Cyberwarfare in the Korean Peninsula: Asymmetries and Strategic Responses

By: Nir Kshetri

Kshetri, N. (2014). Cyberwarfare in the Korean Peninsula: Asymmetries and Strategic Responses. *East Asia, 31(3),* 183-201. doi: 10.1007/s12140-014-9215-1

The final publication is available at Springer via http://dx.doi.org/10.1007/s12140-014-9215-1

Abstract:

In this paper, we argue that the two Koreas' intentions and actions on the cyber front point toward the possibility that they have engaged in cyber warfare against each other. From South Korea's standpoint, a key concern has been North Korea's advanced cyber warfare capabilities and alleged involvement of its substantial workforce in the Internet's dark side activities. These issues need to be looked at the backdrop of the North's nuclear and ballistic missile capabilities. This paper draws principally upon theories and concepts from military strategy and warfare to examine the contexts, mechanisms, and processes associated with the cyber warfare in the Korean peninsula. We also compare the two Koreas in terms of various forms of asymmetries in cyber warfare and cyber attacks. Also highlighted in the paper are South Korea's recent initiatives and actions to enhance cyber-offense and cyber-defense capabilities.

Keywords: Cybersecurity | South Korea | North Korea | Positive and negative asymmetries | Cybersecurity strategy | Reconnaissance General Bureau of the Korean People's Army

Article:

Introduction

Defense specialists have argued that by combining cyber warfare and electronic warfare with other asymmetric assets such as hovercraft, chemical, biological, and radiological weapons, North Korea is likely to strengthen its warfare capabilities significantly [*41*]. Consistent with this observation, in the past few years, South Korea's military, government agencies, businesses, nonprofit organizations, and consumers have faced a number of high-profile cyber attacks. Although it is impossible to prove with certainty, based on indirect and circumstantial evidence, South Korea has accused North Korea for most of the major cyber attacks facing the country. In March 2014, the South Korean Defense Ministry reported that it detected a hacking attempt allegedly from North Korea to steal military data, which used a journalist's computer. According to the Ministry, the journalist covered defense issues, whose

computer was connected to the Defense Ministry's Internet network [*2*]. In October 2013, quoting the country's Defense Ministry, Rep. Chung Hee-soo of the ruling Saenuri Party, noted that North Korea launched over 6,000 cyber attacks against the South since 2010 [*33*]. According to the South Korean government, North Korea's cyber attacks cost the country over 860 billion won (US$805 million) between 2009 and 2013 [*28*].

North Korea has also reported that it has been victimized by cyber attacks. Its officials said that cyber attacks had been launched against the servers of the country's broadband provider Loxley Pacific Co. in March 2013, around the time as the cyber attacks experienced by South Korean banks and TV stations (Table 2) [*82*].

South Korea's hostile and tense relationship with the North has special implications for the country's cyber security. The two countries are still technically at war. While the North has a drastically lower level of economic development, the asymmetric nature of cyber attacks means that actors with limited financial and technical resources possess capability to compromise high-value targets [*58*]. North Korea has reportedly developed advanced cyber warfare capabilities and its substantial workforce is allegedly involved in the Internet's dark side activities with the explicit support of the state. In its annual report on the state of North Korea's military released in March 2014, the US Department of Defense observed that North Korea shifted its focus toward offensive cyber operations (OCO) and other asymmetric tactics [*69*].

North Korea-originated cyber attacks have unique and idiosyncratic characteristics and important strategic and geopolitical dimensions from the perspective of South Korea. For instance, while cybercrimes and cyber attacks originated from China and Russia have allegedly victimized the USA and other Western countries, the West has clearer understanding of the point of view of China and Russia despite occasional tensions and conflicts. China and Russia also maintain diplomatic and economic ties with most countries. The general lack of such understanding with regard to North Korea has increased the complexity of the issue [*18*]. Due to the regime's unpredictability and desperation to survive, North Korea has been described by analysts as involving high perceived threats to its adversaries [*30*]. Moreover, unlike China's People's Liberation Army (PLA), which regularly publishes academic journals and policy documents, North Korea's Korean People's Army (KPA) does not publish any documents. Assessing the KPA's advancement in cyber-weapons is thus an extremely difficult exercise [*83*].

South Korea thus faces unique challenges from the standpoint of cyber attacks and cyber security. Unsurprisingly, it has employed various strategic responses to cyber-threats. In 2010, South Korea reportedly developed and implemented a cyber-strategy to combat the situation. The first part of the plan, which was up and running as of early 2014, focused on protecting networks from cyber attacks [*40*]. It also involves an online propaganda campaign, which includes posting on North Korean social networking websites [*5*]. The second phase of the plan involves developing cyber-weapons that can be deployed to physically damage North Korean nuclear plants and missile facilities. South Korean Defense Ministry has announced its intention

to develop weapons similar to Stuxnet, which was designed to destroy Iran's nuclear enrichment facilities [*5*].

In this paper, we use various concepts related to symmetric and asymmetric advantages [*47*, *61*, *62*] to analyze the cyber warfare in the Korean peninsula. The analysis of this paper is expected to provide important insights into factors that affect positive and negative asymmetries associated with cyber attacks and cyber security from the perspectives of the two Koreas. We also examine the unique natures of cyber-threats facing South Korea and discuss the country's response to such threats.

The paper is structured as follows. We proceed by first examining the current state of cyber warfare in the Korean Peninsula. Next, we provide an assessment of North Korea's cyber attack capability. Then, we compare the two Koreas in terms of various forms of asymmetry from the standpoint of cyber-offense and cyber-defense. The section following this looks at South Korea's recent initiatives and actions on the cyber front. It is followed by a section on discussion and implications. The final section provides concluding comments.

The Current State of Cyber Warfare in the Korean Peninsula

It is important to make clear at the outset that different definitions of cyber warfare exist. Among the earliest examples of cyber attacks that are widely believed to be carried out by a nation state include those on Georgia in 2008 and on Estonia in 2007. Cyber warfare experts, however, debate over whether these qualify as cyber warfare. According to the strictest definition, a cyber attack is considered as a cyber war only if it causes "widespread harm, rather than mere inconvenience" [*79*]. Viewing from this perspective, even the 2008 cyber attacks against Georgia may not qualify as cyber war, since unlike the military operations, cyber attacks did not cause a physical harm. Some observers, on the other hand, argue that a cyber attack qualifies as a "cyber war" if it is combined with conventional military operations. According to this view, the attacks on Georgia would thus qualify as cyber warfare but those on Estonia would not [*79*]. Others argue that the effects of the 2007 cyber attacks in Estonia "were potentially just as disastrous as a conventional attack on this country" [*77*].

