The Organization of Cyber Operations in North Korea

By Jenny Jun, Scott LaFoy, and Ethan Sohn
December 18, 2014

Jenny Jun, Scott LaFoy, and Ethan Sohn *are researchers with the CSIS Korea Chair for the NK Cyber Strategy Project, a year-long research project on the strategic implications of North Korea's cyber operations capabilities. The report will be released in the spring of 2015.*

Sony Pictures Entertainment (SPE) announced last night a cancellation of the upcoming release of "The Interview." U.S. government officials also informally acknowledged that North Korea played a central role in the cyber attacks against Sony. The act against Sony is the first of its kind by North Korea, in terms of both the target and the sophistication of the hack. On the history of past North Korean cyber attacks and their capabilities, see "What Do We Know about Past North Korean Cyber Attacks and Their Capabilities," *http://csis.org/publication/what-do-we-know-about-past-north-korean-cyber-attacks-and-their-capabilities.*

This analysis by our research team looks at how cyber operations in North Korea are organized. In this piece, they focus on where North Korea's cyber operations fit within the larger organizational structure of the government, because it provides insight into their mission, strategy, and history. Aside from the technical analysis of their capabilities, studying the organizational structure can provide insights into what North Korea's cyber strategy might be and what steps the nation has taken to operationalize it.

DPRK cyber operations are generally overseen by two entities: the Reconnaissance General Bureau (RGB) and broadly under the Korean People's Army General Staff Department (GSD). According to South Korean government analysis, there are around 5,900 "cyber warriors" currently in North Korea. Different sources peg this number slightly higher or slightly lower, and it is unclear whether or not this number refers exclusively to operational cyber units or if it includes staff and support members as well.

The RGB was formed in 2009 as an amalgamation of various intelligence and special operations units that previously operated across the North Korean government. Units previously tasked or credited with political warfare, foreign intelligence, propaganda, subversion, kidnapping, special operations, and assassinations have been combined into one organization. Notable examples associated with the RGB and the offices that were combined to create it are provocations short of armed conflict, such as the sinking of the South Korean *Cheonan* naval vessel in 2010, and more historically, the Rangoon bombings in 1983 and the Blue House Raid in 1968. While there is some debate in the open-source analyst community about what organization the RGB is directly subordinate to, it seems that regardless of its de jure status, the RGB de facto answers directly to the National Defense Commission and Kim Jong-un in his role as supreme commander of the Korean People's Army.

This organization is now credited with significant operational cyber capabilities and missions that are, effectively, another means of achieving the objectives of previous provocations. The cyber units most frequently linked to RGB are "Unit 121" (121소 or 121국) and "Lab 110" (110호 연구소 or 110연구소). The English translation as "Unit" or "Lab" may not accurately reflect their bureaucratic placement. Out of the four bureaus identified under RGB (1st Operations Bureau, 2nd Reconnaissance Bureau, 3rd Foreign Intelligence Bureau, and 6th Technical Bureau), it is likely that one of the two units would be subordinate to or synonymous with the 6th Technical Bureau. It is also likely that the 3rd Foreign Intelligence Bureau has a cyber espionage component as well. Unit 121 has been typically linked to the DarkSeoul attack, and Lab 110, among others, has recently been accused of using a front information technology (IT) company in Shenyang named Chosun Baeksul Trading Company to sell malicious software to South Korean customers. The exact operational relationship between Unit 121 and Lab 110 is not known. There is a possibility that offensive cyber operations could be easily combined with human intelligence (HUMINT) or covert operations capability retained in the 1st and 2nd Bureau.

The General Staff Department (GSD) of the Korean People's Army (KPA) is broadly comparable to the U.S. Joint Chiefs of Staff and oversees the operational aspects of the entire KPA. As such, it has authority over numerous operational cyber units, including units tasked with political subversion, cyber warfare, and operations such as network defense. North Korea does not seem to have yet organized these units into an overarching Cyber Command. Specifically, the GSD's Operations Bureau has been attributed with conducting cyber operations, but information about the nature of these operations, as well as the subordinate unit conducting them, has been sparse. Other important subordinate units include the Automation Department's Offices 31, 32, and 56. Unit 204 is also commonly mentioned as a cyber component of GSD, but its missions seem to be more closely aligned with propaganda/psychological warfare using cyberspace as a medium.

Analysts including Joseph Bermudez discuss North Korea's Signals Intelligence (SIGINT) and Electronic Warfare Units as the logical units from which the cyber warfare unit (called "Electronic Information Warfare" in North Korea) evolved. This could mean that the GSD's military-oriented cyber capabilities may have significant disruptive focus, in a similar vein to the RGB, in addition to some network defense capabilities.

The GSD's position in government, much like the RGB, is debated, with some analysts placing it below the Ministry of People's Armed Forces and others putting it directly beneath the National Defense Commission. Either way, it likely is directly overseen by Kim Jong-un in his role as supreme commander of the KPA. That the bulk of North Korea's offensive cyber operations are housed in RGB, a black operations organization, and that its GSD missions stem from SIGINT and electronic warfare, may have strong implications for what they tend to target, what type of attack they rely on, and what mission they hope to achieve via cyber means.

The Korea Chair Platform is published by the Office of the Korea Chair (http://www.csis.org/ program/korea-chair**) at the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy**

positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

The *Korea Chair Platform* is made possible by the generous support of Samsung Electronics America. The views expressed in the *Platform* do not necessarily reflect those of Samsung Electronics America or of CSIS. The Office of the Korea Chair invites essays for consideration for the *Platform*. For inquiries, please email KoreaChair@CSIS.org.

1616 RHODE ISLAND AVENUE NW
WASHINGTON, DC 20036
TEL. (202) 887.0200
FAX (202) 775.3199