Korea Economic Institute of America

ACADEMIC PAPER SERIES

KEI
KOREA ECONOMIC INSTITUTE OF AMERICA | 한미경제연구소

DECEMBER 2, 2014

North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance

By Dr. Alexandre Mansourov

ABSTRACT

Despite an inferior information communication environment, North Korea has a high capacity to conduct robust cyber operations aimed at collecting foreign intelligence, disrupting foreign computers, information and communication systems, networks and critical infrastructures, and stirring public discontent and disorder in the enemy states. The Korean People's Army concentrated its efforts on strengthening the cyber war capabilities through establishing a command and control structure dedicated to cyber warfare, forming military units specializing in cyber warfare, training expert manpower, and advancing research and development of core cyber technologies. North Korea critically depends on outside resources for the conduct of its offensive cyber effects operations.

The U.S.-ROK alliance managers often find their response options limited in the absence of a clearly identifiable North Korean government source of cyber operations. Washington and Seoul must strengthen their cooperation in cyberspace domain to deter North Korean cyber attacks and to promote the resilience of critical infrastructure, including the security of information and computer systems. The allies are well advised to learn the key lessons and operational concepts of Israel's Cyber Iron Dome. Seoul should be more discreet about its cyber offense plans because unwarranted publicity may undermine its cyber and military security and damage its moral and legal standings in the international community. The South should seek to expand cyber cooperation with China, in order to contain the North's cyber threats. Once the inter-Korean military-to-military dialogue is resumed, Seoul should attempt to engage Pyongyang in a cyber arms control discussion.

Keywords: *Cyber warfare, cyber warfare units, cyber bases, computer network operations, proxy wars*

Introduction

Since Kim Jong-il's designation of his son Kim Jong-un as his successor in January 2009, North Korea has come a long way to develop its own doctrine of cyber operations, build the military organizations tasked with the cyber warfare missions, procure the hardware and software required for cyber operations, train a corps of highly skilled professional cyber warriors, and develop operational plans for cyber warfare. Pyongyang demonstrated its cyber capabilities through the conduct of cyber warfare exercises and actual cyber operations aimed against what it considers its enemy states – the Republic of Korea, United States, and Japan. North Korea now has a credible cyber warfare capability threatening the world's advanced nations.

This study analyzes the evolution of the North Korean thinking on the policy dimensions of cyber warfare and cyber war: how the North Koreans define them, what they expect from them, what they believe about the uses and limits of power in cyber space, and how they perceive the utility and efficacy of cyber collection, offense, defense, and other types of operations.

The study also outlines a set of policy recommendations for the US-ROK alliance planners on how to deal with the growing threat of North Korea's cyber warfare capabilities. It is based on thorough research of the publicly accessible DPRK government-sponsored electronic media and Western open source materials.

North Korea Has Secure but Limited Cyberspace

Despite its technological backwardness, North Korea does have its own realm of computer networks in which the information is stored, shared, and communicated online. As everywhere else, North Korea's cyberspace comprises the computers that store

Dr. Alexandre Mansourov is an Adjunct Professor at the U.S.-Korea Institute at the Johns Hopkins University School for Advanced International Studies (SAIS). His paper is the seventy-second in KEI's Academic Paper Series. As part of this program, KEI commissions and distributes approximately ten papers per year on original subjects of current interest to over 5,000 Korea watchers, government officials, think tank experts, and scholars around the United States and the world. At the end of the year, these papers are compiled and published in KEI's On Korea volume. For more information, please visit **www.keia.org/aps_on_korea**.

Korea Economic Institute of America
1800 K Street, NW, Suite 1010
Washington, DC 20006
www.keia.org

digitized data and the systems and hardware that allow it to flow. In other words, North Korea has both its own virtual information environment and physical infrastructure including the domestic Internet of networked computers, closed intranets, cellular technologies, and fiber-optic cables. North Korea's cyberspace is constantly evolving because the technology and the people who use it are changing all the time, affecting the size and scale of cyberspace, its technical modalities and bureaucratic regulations governing it. Although the outward face of North Korea's cyberspace may look more or less the same today as it did three years ago, when half a dozen of its public-facing websites were introduced to the outside world, internally it is very different from its progenitors of 2011 or 2001.