Now let us define cyber warfare for the purpose of this paper. Analyzing a number of documents related to war ultimatum and motivations of war such as those of the World War I era (e.g., statements of British Foreign Minister Edward Grey and German Chancellor Theobald von Bethmann-Hollweg) and the legendary Mongolian warrior and conqueror, Genghis Khan, Hirshleifer [*35*] concluded that wars were fought for material ends as well as for intangible goals such as honor, dominance, reputation, and prestige. Based on this, we define cyber warfare as actions in the cyberspace carried out or initiated by a state actor against another state (an adversary state) for economic gains or with an intention to cause material losses or to destroy the glory, honor, prestige, and reputation of the adversary. A number of cyber attacks that are widely believed to be carried out or initiated by nation states such as the 2007 cyber attacks against

Estonia, the 2008 cyber attacks against Georgia, the Stuxnet worm which was designed to destroy Iran's nuclear enrichment facilities in 2010, and the 2012 cyber attacks against Saudi national oil company Aramco would fit this definition of cyber warfare. To put things in context, Table 1 presents some examples of actions allegedly carried out by the two Koreas. Following Hirshleifer's [*35*] definition of war, these activities qualify as cyber warfare.

Table 1 Some examples of actions allegedly carried out by the two Koreas pointing toward their engagement in cyber warfare

Actions allegedly carried out by North Korea	**Actions allegedly carried out by South Korea**
A number of cyber attacks on South Korean banks, insurance companies and other targets during 2009–2013, which led to significant economic loss (e.g., erasing computer hard drives of one of the largest banks, which left 30 million customers without ATM services for many days) (see Table 2).	The cyber command's efforts on psychological warfare activities against North Korea. Its online propaganda strategy involves posting to North Korean social networking and social media websites.
A number of cyber attacks launched to destroy the honor and glory of South Korea (e.g., during the 63rd anniversary of the Korean War), which victimized the ruling Party, the presidential office website, military personnel, the Defense Ministry, and the National Assembly, etc. (see Table 2).	Plan includes further building psychological warfare capability (e.g., courses in the Korea University's cyber-defense school, which is sponsored by the South Korean army, include breaking malicious codes, psychological preparation for cyber warfare and other techniques).
North Korea's state-sponsored hackers' engagement in criminal activities such as the creation of malware to engage in financially motivated cybercrimes victimizing South Korean businesses and consumers (e.g., servers of MMOs such as "Lineage" and "Dungeon and Fighter").	The Defense Ministry's plan to strengthen offensive capabilities and develop a Stuxnet-like worm to attack North Korea's nuclear facilities.
North Korean agents post online comments to weaken South Korean morale.	Plan to train 5,000 cyber security experts by 2017.

From the material ends perspective, Hirshleifer [*35*] expressed a sense of optimism that nations' chance of engaging in war has diminished due to the rising costs of and low potential benefits from war compared to those that can be realized from peaceful trade and commerce. Because of the potentially high costs associated with a physical war, in terms of human lives and suffering and longer term development, cyber attacks are viewed as a considerably cheaper and more attractive option. From the perspective of South Korea, for instance, cyber attacks may be a low cost means for destroying North Korea's nuclear programs. As noted earlier, in February 2014, South Korea's Defense Ministry outlined its aim to strengthen its offensive capabilities and develop a cyber-tool, which can attack the North's nuclear facilities [*8*]. The tool will be similar

to the Stuxnet worm, which was programmed to damage Iran's centrifuges at the Natanz nuclear site. The Defense Ministry also announced a plan to create a new Cyber Defense Command by May 2014 to carry out these missions. Likewise, as noted earlier, due to the asymmetric nature of cyber attacks, actors with limited financial and technical resources such as North Korea possess capability to compromise high-value targets [*56*].

A survey of government institutions, banks, businesses, and schools indicated that in 2003, 26,000 hacking incidents were reported to the South's Ministry of Information and Communication which was 178 times the level in 1996 [*36*]. Table 2 presents major cyber attacks faced by South Korea in recent years. The president of the Korea Internet and Security Agency (KISA) described the recent cyber attacks as Advanced Persistent Threat (APTs), in which the perpetrators carefully studied the targets for a long period to develop their tactics [*43*]. The National Intelligence Service (NIS) has also accused the North of manipulating the South's online opinion by engaging in activities such as posting blogs and e-mailing journalists [*14*].

Table 2 Major cyber attacks experienced by South Korea in recent years

Time	**Explanation**
July 2009	• Starting July 4, websites of the South Korean and the US government and South Korean financial firms were disrupted by DDOS attacks for many days with millions of requests per second, which was the first major attack facing the country [*16*]. The websites of the presidential office, the Defense Ministry, and the National Assembly were among the key targets.
March 4, 2011	• A second major cyber attack launched malware, which erased computer hard drives of one of the largest banks and left 30 million customers without ATM services for many days [*16*]. • Cyberattacks that were believed to be originated from North Korea jammed GPS signals during joint U.S.–South Korea military drills. The attacks lasted for 10 days [*12*].
April–May 2012	• North Korea allegedly launched a jamming attack against the South, which affected GPS navigation of 337 commercial flights, 122 ships, and a number of vehicles [*45*].
March 20, 2013	• Three broadcasters KBS, MBC, YTN; three banks Shinhan, Nonghyup, and Jeju; and two insurance firms reported cyber attacks to their networks to the National Police Agency.
June 25–July 1, 2013	• A series of cyber attacks paralyzed the country's 69 government offices, major banks (e.g., NongHyup and Shinhan), major telecommunications companies, news outlets, broadcasters, and other institutions. In addition, the attacks also victimized the presidential office website, which stored massive personal data of 2.5 million members of the ruling Saenuri Party, 300,000 military personnel, and 200,000 registered users [*7*]. The attacks coincided with the 63rd anniversary of the Korean War, which started on June 25, 1950.

South Korea's unique geographic position bordering North Korea makes it especially vulnerable to some types of cyber attacks. For instance, regarding numerous GPS attacks against the South allegedly carried out by the North, geography has an important role to play. In the 2012 GPS attacks, the jamming signals were identified as coming from Kaesong in North Korea about 10 km from the border and 50 km from the Incheon International Airport [*45*].

Quoting an NIS official briefing her, a lawmaker, who served the country's intelligence committee, noted that most of the websites victimized by the attacks belonged to conservative South Korean organizations that support a hard-line approach to North Korea [*67*]. A major target in the June–July 2013 cyber attacks was South Korea's Hyundai Merchant Marine (HMM). This has been a puzzling mystery for some analysts due to the lack of obvious benefit to North Korea from cyber espionage against HMM. Ulsch [*80*] concluded that a more probable explanation of the cyber attacks against HMM would be that North Korea might have been hired by China to do so. Other possible explanations could be that North Korea launched the attack with a different motivation: to sell the information to China. Still another explanation offered was that China may have launched the attack but did in such a way that it looked like one that was perpetrated by North Korea[*80*].

The regulatory developments that have occurred in South Korea in response to the North-originated cyber attacks have far reaching implications. For instance, while Google Maps can provide directions for public transport in South Korea, they cannot do so for driving. In order to block from falling into North Korean hands, South Korean security restrictions put in place after the Korean War prohibit the export of map data. Thus, Google and other foreign companies are not allowed to provide driving maps for South Korea [*70*]. As another example of regulatory development, following foreign hackers' alleged cyber attacks in 2004, South Korea made it mandatory for Internet-related firms to report hacking incidents [*36*]. The country became one of the first in the world to introduce such regulations.

