North Korea, Cyberdefense and Cybersecurity

Daniel Ventre, Chair-holder of the Chair of Cybersecurity and Cyberdefense

March 2016. Article III-24
Translated from French

On March 6th of 2016, North Korea threatened the United States and South Korea with blind nuclear attacks if a large joint military exercise between the two countries (scheduled for March 7th) was carried out. In the last few months, with the announcement of nuclear tests and missile trials, there has been increased international tension with Pyongyang, which has resulted in, among many things, a UN resolution and measures passed by the U.S. House of Representatives. This new phase of tension is a continuation of decades of unfinished conflict between the two Koreas. North Korea's mounting military power has stirred feelings of insecurity in neighboring countries, and prompted them to develop their capabilities in terms of security and defense. However, the threat is not only regional. With today's long-range missiles, North Korea could even attack the U.S., as it has confirmed. In terms of cyberattacks, North Korea's scope of targets are potentially global. In this context of elevated tensions, cyberspace has become, over the years, a space in which confrontation extends. We must ask ourselves, what role cyberspace plays in on-going conflict. Does it intensify the situation or, on the contrary, does it diffuse it?

1 - The Cyber News of North Korea

In recent years, North Korea has been accused of carrying out cyberattacks on multiple occasions. While cyber incidents between the two Koreas are the source of great conflict, some attacks also involve Japan, the U.S. and several other nations. Below is a succinct table with a brief overview of cyberattacks that involve North Korea both as a target and as the responsible party.

South Korean accusations against North Korea	
	In 2003, paralysis of South Korean media business networks (broadcasting) and of banks
	In 2014, an attack against Korea Hydro & Nuclear Power Co. attributed to North Korea
	In late January 2016, the government in Seoul confirmed that South Korea was

	attacked by North Korea, however, they refused to offer precise details about what targets were effected and the extent of the impact.
	The South Korean intelligence services accuse Pyongyang of spying on the cellphones of its ministers (taking historic call information, texts, and intercepting voice calls) in February and March of 2016 (Mu-Huyn, 2016).[1]
North Korean accusations against South Korea	
	North Korea accuses South Korea and the U.S. of continuous and intensive cyberattacks.[2]
U.S. accusations against North Korea	
	On December 19th 2014, the U.S. attributed the attacks against Sony pictures in November of the same year to North Korea. On December 20th, North Korea requested a joint investigation into the events with the U.S. A few days later the U.S. published a list of North Korean organizations and individuals thought to be responsible.
	In July of 2015, the New York stock exchange had an interruption in services. North Korea claimed responsibility for the cyberattack that resulted in the malfunction.

Table: Some cyberattacks involving North Korea

2 - Discourse on the North Korean Cyberthreat

In December of 2015, CSIS (the Center for Strategic and International Studies) published a report on North Korean cyberoperations (Jun, LaFoy, Sohn, 2015).[3] The report examines the strategic context in which North Korea opts for asymmetric confrontation and irregular operations to confront the conventional power of the United States and South Korea. This corresponds to the cyberstrategy of North Korea, which regards cyber-capabilities as instruments of asymmetric conflict, allowing it in peacetime to maintain a status quo with a low risk of retaliation, and in peacetime to reach C4ISR enemy systems.

The report describes the organization of the actors in this cyberstrategy including the central office of intelligence; the General Staff department, and an industrial technology base in both software and hardware. The report makes a number of recommendations for U.S. policy such as creating scaled responses for those responsible, restricting freedom of North Korean action in cyberspace, identifying vulnerabilities in North Korean cyberspace, adapting the level of response to the severity of an incident, including the development of a national legal framework, and promoting the development of the international legal system. The report also

[1] MU-HYUN C. (2016), "South Korea Claims North hacked government official's smartphones", ZDNet, 8 February, http://www.zdnet.com/article/south-korea-claims-north-hacked-government-officials-smartphones/?tag=nl.e305&s_cid=e305&ttag=e305&ftag=TRE21e7bbc

[2] AFP (2013) "North Korea Cyber Attacks: Pyongyang accuses South, U.S. of 'persistent and intensive' cyberattack," 15 March, http://www.huffingtonpost.com/2013/03/15/north-korea-cyber- attacks_n_2881767.html

[3] JUN J., LAFOY S., SOHN E. (2015), "North Korea's Cyber Operations. Strategy and Responses," *Center for Strategic and International Studies*, Washington D.C., December, 110 pages, https://csis.org/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf

talks about rapprochement with South Korea that would include information sharing, dialogue, and fostering of trust and expansion of cooperation within the region.