In the past few years, North Korea installed millions of computers, routers, and servers in the government, industry, service sector, health and educational institutions, and the military, thanks to growing Chinese imports and domestic computer hardware manufacturing. Thousands of North Korean programmers develop indigenous mostly Linux-based software to run them. Millions of ordinary users now operate these machines inter-connected in one way or another on a daily basis. Local area networks and closed intranets are steadily proliferating.

The country's highly censored national intranet called the *Kwangmyong* ("Bright Star") Network runs through fiber optic cable with a backbone capacity of 2.5 gigabytes per second. Developed in 1996 with the goal of linking various research and academic institutions, the "Bright Star" Network now also includes government agencies, military units, corporate entities, and public access. Many PC cafés operate in Pyongyang and provincial capitals, providing public access to e-mail, internal websites, chat, online games, and streaming movies over a 100 megabit-per-second fiber optic link to the national intranet, which is policed by the Korea Computer Centre (KCC), North Korea's window on the worldwide web and its leading high-technology research and development hub. The KCC, set up in 1990, acts as the regime's gatekeeper, selecting only approved information and downloading it onto the Intranet. Content is mostly limited to science and technology, culture and arts, health and sports, and available only to selected government organizations, research institutes, universities, factories, and selective group of individuals.

Almost 2.5 million people (equal to ten percent of the total population) have cellular phones, using the mobile communications technology based on a 2100 Megahertz SMS-based standard 3G network called *Koryolink*, which is a joint venture between the DPRK Ministry of Posts and Telecommunications and Orascom. Although, at present, the government does not allow most users to have a data connection and use smart phones, according to Google CEO Eric Schmidt, who visited North Korea in January 2013, "it would be very easy for them to turn the Internet on for this 3G network."[1] Some privileged users vetted by the government already have the capability to access the nascent domestic web, using the locally assembled Android-based AS1201 *Arirang* smart phones.[2]

Today, North Korea remains by and large disconnected from the world wide web: this is the extreme case of the most restrictive cyber security policy in action. This ultimate firewall makes North Korea relatively secure in its cyber domain because it is virtually unplugged from the global Internet. Since North Korea's very restricted gateway to the world wide web is China, Beijing's "Great Firewall" offers an additional layer of protection, censorship and surveillance for North Korea's cyber space. In a way, North Korea has a "secure" model of the Internet designed primarily with security in mind, which solved the problems of anonymity and inability to limit access. The Kim regime was able to build a more "secure" section of the cyberspace, creating a domain of trusted networks inside the Internet.

As the country's digital transformation gains momentum, the Kim regime will be more pressed to revisit its current solution to the problem of securing the national cyberspace: unplug it. Although the relative isolation of North Korean cyberspace from the global Internet cannot guarantee absolute security, it helps the regime to maintain the confidentiality of digital data, the integrity of computer systems, and the availability and resilience of the information and communications infrastructure despite persistent security threats. It cost the government a lot of resources and time to build and sustain such a "secure, protected cyber zone." One wonders whether the Kim regime will ever feel politically secure and technically confident enough to take the leap of faith and plug the country into the world wide web. For if and when it does so, North Korea will be exposed to the same cyber threats as the rest of the world is facing today.

Difficulty in Assessing North Korea's Cyber Threat

To do a proper assessment of North Korea's cyber threat, one has to (1) evaluate to what extent the North Koreans are able to identify and exploit our vulnerabilities in cyberspace, (2) mea-

sure the effects if they were to take advantage of these vulnerabilities, and (3) estimate the likelihood that they will be willing to do so.

Obviously, it is very hard to do on all three accounts because of a high degree of uncertainty about our own vulnerabilities, the North's cyber capabilities, let alone their intentions in the cyber realm. Cyber operations in open and democratic societies are covered in many layers of secrecy because they are enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities. Once the vulnerabilities in hardware and software are uncovered and publicly discussed, they are quickly eradicated. This makes the analysis of cyber operations a daunting task. To analyze and understand cyber operations in closed and totalitarian societies like North Korea is even more challenging because of their isolation, total government control over publicly accessible information, dated nature of data, suspicious sourcing, culturally skewed perceptions, biased media coverage, selective redactions, and intentional denial and deception. The lack of objective information makes it problematic to have any serious public debate about the North's cyber capabilities and intentions, as well as the role of cyber power and cyber warfare in North Korea's national security.