An Assessment of North Korea's Cyber Attack Capability

It is important to recognize that, as is the case of any underground economy [*65*], estimating the size of a country's cybercrime industry or its cyber attack capability is a challenging task. Cyber attack-related studies and surveys are replete with methodological shortcomings, conceptual confusions, logical challenges, and statistical problems. The reliability and validity of indicators used to measure cyber attack-related constructs are of major concern [*48*]. The newness of the phenomenon further compounds the problem. Nonetheless, instead of burying our heads under the sand, it would be better to address the issue with whatever clarity, rigor, and systematization that can be achieved.

Regarding the development of the North Korean IT industry, it is worth noting that the country launched fiber-optic, computer hardware, and commercial software industries in the late 1990s. It has developed its own operating system called Red Star. Software development has been a key

focus of the North Korean IT industry due primarily to the low entry barriers in this industry. Estimates suggest North Korea has 4,200 software developers working for various agencies [*14*]. The Korea Computer Centre (KCC) has achieved some success in developing software products such as computer games [*11*].

North Korean rulers also view that a well-developed IT industry can overcome the adverse effects of economic sanctions facing the country. According to a South Korean official, in February 2013, the North Korean leader Kim Jong-un reportedly said: “If we have strong information technology and brave warriors like the Reconnaissance General Bureau, we will be able to break any sanctions and have no problem building a strong and prosperous country” [*13*].

It was reported, however, that North Korea’s efforts to develop electronic warfare capabilities dates back as early as the mid-1980s [*51*]. In 1986, it founded Mirim University in the mountainous region of Hyungsan, which is currently known as Automation University. According to testimonies by defectors who had graduated from the University, 25 computer experts from Kyrgyzstan were invited to establish a cyber warfare program. According to former students from the University, more than 100 hackers graduate from the program every year. Graduates of the University are skilled in writing computer viruses, penetrating network defenses and programming weapon guidance systems, and other areas [*60*]. Such programs are also known to exist in several branches of the KPA.

The KPA is reported to have a cyber warfare unit in the Reconnaissance General Bureau, also known as “Unit 121”. According to Won Sei-hoon, then chief of South Korea’s National Intelligence Service (NIS), in 2010, there were 1,000 professional hackers in North Korea’s cyber warfare unit [*55*]. In 2009, then-leader Kim Jong Il was reported to order the cyber command unit to expand to 3,000 hackers. Currently, the Unit is estimated to have 3,000–4,000 personnel engaged in cyber warfare. As a point of comparison, this unit is much larger than South Korea’s Cyber Command force, which consisted of around 400 personnel in 2013 [*6*,*28*].

According to the NIS, North Korea has developed cyber attack capability to take over South Korea’s power supply systems. North Korea is also reported to be active on about 400 social media sites. One such site is the state-run, Uriminzokkiri, a site for Korean speakers, which is allegedly used for psychological warfare [*14*].

According to testimony of a North Korean defector, who taught hacking in the country before defection, students with a high level of proficiency in math and science are enrolled into a 6-year program of Pyongyang’s elite Keumseong High-Middle Schools. After graduating from Keumseong, they are sent to attend top technology institutes and universities such as the Kim Il Sung University, Kim Chaek University of Technology, Mirim University under the General Staff Department or Moranbong College under the Reconnaissance Bureau, and various others in Pyongyang or Hamheung [*13, 57*]). Following an expedited 2-year program at one of the universities, the students are sent to China or Russia for 1 year to solidify and polish their

knowledge of hacking and other skills. They receive significant stipends during overseas deployments [*86*]. After overseas training, they are placed in various cyber warfare units [*55, 86*]. These overseas-trained hackers and their families also receive special housing, food subsidies, and other benefits including the opportunity to live in Pyongyang, which is considered to be a special privilege [*86*]. A main reason why the hackers get such a special treatment is that they are allowed access to the Internet and thus have knowledge of the outside world's relative prosperity. Moreover, the North Korean regime believes that such a treatment may reduce the skilled hackers' temptation to defect [*38*].

According to a South Korean security official, North Korea also has about 12,000 highly skilled civilian hackers [*13*].[1] In a report given in November 2013 to the intelligence committee of the National Assembly, South Korea's NIS noted that there were seven North Korean hacking organizations and a network of spies operating in China and Japan [*76*]. In addition, the South Korean police estimates also suggested that there were about 10,000 North Korean hackers who operate criminal activities from China. These hackers are graduates of elite institutions such as Kim Il Sung University and allegedly report to North Korean government agencies such as the Korea Computer Center and Rungrado General Trading Corporation. The South Korean police also estimated that each North Korean hacker operating from China sends about US$500 per month to the "Office 39" or "Bureau 39", which is a secretive branch of the North Korean regime that provides financial support to the country's leadership in part through alleged engagement in illicit activities [*21*].

The forces described above, and perhaps others have provided pressures to North Korean IT industry to internationalize. The stated objective of North Korean software industry's internationalization is to learn from foreign IT trends and to promote the development of the domestic IT industry [*11*]. An estimated 1,000 North Korean hackers are believed to be in undercover assignments working for educational software companies, animation companies and other firms in China, and economies in Southeast Asia, and Europe [*13*].

According to a South Korean security official, there are a number of instances of North Korean hackers' collaborating with South Korea criminal networks abroad, who take orders from the latter to create websites for video and online games and gambling and other related assignments. The hackers are provided with servers, laptops, and other resources. In August 2011, the South accused that the North's government rented out its team consisting of 30 highly skilled programmers from the state-run Korea Computer Center in Pyongyang and the Korea Neungnado General Trading Company to a group of fraudsters operating out of China. A South Korean internet café owner allegedly worked with the North Korean team to create a malware that exploited South Korean servers of massively multi-player online games (MMOs) such as "Lineage" and "Dungeon and Fighter" and played them automatically. According to the South Korean police, in less than 2 years, the China-based group of fraudsters made about US$6 million from the malware created by the North Korean team. The hackers' share of the money, which was reported to be 55 %, was believed to be remitted to the "Office 39" [*21*, *74*].

In some cases, the gaming websites allegedly serve as the infrastructure for cyber attacks against critical South Korea targets [*13*]. In June 2013, South Korean police discovered that North Korea had used free-to-download video games to infect about 100,000 computers, which were used to launch cyber attacks against the Incheon International Airport. The attacks were traced back to a South Korean businessman, who had reportedly met with the members of the "Bureau 39" in China. The businessman, who was arrested, allegedly paid tens of thousands of US dollars to buy the game, which was then sold to South Korean online gaming companies [*26*]. In this way, the North Korean game developers have been able to kill two birds with one stone: making money and launching cyber attacks against key targets in the South.

Various Forms of Asymmetry: A Comparison of the two Koreas

The concepts of symmetric and asymmetric advantages and threats would help us to further understand the real and perceived risks associated with cyber warfare. Prior research has noted that nations are employing information and communications technologies (ICTs) strategically to minimize vulnerabilities associated with negative asymmetry [*46*]. Before proceeding further, we define several terms: symmetric advantage is the advantage that can result from matching the opponent in terms of strategic resources [*61*]. Positive asymmetry entails capitalizing on differences to gain an advantage. Negative asymmetry involves "an opponent's threat to one's vulnerabilities" [*61*]. Strategic asymmetry involves employing "some sort of differences to gain an advantage over an adversary" [*61*]. It could be real as well as perceived.