Several topics are focused on in the discourse surrounding North Korean cybercapabilities, both in the press and in expert reports, as well as in academic studies. The North Korean cyberthreat is manifested in intrusions and attempted intrusions of corporate and foreign government networks and servers. The North Korean cyberforces have some 5,000 to 6,000 military hackers. According to Kim Heung-kwang and Jang Sae-yul, two North Korean defectors, the idea of using computers to attack their enemies and the building of their cyberoffensive capabilities began in the 1990s (at the same time as the rest of the world).[4] After years of training, notably training that took place abroad, the North Korean army opened its Bureau 121 (a cyberwarfare unit) in 1998.

According to the White Book of the South Korean Minister of Defense, the North Korean army have between 5,000 and 6,000 agents in their cyberwarefare units. According to a report from NKIS, a Seoul-based think tank, these units have been established or have been under construction for 16 years. The history of these North Korean cyberwarfare military units is a bit vague, with one unit's origin dating back to the 1990s and another to the 2000s. However, there is consensus that North Korean cyberdefense capabilities are not in their infancy.

The North Korean internet did not exist	The North Korean network is in such a basic state at this time that it is an exaggeration to call it "the internet"
North Korea cannot be victims of cyber attacks	North Korea is safe from cyberattacks as it basically does not have a real internet (Peterson, 2015)[5]
North Korea is accused of cyberattacks against South Korea and Japan	The North Korean network remains rudimentary though it provides enough capacity to carry out cyberattacks. North Korea is able to attack while not being vulnerable themselves because they have little dependency on cyberspace.
North Korea denies charges against them	States do no recognized the attacks for which they are accused. North Korea is no exception to this idea.[6]
North Korea makes accusations	North Korea accuses the United States of cyberattacks against their internet network; on December 22nd of 2014 there are disturbances in the North Korean network.
North Korea is suspicious of and against the introduction of any foreign telecommunication technologies, which are beyond their capacity to control	North Korea wants to curb the illegal and uncontrolled spread of Chinese mobile phones in the country.[7] The authorities monitor citizens and the use of such technologies is considered a crime. Contact abroad is also considered a crime.

[4] Cited in: SANGER D.E., FACKLER M. (2015), "NSA breached north Korean networks before Sony attack, Officials say," The New York Times, 18 January, http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0

[5] PETERSON A. (2015), "A U.S. cyberattack on North Korea failed because North Korea has basically no Internet," *The Washington Post*, 1 June, https://www.washingtonpost.com/news/the-switch/wp/2015/

[6] http://www.huffingtonpost.com/huff-wires/20130412/as-koreas-cyberattack/

[7] http://www.lefigaro.fr/international/2016/03/09/01003-20160309ARTFIG00385-kim-jong-un-en-croisade-contre-les-telephones-portables-chinois.php#xtor=AL-201

North Korea has military cyber offensive and defensive capabilities	The actual level of their abilities is difficult to assess, however, that is the same for all countries with these capacities
North Korean cyberdefense capabilities are not a recent development	North Korea develops its cyberdefense capabilities starting in the 1990s and it can no longer be considered behind in this domain
North Korea is able to carry out cyberattacks abroad	Can North Korea rely on its foreign allies to support and help carryout cyberattacks?

Table: Some key themes that feed discussions surrounding cybersecurity/defense and the North Korean internet.

3 - The implications of the North Korean cyberthreat

3.1. A set of measures taken against the North Korean cyberthreat

The sanctions taken by a range of international actors cover several themes: Defense (nuclear weapons and weapons of mass destruction); international commerce (control of arms export to and from North Korea, the nuclear sector, and also the fishing industry and other business industries, etc.); the finance sector; culture (prohibited communications between the two Koreas); and the reception of North Koreans in foreign countries. In early 2016 the UN adopted a new resolution (No. 2270) against North Korea in addition to resolutions 1718 of 2006, 1874 of 2009, and 2087 and 2094 of 2013.[8] South Korea imposed the closure of the Keasong complex, while Japan strengthened existing measures against North Korea. The European Union supports the whole decisions of the Council since 2013.[9] In recent months additional cybersecurity measures have been taken.

On January 2nd 2015, the United States revealed the parties responsible for the cyberattacks against Sony[10] (these imputations are possible thanks to the information collected by the NSA[11]):

- The central bureau of intelligence (Reconnaissance General Bureau), which is the principle intelligence agency in the country
- The KOMID (Korea Mining Development Trading Corporation), a North Korean arms dealer, exports goods and equipment for ballistic missiles and conventional weapons
- The Korea Tangun Trading Corporation, which uses various names around the world including Ryung Seng Trading Corporation, Ryungseng Trading Corporation, and Ryungsong Trading Corporation
- Kil Jong Hun, North Korean government official (representative of KOMID in Namibia)

[8] A summary of resolutions is available on the following website: https://www.armscontrol.org/factsheets/UN-Security-Council-Resolutions-on-North-Korea