Because very little is known about North Korea's cyber capabilities, weapons, and intentions, its cyber threat tends to be inflated. A tendency to play it safe emerges or an assumption of a worst-case scenario – a "Cyber Pearl Harbor" in Seoul or Tokyo. Fears of the unknown increase the risk of threat inflation dramatically. In particular, South Korean experts sound a great deal of alarm about Pyongyang's cyber warfare capabilities. In 2004, South Korea's Defense Security Commander General Song Yeong-geun asserted that North Korea's computer hacking capability was so outstanding that it was second only to that of the U.S. Central Intelligence Agency. In June 2012, the ROK Defense Security Commander Bae Deuk-shik agreed with the opinion that "North Korea is the world's third most powerful nation in cyber warfare after Russia and the United States."[3]

In contrast, U.S. analysts tend to disagree with such alarmist assessments of the North Korean cyber infrastructure and threat, but opinion ranges on its overall abilities. Citing the lack of hard evidence, James Lewis questions the efficacy of North Korean cyber warfare capabilities, arguing that Pyongyang has "strong interest and ragged, self-made technologies," but uses a lot of "bluster and exaggeration" to intimidate its enemies. In his judgment, "we have seen nothing from the North that could qualify as a cyber attack, cyber war, or as an act of cyber terrorism yet."[4] On the opposite, Frank Cilluffo, co-director of the Cyber Center for National and Economic Security at George Washington University, believes that North Korea's cyber capability constitutes "an important 'wild card' threat, not only to the United States but also to the region and broader international stability."[5] Echoing his view, Egle Murauskaite states that "the DPRK has successfully cross-purposed the cyber offensive tools at its disposal, utilizing data collection and system penetration of foreign targets in the public and private sector not only to exfiltrate information, but also to test adversaries' defenses, detection capabilities and their range of responses." In her opinion, "a cyber arsenal offers North Korea a cheaper way of developing global military reach, in contrast to the enormous political costs of its nuclear pursuits, and the price tag attached to WMD technology."[6] The authors of a recent HP report appear to take the middle road by admonishing that "we should not overestimate the regime's advanced cyber capability, yet we should never underestimate the potential impact of North Korea utilizing less advanced, quick-and-dirty tactics like DDoS to cripple their high-tech targets."[7]

> **"The U.S.-ROK alliance managers often find their response options limited in the absence of a clearly identifiable North Korean government source of cyber operations."**

Personally, this author is always skeptical about the source, intent, and scope of any cyber attacks publicly attributed to North Korea, recognizing the inherent uncertainties of cyberspace and limitations in our knowledge of what North Korea may or may not have, what it does, and why the regime does it. In cyberspace, many of the North Korean capabilities and intentions may be revealed only after a real attack takes place in the virtual domain, for which they will either claim responsibility or which will be undeniably traced back to the North Korean government or the non-state actors commissioned or controlled by Pyongyang. Do North Korea's cyber capabilities pose an advanced persistent threat to the U.S. and its allies in the region? It probably does, but it is a Herculean task to prove it.

Developing Indigenous Cyber War Doctrine

North Korea is still at the early stages of conceptualizing what cyber warfare will look like in the future. Careful reading of North Korea's authoritative media suggests that Pyongyang has recently begun to develop its own doctrine of cyber operations, which reflects its growing appreciation of the uses and limits of power in cyberspace and application of cyber power in modern warfare.

North Korean military theoreticians differentiate between cyber warfare (싸이버전) as one of the methods of the conduct of war and cyber war (싸이버 전쟁) as a way to affect the enemy's will and force him to do what one wants.[8] They distinguish cyber warfare (싸이버전) from traditional electronic warfare (EW) (전자전) and signals intelligence (SIGINT) (신호 정보). In their thinking, cyber warfare includes the elements of electronic intelligence warfare (전자정보전), computer network warfare (NW) (콤퓨터네트워크전), psychological warfare (심리전), military deception, and information warfare (IW) (정보전). A review of North Korean open sources indicates that media coverage of all of the above-mentioned forms of warfare increased considerably, starting from 2009. It is noteworthy that references to NW, IW, and PsyOps are now included in more general media reports on cyber warfare, indicating that cyber warfare probably encompasses these types of warfare.