Experts argue that only "desperate antagonists" rely solely on ICT-created or other types of asymmetric methods [*62*]. That is, integrated approaches that appropriately combine symmetric and asymmetric methods are more likely to give intended results and defeat adversaries [*61*]. In particular, given the limitations of ICTs, approaches that combine non-ICT and ICT tools are likely to be more effective. Cyber war is strongly tied and related to conventional forms of warfare [*27*]. The above facts thus need to be considered in relation to more conventional threats to South Korea posed by North Korea's nuclear and ballistic missile capabilities. This is because an adversary that possesses capability to combine cyber attacks with traditional methods such as kinetic warfare can maximize the potential benefits from cyber war. One way to operate for such adversary is to gain some temporary advantages with cyber war and subsequently launch traditional military attacks [*27*]. Thus, just like its nuclear capability [*31*], cyber warfare capability is likely to have a key role in North Korea's offensive warfare strategy.

Table 3 compares the two Koreas in terms of various asymmetries identified by prior researchers [e.g., 46, 61] in the context of cyber warfare. These are linked with the sources of positive asymmetry as well as the adversary's negative asymmetry.

Table 3 Various forms of asymmetries in cyber warfare: a comparison of the two Koreas

Form of asymmetry	**Explanation**	**Examples**

Organization	An adversary adopts a different form of organization (e.g., different combination of networked and hierarchical forms)	• While North Korea's cyber-warriors are organized hierarchically like a state actor, they are also organized in a network fashion in foreign countries. North Korean hackers reportedly work undercover in China, Southeast Asia, and Europe. To some extent, this structure resembles like a non-state actor. • South Korea has teamed up with the USA.
Will	Willingness to bear higher costs and take greater risk.	• In light of the sanctions and increasing *isolation* facing North Korea, cyber attacks and cybercrime activities are more attractive options compared to "kinetic" actions.
Morale	Using different tactics than the enemy to boost the morale of cyber-warriors.	• Successful cyber attacks may have bolstered the morale of North Korea. • North Korean propaganda organs have portrayed the South as a "puppet" controlled by USA "imperialists". • Manipulating the morale of troops in order to create an asymmetric advantage is effective in the North due to the ban on the Internet use by the average citizens.
Patience	An adversary's greater patience to remain in a conflict for a longer period.	• In general, Asians arguably exhibit greater patience than Westerners but it is not clear whether any of the two countries has an advantage over the other.
Method	Using operational and/or tactical means that are different from used by or expected by the adversary.	• North Korea has employed methods that are tricky and effective to penetrate the networks in the South (e.g., infecting computers through online games). Perusal of puzzling and unexpected targets such as HMM.
Technological	Using cyber-weapons and weapon systems against an adversary that is technologically superior and innovative.	• South Korea has more resources to develop cyber-offense and defensive capabilities • Major local antivirus firms have capabilities to detect and stop cyber attacks.
Normative	Exploiting the differences in ethical and legal standards between adversaries.	• The North Korea regime is not required to follow strict legal rules and requirements to engage in cyber warfare. • South Korea: The nationalist Left, internal political dissidents, and other North Korean sympathizers may oppose attacks against the North [*25*].

Source: Based on [*47*, *62*]

North Korea

It is clear that North Korea has very much to gain and very little to lose from engaging in cyber warfare activities. Internet penetration in North Korea is difficult to estimate accurately but is

expected to be extremely low. According to BBC, only a “few dozen families” have full and unfiltered Internet access [*54*]. Other estimates range from “a few hundred people” to “1,000 at most” [*37*]. As of 2012, there was only one cybercafé in the capital, Pyongyang [*37*]. Moreover, the closed nature of North Korea’s Internet system makes it is easy to defend giving it a strategic and tactical advantage [*76*].

In order to better explain North Korea’s approach, it is important to understand the Chinese military’s viewpoint regarding cyber warfare. Two senior colonels of the Chinese military Qiao Liang and Wang Xiangsui, in their 1999 book *Unrestricted Warfare*, have argued that since China’s PLA lacks resources to compete with the USA in conventional weapons, it should focus on the “development of new information and cyber war technologies and viruses to neutralize or erode an enemy’s political, economic and military information and command and control infrastructures”. The authors have urged on the development of a means of challenging the USA through asymmetry rather than matching it in terms of all types of resources. The authors also observed that the US Army is too focused on “weapons whose immediate goal is to kill and destroy” and may not be well equipped in assimilating ICTs in the warfare. The North Korean regime may have observed the South in the same manner.

Low cost and deniability make cyber attack an attractive option for North Korea. In light of the sanctions and increasing isolation facing North Korea, it is worth noting that compared to so called “kinetic” actions such as dropping bombs and shooting bullets, anonymity of cyber attacks make it difficult in attributing such attacks to a specific source. Clark and Landau [*15* p. 2] highlight how problems associated with attribution may limit the ability of a government to deter and retaliate: “Retaliation requires knowing with full certainty who the attackers are”. In South Korea’s case, it is argued that politically motivated cyber attacks are not just external since it also has internal political dissidents [*42*]. Some of the malware used in the attacks against the South Korean targets was traced to a computer in Seoul. Some of the codes also came from the USA and three European countries [*54*]. North Korea may thus launch cyber attacks and avoid sanctions and retaliatory attacks. In this way, the development of cyber warfare capability would give North Korea the ability to harm enemies without potential negative consequences [*59*].

Some analysts have noted that while technologically advanced states are more fearful of cyber warfare, technologically backward states may face greater challenges and difficulties for this new mode of warfare [*27*]. For North Korea, one way to overcome the challenges associated with limited resources and infrastructures has been to operate from China, which has more developed Internet infrastructures. North Korea is believed to gain cooperation and support from China and is believed to establish hacking points there. Some analysts argue that North Korea is launching the attacks against the South under China’s “tacit consent” using its more developed Internet infrastructure [*76*]. For instance, the Unit 121 of the Reconnaissance General Bureau of the KPA reportedly operates from China, including a luxury hotel in Shenyang, the capital of Liaoning Province [*16*]. According to Kaspersky Lab, in the June–July 2013 cyber attacks, for instance, ten of the IP addresses originated in the Jilin Province Network and the Liaoning

Province Network. Note that these two provinces are near North Korea. The ISPs that serve the region are believed to maintain communication lines into parts of North Korea [*80*],

North Korea's expertise and experience in the dark side of the Internet is also a source of positive asymmetry. North Korea has used some "tricky" methods to launch attacks against the South (Table 3).

Finally, as a source of negative asymmetry, the lack of resources deserves mention. North Korea's lack of infrastructures such as a reliable electrical grid may prove a serious hindrance to develop cyber warfare capabilities. It also lacks resources to train its cyber warfare force with state-of-the-art hacking and cracking technologies and advanced cyber warfare capabilities.

