus on cyber issues by identifying and implementing CBMs and capacity building efforts.

g. **Leverage existing bilateral coordination on international norms and standards as a platform for their further adoption regionally and globally.** Over the past few years the U.S. and ROK have been involved in multi-agency bilateral Cyber Policy Consultations that resulted in a common understanding regarding international norms regarding cyberspace. North Korea's cyber threat has provided a concrete situation around which norms could be further refined, and these efforts should not be thought of as just limited to the Korean Peninsula. The U.S. and ROK should further coordinate on international cyber policy in regional and global forums in order to place further weight on such norms.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 RHODE ISLAND AVENUE NW WASHINGTON, DC 20036

202.887.0200 | WWW.CSIS.ORG