In the 1990s, Kim Jong-il used to say that "modern warfare is electronic warfare" ("현대전은 전자전이다"). But, right after the war in Iraq, *Rodong Sinmun* – the official mouthpiece of the Korean Workers' Party – concluded that "In the end, Iraq disintegrated and collapsed helplessly by succumbing to a psychological warfare aimed at inspiring shock and awe, not due to the attacks by precision military equipment, as the United States publicizes."[9] On several occasions in the 2000s, Kim Jong-il reportedly told senior party and military cadres that information warfare would be the war of the 21st century and that the Korean People's Army (KPA) must learn and understand enemy military information technology and operations.

In contrast to his father's emphasis on information warfare, Kim Jong-un prefers to talk about cyber warfare. He reportedly believes that alongside nuclear weapons and missiles, cyber warfare capabilities are "a magic weapon" that empowers the Korean People's Army to launch "ruthless strikes" against the South.[10]

North Korean military strategists share the view that "cyber warfare has become a new form of warfare," but they apparently disagree in their assessment of its strategic importance: some assert that "cyber warfare replaces the traditional method of war,"[11] whereas others contend that it simply complements the kinetic methods of warfare. Some go as far as to speculate that the "third world war will be the global cyber war." They all designate cyberspace as the fifth major battlefield,[12] following sky, land, sea, and space.[13] They stress that cyberspace is its own medium with its own rules, and yet they struggle to define the uses and limits of power in cyberspace.

They recognize cyber war capability as a core military combat power,[14] but insist that the enemy does not have the right to retaliate for cyber attacks because of the technical complexity of determining the perpetrators of cyber operations.

Noteworthy is the fact that Pyongyang took particular issue with the U.S. Defense Department's announcement of "a cyber strategy of viewing hacker attacks from the outside as an act of war and responding by even using military force."[15] In July 2011, *Rodong Sinmun* slammed "a high-ranking DoD official who said that, should someone incapacitate the U.S. power network with a cyber attack, [the DoD] can attack the opposing country's industrial base with missiles."[16] It took notice of the U.S. Defense Science Board's assessment that "the cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War."[17]

The North Korean government took notice of the U.S. presidential policy directive No. 20 and its impact on the U.S. approach to cyber operations. In its commentary on 10 August 2013, the DPRK Cabinet newspaper *Minju Chosun* emphasized that "in the top-secret document 'PPD 20' the U.S. termed the cyber attack an indispensable capability to restrain and overthrow the enemy doing harm to the U.S. interests in times of peace and war. This means that the U.S. is ready to mount a fierce cyber attack on anyone going against the grain with it any moment."[18] Under such conditions, the United States is attempting to find a new pretext for military aggression and intervention in other countries," asserted *Rodong Sinmun*.[19]

North Korea's Cyber Threat Perceptions

North Korean official media highlighted six types of cyber threats facing the country: cyber crime, international hacktivism, international cyber terrorism, cyber defections, cyber espionage, and cyber warfare.

While North Korea often seeks to exploit cyber crime in South Korea, sometimes it falls victim to it. The high level of digitalization of South Korea's economy, society, and government makes it vulnerable to domestic cyber crime, including cyber hacking, identity theft, and malicious misinformation campaigns for personal, political, pecuniary, industrial espionage and other reasons. High cyber crime environment in the South makes it easier for the North to exploit it for the benefit of its own cyber operations and IW, but also exposes it to the risks of falling victim to sophisticated cyber criminals from the South, who often attack their targets in the ways designed to deceive the investigators and lead them to believe that the attack is coming from outside Korea. It also enables Seoul to surreptitiously conduct its own cyber operations and strategic misinformation campaigns designed to undermine the North's capabilities and interests and tarnish its image.