South Korea

South Korea undoubtedly demonstrates a higher level of resourcefulness in developing greater levels of cyber-offense and defensive capabilities. For instance, according to the United Nations (UN), in 2012, South Korea's per capita Gross National Income (GNI) was US$23,180 compared to North Korea's US$583 [*81*]. In order to understand the significance of this difference, it is important to note that an asymmetric threat that is effective at one point of time may stop producing results subsequently as the adversary adjusts its strategy and tactics [*62*]. This huge difference thus has the consequence that North Korea would face difficulty in matching the South in resource-intensive strategies and tactics.

South Korea's major local antivirus firms such as HAURI and AhnLab have capabilities to detect and stop cyber attacks. In October 2013, AhnLab detected distributed denial-of-service (DDOS) attacks on local companies which infected over 10,000 computers.

The South Korean Defense Ministry announced that it would work with the USA in the development of cyber-offense capabilities [*4*, *22*, *78*, *85*]. Note that the USA has teamed up with South Korea and other Asian allies such as Japan in addressing the threats associated with North Korea and China [*68*]. In recent years, the cooperation has been extended to the cyber domain. South Korea and the USA have started holding joint cyber-defense exercises regularly and are training professionals to protect from the cyber-threats. In the annual war exercise of August 2012, military forces of the two countries conducted first basic cyber warfare operations, which were viewed as a step to enhance cyber-defenses [*44*].

A big concern is a general lack of cyber security orientation among individuals, businesses, and government agencies in South Korea. The country's businesses and government agencies have failed to invest in security systems adequately. This is a serious concern, given the widespread use of ICTs in the South. For instance, according to the National Information Society Agency, South Korean government's budget for information protection for 2013 was US$214 million [*7*]. According to a Panda Labs' Annual report 2012, South Korea had the world's second highest percentage of computers infected with malware (54.2 %) only behind China (54.9 %). A

simulated cyber attack carried out by the Korea Advanced Institute of Science and Technology (KAIST) in an agreement with a Korean bank indicated that the bank's security mechanism could be broken in a few weeks [*7*]. Observers have also noted that the South Korean military is unprepared to deal with counterattacks [*34*].

South Korea's high dependence on digital technologies can be viewed as a weakness that adversaries can exploit. One estimate suggested that daily online banking transactions in South Korea amounted to US$29.3 billion in 2013 [*7*]. Likewise, car navigation, air traffic control as well as US and South Korean military systems heavily rely on the GPS navigation system [*83*]. South Korea's information superiority makes its networks extremely lucrative targets and highly vulnerable to the threats of asymmetric technologies.

There are a number of additional constraints and challenges. The nationalist left and other North sympathizers in the South may oppose attacks against the North [*25*]. According to an opinion poll reported in the Munhwa Ilbo newspaper in May 2005, 48 % of South Koreans said that they would back the North if the USA bombed it [*63*]. Especially young people, who did not experience the Korean War, are found to be more sympathetic to North Koreans [*52*]. Another poll conducted among 15 to 25 year olds in the South, which was published by the Chosun Ilbo newspaper in August 2005, reported that about two thirds of respondents would support the North in a war with the USA [*63*]. North Korea's United Front Department is allegedly engaged in cyber psychological warfare. There are reportedly about 200 agents whose job is to post online comments to weaken the morale of South Koreans. They allegedly do so through about 140 websites that have servers in 19 countries. In 2011, these agents were reported to post about 27,000 items of propaganda materials against South Korea and the number of items posted was estimated to exceed 41,000 in 2012 [*52*].

A final consideration with the South is the reputation damage that the South Korean cyber warfare command suffered from the alleged engagement in psychological warfare capabilities on its own population, which may also lead to a reduced public support for the organization. Critics have noted that a major weakness of South Korea is its politicized military [*19*]. It was accused that the South Korean military tried to influence voters during the 2012 presidential elections [*5*]. According to the South Korean Defense Ministry, at least 11 officials at its cyber warfare command spread online political messages, which praised President Park Geun-hye and her party or attacked the opponents before the 2012 election [*75*].

South Korea's Recent Initiatives and Actions

Given the unique threat that the North presents, South Korea has realized the importance of developing cyber-offense and cyber-defense capabilities. It is taking measures to develop symmetric advantage by matching its adversary (North Korea) in terms of strategic resources and is attempting to make adequate institutional, financial, and policy preparations for strengthening

cyber security. South Korea established a cyber command in January 2010 and a cyber-protection policy team at the Defense Ministry in March 2011 [*73*].

The cyber command has focused its efforts on psychological warfare activities against the North's propaganda and other cyberspace tactics that it considers as offensive [*23*]. The South's online propaganda strategy, on the other hand, involves posting to North Korean social networking and social media websites. The South Korean Defense Ministry's plan also includes further building its psychological warfare capability [*23*]. Moreover, South Korea blocks access to North Korean websites and broadcasts [*9*],

In 2012, the South Korean army teamed up with Korea University to open a cyber-defense school, which enrolls 30 students per year. Courses included in the 4-year program include breaking malicious codes, psychological preparation for cyber warfare, and other techniques to protect against cyber attacks [*1*].

The Defense Ministry also established a Cyber Policy Department in 2013. The NIS announced that its Third Department[2] would give greater attention to "monitoring of cyberspace and telecommunications" [*78*]. South Korea also announced a plan to have a secretary of cyber security.

Military theorists and analysts have the category of asymmetric strategic means should be such that the adversary cannot effectively counter [*62*]. This is especially important for asymmetries that are deliberately created than those that arise by default [*47*]. South Korean policy makers believe that cyber-threat is a serious problem facing the country and worthy of serious efforts and strategies to combat it. If there is one thing that North Korea is unable to effectively replicate, it is South Korea's resourcefulness and technological might. In July 2013, South Korea announced that it would double its cyber security budget and spend 10 trillion won ($8.76 billion) by 2017. It also plans to train 5,000 cyber security experts by that time [*50*].

The South Korean military has also established a special alert level system called Information operations condition (INFOCON), which measures the cyber security threat level. Similarly, in March 2013, South Korea's Defense Ministry announced that it would increase cyber warfare forces and team up with the USA to develop deterrence scenarios [*22*]. In October 2013, the South Korean Minister of National Defense and US Secretary of Defense announced that the two countries would enhance cyber security cooperation. They also signed an agreement to establish a working-level council for cyber security policy [*10*].

In response to alleged North Korea-originated GPS attacks against its commercial flights and maritime navigational units in 2012 and 2013, South Korea is making efforts to enhance its GPS system capability and is working to develop more advanced GPS technology. For instance, the Ministry of Science and Future Planning announced plans to develop systems that can locate the "attack point and impact of jamming attempts" [*64*].

Discussion and Implications

The two countries are asymmetrically motivated to respond to adversaries in the cyberspace. Cyber attacks on South Korea, most of which allegedly are associated with the North, are frequently motivated by material and monetary gains. Each country is also attempting to destroy the honor of the other through cyber attacks and cyber warfare strategies and tactics.