[9] The full list of measures that apply to North Korea (and also other countries) is available in the summary document online at: http://eeas.europa.eu/cfsp/sanctions/docs/measures_en.pdf

[10] "Treasury imposes sanctions against the government of the Democratic People's Republic of Korea," *U.S. Department of the Treasury*, February 2015, https://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx

[11] The NSA would have been in the North Korean networks well before the attacks against Sony.
- WILLAMS M. (2015), « NSA had access to North Korean computer network, says report", North Korea Tech, 19 January, http://www.northkoreatech.org/2015/01/19/nsa-had-access-to-north-korean-computer-network-says-report/
- SANGER D.E., FACKLER M. (2015), "NSA breached north Korean networks before Sony attack, Officials say," The New York Times, 18 January, http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0

- Kim Kwang Yon, North Korean government official (representative of KOMID in Africa)
- Jang Song Chol, representative of KOMID in Russia, North Korean government official, and also works with Sudan
- Yu Kwang Ho, North Korean government official
- Kim Yong Chol, representative of KOMID in Iran and a North Korean government official
- Jang Yong Son, representative of KOMID in Iran and a North Korean government official
- Kim Kyu, head of foreign affairs at KOMID and a North Korean government official
- Ryn Jin, operating for KOMID in Syria and a North Korean government official
- Kang Ryong, operating for KOMID in Syria and a North Korean government official
- Kim Kwang Chin, representative of Korea Tangun Trading Corporation in Shenyang, China, and also a North Korean government official

There are two types of accused in this case, organizations and individuals (more precise information surrounding their identities such as birthdays and passport numbers are available on the U.S. Department of the Treasury website).[12] This method of accusing individuals is reminiscent of the procedure used by the U.S. in May 2014 regarding five Chinese military members accused of cyberespionage.

Notably, after a succession of cyber-related incidents attributed to North Korea (but not solely), the authorities in Seoul were convinced of the need to strengthen their cybersecurity systems. Officials created a position to oversee cybersecurity and appointed a professor at the Korea University to advise the government surrounding issues of cybersecurity.

In February 2016, the U.S. House of Representatives passed new sanctions against North Korea[13] that take measures in several domains including in cybersecurity (WERTZ, 2016).[14] The text cites that North Korea was implicated several times in illegal activities, including incidents relating to the cybersecurity of the United States (the text mentions the Sony hacks). The text also references the cyberattacks against South Korea, referencing the attacks dubbed "Dark Seoul" of the 20th of March 2013 that hit the infrastructure of the South Korean media and finance sectors. The United States applies sanctions against those involved in aggressive cyber operations. The document talks about both the institutions and individuals implicated in cyberterrorism and the development of cyberwarfare capacities and expressed the hope that other members of the United Nations will follow the same path in terms of applying sanctions.

3.2 International cooperation organized against the North Korean threat

Beyond cybersecurity, international relations are developing in the political, military, and commercial arenas in particular. In Korea, Microsoft established a cybersecurity center. On a political level, South Korea and the United States have announced their will to strengthen their cybersecurity coordination (October 2015). The United States is looking for allies in their on-going conflict with North Korea and cybersecurity has become a reason for pursuing rapprochement with other countries. It has also become a vehicle for strengthening the North American presence in the region. More concretely, what is this cybersecurity cooperation composed of? Are these cooperations really effective, when they are not just declarations of intent?

[12] Detailed information: https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20150102.aspx
[13] Full Document: https://www.congress.gov/bill/114th-congress/house-bill/757/text
[14] WERTZ D. (2016), "Summary of the North Korea Sanctions and Policy Enhancement Act of 2016," Washington, February, 7 pages, http://www.ncnk.org/resources/publications/HR757_Summary_Final.pdf

Conclusion

Opinions are sharply divided when it comes to assessing the degree of danger North Korea poses in terms of cyberdefense and the level of their capabilities in that domain. What are the military cyber-capabilities within the North Korean defense system? According to the defector Kim Heung-kwang in statements made to the BBC, 10 to 20% of the North Korean defense budget is dedicated to online operations. For some, North Korea represents a major cyberthreat, while others disagree and see it as a threat that should kept in perspective (Lee Kwek, 2015).[15] Is North Korea as aggressive in cyberspace as South Korea and the United States have suggested? The list of incidents attributed to North Korea in a 2015 report published by the CSIS is quite short and only mentions nine such incidents since 2009.

Chaire Cyber-Défense et Cyber-sécurité (Chair of Cyberdefense and Cybersecurity)
Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris
Phone number: 01-45-55-43-56 - Email: contact@chaire-cyber.fr;
SIRET N° 497 802 645 000 18

The Chair thanks its partners

[15] LEE D., KWEK N., "North Korean hackers 'could kill', warns key defector," BBC News, 29 May, http://www.bbc.com/news/technology-32925495