Some argue that cyber-conflicts are the most serious security threat facing nations since the development of nuclear weapons in the 1940s [*17*]. An *Economist* article noted: "After land, sea, air and space, warfare has entered the fifth domain: cyberspace" [*20*]. This perspective has been echoed by numerous countries. For instance, the Japanese military has defined cyberspace as "a 'territory' where various activities such as information gathering, attack, and defence occur, on the same way as land, sea, air and space" [*3*]. Prior researchers have noted that drastic changes in the environment such as those associated with the current cyber-conflicts may create confusion and uncertainty and produce an environment that lacks norms, templates, and models about appropriate strategies, structures, and legitimacy [*29*, *66*]. A significant change also creates ambiguity in cause effect relationships, making learning difficult and inhibiting organizations' ability to undertake a rational search for solutions [*53*, *66*]. Moreover, it is difficult to learn from experience during a period of significant institutional change, because past experience is not an appropriate guide for future actions [*84*]. These conditions fit squarely in the context of cyber warfare. While the two Koreas are still technically at war and there have been frequent tensions between them, cyber-conflicts are a more recent phenomenon. Under such conditions, "superstitious learning" may occur [*56*], and organizations and nations may engage in strategically confused behavior [*32*]. A related point, as noted earlier, is that South Korea's cyber security performance has been poor. The need for change is thus apparent. Prior researchers have suggested that organizations tend to change structures when confronted with ambiguity and poor performance [*66*]. To put things in context, it may very well be the case that each country's operations in the cyber domain have been complicated by the lack of an accurate assessment regarding the possible response of the rival.

The Mongolian warrior and conqueror, Genghis Khan famously said that one of the main goals of the war was "to rob them [the enemies] of their wealth, [and] to see their near and dear bathed in tears", which provided him "the greatest pleasure" [*72*]. To put things in context, the North Korea rulers may derive pleasure from the cyber attacks-led sufferings of businesses, consumers, and government agencies in South Korea. Moreover, gains from cyber attacks on South Korean targets may also strengthen North Korean rulers' economic position. An analysis of the North Korean regimes' use of cyber attacks as a means of raising money for the ruling elites provides ample evidence to confirm the views of the skeptics, from economics and political science fields, who have questioned the effectiveness of international economic sanctions in producing desired economic and political consequences in the target country [*39*].

The two Koreas' activities in the cyber domain have important implications for them as well as other countries. Regarding South Korea's planned Stuxnet-like worm, some experts argue that the worm may damage things that are not intended targets. For instance, the Stuxnet worm also attacked Siemens control systems used in a number of facilities such as electrical generation plants, factories, and water treatment works [*5*]. It is also possible that the code may spread internationally and victimize unintended targets. Again, returning to the Stuxnet worm example, its unambiguous target was the Iranian nuclear program, it also disrupted the operations of industrial control computers in plants in China, India, and Indonesia [*24*, *49*]. Given these limitations of a Stuxnet-like worm, some analysts have suggested that a more effective approach for the South would be to intensify its "information operations" so that North Koreans have access to outside news and information, which can change their perception of the country's socio-political and economic development status [e.g., *71*].

Concluding Comments

It is fair to say that the two Koreas' intentions and actions on the cyber front point toward the possibility that these countries have engaged in cyber warfare against each other. Each country has been attempting to fight the dominance of the other in the cyberspace. Each is also bolstering its ability to defend the cyberspace against the threats posed by the other.

The North's cyber warfare capabilities may be more sophisticated and complex than many analysts give the country credit for. While it severely lacks the capability to match the South in terms of technological resources, it may have surpassed the South in terms of some aspects of cyber warfare capability. For one thing, North Korea's alleged engagement in the Internet's dark side activities is likely to produce high externalities and spillover effects for cyber attacks. The North has also displayed strong will and confidence in cyber attacks.

Some types of positive asymmetries can be deliberately created. Likewise, although negative asymmetries created by ICTs cannot be completely eliminated, they can, at least, be lessened. In this regard, some of the recent initiatives and actions taken by South Korea seem to be in the right direction and would help the country maximize positive asymmetries and minimize vulnerabilities of negative asymmetries. South Korea's case demonstrates that adoption of an appropriate combination of institutional, financial, and policy preparations are needed to deal with the growing cyber-threat. In light of the concerns raised above, South Korea needs to make further efforts to improve cyber security orientation of businesses, consumers, and government agencies.

Acknowledgment

Two anonymous *East Asia* reviewers' comments on an earlier version helped to improve the paper substantially.

References

1. Agence France-Presse (2011). South Korea to open cyber warfare school. http://gadgets.ndtv.com/others/news/south-korea-to-open-cyber-warfare-school-225865. Accessed 28 March 2014.

2. Agence France-Presse (2014). S. Korea detects suspected N. Korea hacking attempt. http://www.globalpost.com/dispatch/news/afp/140327/s-korea-detects-suspected-n-korea-hacking-attempt. Accessed 28 March 2014.

3. Alabaster, J. (2012). Japanese defense panel: cyber attacks can be basis for military self-defense. <http://www.pcworld.com/article/262010/japanese_defense_panel_cyber_attacks_can_be_basis_for_military_self_defense.html>. Accessed at 4 October 2013.

4. Arrirang News (2013). Defense Ministry to establish cyber policy department, www.arirang.co.kr/News/News_View.asp?nseq=145526. Accessed 28 March 2014.

5. bbc.com (2014). South Korea to develop Stuxnet-like cyberweapons. http://www.bbc.com/news/technology-26287527. Accessed 28 March 2014

6. Bechtol, B. E. (2013). South Korea: responding to the North Korean threat, American Enterprise Institute. http://www.aei.org/outlook/foreign-and-defense-policy/defense/south-korea-responding-to-the-north-korean-threat/. Accessed 28 March 2014.

7. beSUCCESS (2013). South Korea cyber security concerns go far beyond financial industry. http://e27.co/south-korea-cyber-security-concerns-go-far-beyond-financial-industry/. Accessed 28 March 2014.

8. Boyle, J. (2014). South Korea's strange cyberwar admission. 2 March http://www.bbc.com/news/world-asia-26330816. Accessed 28 March 2014.

9. Boynton, R. S. (2011). North Korea's digital underground, February 24, http://www.theatlantic.com/magazine/archive/2011/04/north-koreas-digital-underground/308414/. Accessed 28 March 2014.

10. businesskorea.co.kr (2013). Strengthened cyber security: Korea and US lay institutional foundation for cooperation in cyber security. http://www.businesskorea.co.kr/article/1601/strengthened-cyber-security-korea-and-us-lay-institutional-foundation-cooperation-cyber. Accessed 28 March 2014.

11. Chen, C., Ko, K., & Lee, J. (2010). North Korea's Internet strategy and its political implications, *The Pacific Review*, 23 (5), 649–670.

12. chosun.com (2011). Seoul's makeshift answer to N. *Korean Jamming Attacks*. http://english.chosun.com/site/data/html_dir/2011/09/23/2011092300630.html. Accessed 28 March 2014.

13. chosun.com (2013a). N. Korea 'confident' in cyber warfare capabilities. http://english.chosun.com/si, te/data/html_dir/2013/04/08/2013040801313.html. Accessed 28 March 2014.

14. chosun.com (2013b). KSTN. Korea boosting cyber warfare capabilities. http://english.chosun.com/site/data/html_dir/2013/11/05/2013110501790.html. Accessed 28 March 2014.

15. Clark, D. D., & Landau, S. (2011). Untangling attribution, *Harvard National Security Journal*, 2 (2), 25–40.

16. Clayton, M. (2013), In cyberarms race, North Korea emerging as a power, not a pushover. http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover. Accessed 28 March 2014.

17. Cobb, A. (1999). Electronic gallipoli? *Australian Journal of International Affairs* 53 (2):133–149.

18. Corbin, K. (2013). Iran is a more volatile cyber threat to U.S. than China or Russia, *CIO*, March 21, http://www.cio.com/article/2387362/government/iran-is-a-more-volatile-cyber-threat-to-u-s--than-china-or-russia.html. Accessed 28 March 2014.

19. Drennan, W. M. (2003). North Korea's non-military threats. *East Asia: An International Quarterly*, 20 (2), 48–59.

20. economist.com. (2010). War in the fifth domain: are the mouse and keyboard the new weapons of conflict? http://www.economist.com/node/16478792. Accessed 28 March 2014.

21. economist.com. (2011). North Korean computer hackers: black hats for hire. http://www.economist.com/blogs/banyan/2011/08/north-korean-computer-hackers. Accessed 28 March 2014.

22. Eun-jung, K. (2013). S. Korean military to prepare with U.S. for cyber warfare scenarios. http://english.yonhapnews.co.kr/national/2013/04/01/20/0301000000AEN20130401004000315F.HTML. Accessed 28 March 2014.

23. Eun-jung, K. (2014). S. Korea pushes to develop offensive cyber warfare tools, February 19, http://english.yonhapnews.co.kr/national/2014/02/19/3/0301000000AEN20140219003100315F.html. Accessed 28 March 2014.

24. Fildes, J. (2010). Stuxnet worm "targeted high-value Iranian assets". Retrieved from http://www.bbc.co.uk/news/technology-11388018. Accessed 28 March 2014.

25. Firn, M. (2013). North Korea builds online troll army of 3,000. http://www.telegraph.co.uk/news/worldnews/asia/northkorea/10239283/North-Korea-builds-online-troll-army-of-3000.html. Accessed 28 March 2014.

26. Fisher, M. (2013). North Korea may have secretly engineered computer games to launch mass cyber attack. http://www.washingtonpost.com/blogs/worldviews/wp/2013/10/23/north-

korea-may-have-secretly-engineered-popular-computer-games-to-launch-mass-cyber-attack/. Accessed 28 March 2014.

27. Gartzke, E. (2013). The myth of cyber war: bringing war in cyberspace back down to earth, *International Security*, 38 (2), 41–73.

28. globalpost.com. (2013), Damage from N.K. cyber attacks estimated at 860 bln won: lawmaker. http://www.globalpost.com/dispatch/news/yonhap-news-agency/131015/damage-nk-cyber-attacks-estimated-at-860-bln-won-lawmaker. Accessed 28 March 2014.

29. Greenwood, R., Hinings, C. R. (1993). Understanding strategic change: the contribution of archetypes. *Academy of Management Journal*, 36, 1052–1081.

30. Gross, G. (2013). Experts: Iran and North Korea are looming cyberthreats to U.S, *CIO*. March 20, 10. Accessed 28 March 2014. http://www.computerworld.com/s/article/9237759/Experts_Iran_and_North_Korea_are_looming_cyberthreats_to_U.S.

31. Habib, B. (2011). North Korea's nuclear weapons programme and the maintenance of the Songun system, *The Pacific Review*, 24 (1), 43–64.

32. Haveman, H. A. (1992). Between a rock and a hard place: organizational change and performance under conditions of fundamental environmental transformation. *Administrative Science Quarterly*, 37, 48–75.

33. Hern, A. (2013). North Korean 'cyber warfare' said to have cost South Korea £500 m. http://www.theguardian.com/world/2013/oct/16/north-korean-cyber-warfare-south-korea. Accessed 28 March 2014.

34. Hickey, W. (2012). Cyber war: North Korea is getting dangerously good at knocking out networks. http://www.businessinsider.com/cyber-war-north-korea-is-getting-dangerously-good-at-knocking-out-networks-2012-6. Accessed 28 March 2014.

35. Hirshleifer, J. (1998). The bioeconomic causes of war. *Managerial and Decision Economics*, 19 (7/8), 457–466.

36. Ho, S. (2004). Haven for hackers, *Foreign Policy*, November/December, 145.

37. Hudson, J. (2013a). A total cyber blackout in North Korea would affect about 1,000 citizens. http://blog.foreignpolicy.com/posts/2013/03/15/a_total_cyber_blackout_in_north_korea_would_affect_about_1000_citizens#sthash.oU9LzCvV.dpbs. Accessed 28 March 2014.

38. Hudson, J. (2013b). 7 things North Korea is really good at. http://www.foreignpolicy.com/articles/2013/04/29/7_things_north_korea_is_really_good_at#sthash.psVqvAU2.dpbs. Accessed 28 March 2014.

39. Kaempfer W.H., & Lowenberg, A.D. (1988). The theory of international economic sanctions: a public choice approach, *American Economic Review*, 78 (4),786-793.

40. Keck, Z. (2014). S. Korea seeks cyber weapons to target North Korea's nukes. http://thediplomat.com/2014/02/s-korea-seeks-cyber-weapons-to-target-north-koreas-nukes/. Accessed 28 March 2014

41. Kim, D. (2012). The Republic of Korea's counter-asymmetric strategy. *Naval War College Review*, 65 (1), 55–74

42. Koo, S. (2013). Cyber security in South Korea: the threat within. http://thediplomat.com/2013/08/cyber-security-in-south-korea-the-threat-within/. Accessed 28 March 2014.

43. koreaittimes.com (2013). Responses to cyber threats and future tasks—IPAK seminar, July 11th. http://www.koreaittimes.com/story/30252/responses-cyber-threats-and-future-tasks-%E2%80%93-ipak-seminar. Accessed 28 March 2014.

44. koreatimes.co.kr (2012). Korea, US mull regular cyber warfare drills. http://www.koreatimes.co.kr/www/news/nation/2013/07/205_119780.html. Accessed 28 March 2014

45. Kovacs, E. (2012). Navigation affected after North Korea launched GPS jamming attack. http://news.softpedia.com/news/Navigation-Affected-After-North-Korea-Launches-GPS-Jamming-Attack-268714.shtml. Accessed 28 March 2014.

46. Kshetri, N. (2005). ICTs, strategic asymmetry and national security, *Journal of International Management*, 11 (4), 563–580.

47. Kshetri, N. (2010). *The global cyber-crime industry: economic, institutional and strategic perspectives*, Springer-Verlag: Heidelberg.

48. Kshetri, N. (2013a). Reliability, validity, comparability and practical utility of cybercrime-related data, metrics, and information, *Information*, 4 (1), 117–123.

49. Kshetri, N. (2013b). *Cybercrime and Cybersecurity in the Global South*, Palgrave Macmillan: Houndmills, Basingstoke, U.K.

50. Kshetri, N. (2014). Japan's changing cyber security landscape, *IEEE Computer*, 47 (1), 83–86

51. Kwon, Y. (2011), Cyber-attacks add to North Korean arsenal. www.atimes.com/atimes/Korea/MC17Dg01.html Accessed 28 March 2014.

52. Kwony (2013). North Korea's vast cyber warfare army. http://cybersecurity.mit.edu/2013/09/north-koreas-vast-cyber-warfare-army/. Accessed 28 March 2014.

53. Lant, T. K., & Mezias, S. J. (1992). An organizational learning model of convergence and reorientation. *Organization Science*, 3, 47–71.

54. Lee, D. (2012). North Korea: On the net in world's most secretive nation. http://www.bbc.co.uk/news/technology-20445632. Accessed 28 March 2014.

55. Lee, Y. (2013). North Korea cyber warfare: hacking 'warriors' being trained in teams. http://www.huffingtonpost.com/2013/03/24/north-korea-cyber-warfare-warriors-trained-teams_n_2943907.html Accessed 28 March 2014.

56. Levitt, B., & March, J. G. (1988). Organizational learning. *Annual Review of Sociology*, 14, 319–340.CrossRef

57. MacKinnon, R. (2010). Hermit hackers. http://www.foreignpolicy.com/articles/2005/01/05/hermit_hackers. Accessed 28 March 2014.

58. Masters, J. (2011). Confronting the cyber threat, *Council on foreign relations.* http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577. Accessed 28 March 2014.

59. McGee, J. (2011). The difficulties of assessing North Korea's cyber strategy. https://csis.org/blog/difficulties-assessing-north-koreas-cyber-strategy. Accessed 28 March 2014.

60. McWilliams, B. (2003). North Korea's school for hackers. http://www.wired.com/politics/law/news/2003/06/59043?currentPage=all. Accessed 28 March 2014.

61. Metz, S. (2001). Strategic asymmetry, *Military Review*. July-August, 23–31.

62. Metz, S., & Johnson, D. V. II., (2001). *Asymmetry and U.S. military strategy: definition, background, and strategic concepts, Carlisle Barracks*, PA.: US Army War College, Strategic Studies Institute, January.

63. Miller, O. (2006). North Korea's hidden history. http://www.isj.org.uk/?id=166. Accessed 28 March 2014.

64. Minji, L. (2013). S. Korea to set up GPS jamming surveillance system. www.globalpost.com/dispatch/news/asianet/130410/s-korea-set-gps-jamming-surveillance-system. Accessed 28 March 2014.

65. Naylor, R. T. (2005). The rise and fall of the underground economy, *Brown Journal of World Affairs*, 11 (2), 131–143.

66. Newman, K. L. (2000). Organizational transformation during institutional upheaval. *Academy of Management Review*, 25, 602–619.

67. Olsen, K. (2009). South Korea websites under renewed attack: state official. http://www.huffingtonpost.com/2009/07/09/south-korea-websites-unde_n_228464.html. Accessed 28 March 2014.

68. Ong, R. (2008). South Korea and China's security objectives in East Asia, *Asia-Pacific Review*. 15 (2), 102–119

69. Panda, A. (2014). Pentagon North Korea report for 2013: unimpressive hardware, focus on cyber attacks. http://thediplomat.com/2014/03/pentagon-north-korea-report-for-2013-unimpressive-hardware-focus-on-cyber-attacks/. Accessed 28 March 2014.

70. Pfanner, E. (2013). Google jousts with wired South Korea over quirky Internet rules. http://www.nytimes.com/2013/10/14/business/international/google-jousts-with-south-koreas-piecemeal-internet-rules.html?_r=1&. Accessed 28 March 2014.

71. Raska, M. (2014). Cyberwars on the Korean Peninsula, 22 April, http://www.aljazeera.com/indepth/opinion/2014/04/cyberwars-korean-peninsula-2014422531782925.html. Accessed 28 March 2014.

72. Royle, T. (1990*). A dictionary of military quotations*, New York: Simon & Schuster.

73. Sang-ho, S. (2012). S. Korea strives to bolster cyber combat capabilities. http://www.koreaherald.com/common_prog/newsprint.php?ud=20120610000219&dt=2. Accessed 28 March 2014.

74. Sang-Hun, C. (2011). Seoul warns of latest North Korean threat: an army of online gaming hackers. http://www.nytimes.com/2011/08/05/world/asia/05korea.html?_r=4&. Accessed 28 March 2014.

75. Sang-Hun, C. (2013). South Korean officials accused of political meddling http://www.nytimes.com/2013/12/20/world/asia/south-korean-cyberwarfare-unit-accused-of-political-meddling.html. Accessed 28 March 2014.

76. Schearf, D. (2013). North Korea's 'world class' cyber attacks coming from China. http://www.voanews.com/content/north-koreas-world-class-cyber-attacks-coming-from-china/1795349.html. Accessed 28 March 2014.

77. Shackelford, S. J. (2009). From nuclear war to net war: analogizing cyber attacks in international law. *Berkeley Journal of International Law*, 27 (1), 192–251.

78. Tae-gyu, K. (2013). Spy agency ups capabilities against cyber attacks, *Korea Times*. www.koreatimes.co.kr/www/news/nation/2013/04/116_133851.html. Accessed 28 March 2014.

79. The Economist. (2008). Marching off to cyber war. 389 (8609), 20, December 8. http://www.economist.com/node/12673385. Accessed 28 March 2014.

80. Ulsch, M. (2013). The axis of cyber evil: a North Korean case of cyber espionage. http://www.hstoday.us/blogs/critical-issues-in-national-cybersecurity/blog/the-axis-of-cyber-evil-a-north-korean-case-of-cyber-espionage/3072be3aacf419cc494e3910a62107b2.html. Accessed 28 March 2014.

81. United Nations (2014). *National accounts main aggregate database*, http://unstats.un.org/unsd/snaama/resCountry.asp. Accessed 28 March 2014.

82. Vlahos, K. B. (2014). Special report: the cyber war threat from North Korea. http://www.foxnews.com/tech/2014/02/14/cyberwar-experts-question-north-korea-cyber-capabilities/. Accessed 28 March 2014.

83. Waterman, S. (2012). North Korean jamming of GPS shows system's weakness, *Washington Times*. www.washingtontimes.com/news/2012/aug/23/north-korean-jamming-gps-shows-systems-weakness. Accessed 28 March 2014.

84. Weick, K. E. (1979). *The social psychology of organizing* (2nd ed.). Reading: Addison-Wesley.

85. Yonhap, (2013). Seoul needs to counter N. Korea's cyber espionage capabilities: defense chief, www.globalpost.com/dispatch/news/yonhap-news-agency/130620/seoul-needs-counter-n-koreas-cyber-espionage-capabilities-de. Accessed 28 March 2014.

86. Yoon, S. (2011). North Korea recruits hackers at school, 20 June. http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html. Accessed 28 March 2014.

Footnotes

1. According to a defector from the Electronic Warfare Unit of the KPA, over 30,000 people in KPA may be engaged in cyber attacks against foreign targets (Yoon, 2011).

2. The first department focuses on gathering foreign intelligence and anti-communist, anti-terror, and anti-espionage efforts remain within the second department's purview.