International hacktivism constitutes a major cyber concern for the DPRK government, which regards it as a tool of subversion and smear campaign in the hands of its enemy states. Ample evidence suggests that the DPRK government believes that most international hackers are employed or coerced into action by foreign governments, especially in the case of anti-North hackers.[20] Following the persistent cyber attacks against the North Korean government-run propaganda websites in late March and early April 2013 (up to 30,000 hacking attempts by some counts),[21] which coincided with the joint US-ROK military exercises, KCNA and *Minju Chosun* accused the South Korean government of employing "international hacker groups" in the "smear campaign against the DPRK" whereby they "intruded into Internet homepages of the DPRK, posted on them articles malignantly slandering the DPRK's dignity and stole and made public the list of subscribers."[22] In response to another round of cyber attacks on the eve of April 15, 2013, commemorating Kim Il-sung's birthday, the Secretariat of the Committee for the Peaceful Reunification of Korea (CPRK), North Korea's equivalent of the South's Ministry of Unification, repeated the accusation that the ROK government was behind the "international hackers' group" that attacked the DPRK's Internet websites, including China-based "Uriminzokkiri," and stole their subscribers' lists "in a bid to weaken the influences of the DPRK's Internet websites" and to flush out the "North's spies" and "those following the north"[23] and threatened merciless retaliation. On June 21, 2013, the North Korean government publicly accused the international hacking group "Anonymous" of waging repeated cyber attacks against DPRK targets, on the occasion of the 60th anniversary of the start of the Korean War on June 25.[24] While claiming that "Anonymous" has failed to achieve its political and technical objectives, Pyongyang branded it as an "international terrorist organization supported by the political forces hostile to the DPRK and funded by the U.S. and ROK intelligence services."[25] More recently, the Kim regime has taken notice of and condemned the "Hack North Korea" movement, which is sponsored by some of the wealthiest entrepreneurs in Silicon Valley and the Human Rights Foundation. The group is focused on finding new ways to get information in and out of the DPRK by bringing together North Korean defectors, international hackers, and human rights campaigners.

Regime survival is the paramount goal of the Kim family. Any cyber activity threatening the Kim regime is branded as cyber terrorism. In particular, the regime fears the introduction of the so-called "underground Internet" or "stealth Internet" which serves the purpose of "providing information for impure elements who concoct anti-government conspiracies in anti-imperialist, independent countries." [26] The DPRK government fears that through the underground Internet "the United States attempts to largely disseminate a US-style sense of values, bourgeois ideology and culture, and falsely fabricated materials, whereby it fosters social disturbance and political instability and instills the reactionary and tainted US-style ideology, culture, and way of life into people."[27] This is what constitutes "cyber terrorism" in North Korean propaganda, which condemns the ROK and U.S. authorities as the "real kingpins of cyber terrorism."[28]

The defection of Kim Heung-kwang, a former professor at the elitist Pyongyang Computer Technology University, who became a staunch advocate of the freedom of information and democratization of North Korea in his new capacity as the executive director of Seoul-based North Korea Intellectual Solidarity, highlighted the ever-present threat of cyber defections for the North Korean regime. In as much as the North Korean government strives to expand the ranks of cyber experts and warriors, it is worried about their loyalty and dependability. As the country's cyber capabilities grow, the more they know and the better their computer skills are, the more values they can compromise and the more damage they can do if they defect and turn against the regime. Hence, the growing importance of cyber counterintelligence.

The DPRK government regards cyber espionage as the clear and present danger to its state sovereignty and national security. Edward Snowden's revelations in summer 2013 presented Pyong-

yang with the opportunity to draw international attention to the fact that the U.S. National Security Agency reportedly monitored DPRK embassies and wire-tapped North Korean government communications all over the world,[29] attempted to infiltrate its telephone and computer networks, and eavesdropped on phone calls of North Korean citizens traveling abroad.[30] At the Third Committee of the 68th UN General Assembly, North Korea co-sponsored the German-Brazil-proposed resolution on the "Right to private life in IT era" designed to cope with the U.S. illegal eavesdropping, and, on November 26, 2013, the DPRK representative condemned U.S. electronic spying as "a wanton violation of the UN Charter because it is an infringement upon the sovereignty of states, intervention in the internal affairs of sovereign states, and the worst abuse of human rights."[31]

Establishing KPA Cyber Command

Pyongyang cyber experts observe that "many countries and military organizations are adopting cyber strategies in response to cyber war, spurring on the creation of cyber military headquarters and strengthening cyber war capabilities," according to *Minju Chosun*.

This author assesses that the KPA may have already established its own cyber warfare headquarters because of repeated references in North Korea's authoritative media to the creation of cyber military headquarters in various countries as a way to address new security challenges posed by the intensifying cyber arms race, escalating confrontation in cyberspace, and growing threat of outright cyber war,[32] as well as Korean Central News Agency (KCNA)'s tongue-in-cheek denial of the "misinformation" floating in the South that "the North operates a unit exclusively in charge of cyber warfare."[33] Pyongyang often uses a description of events in third countries and tongue-in-cheek refutations of the so-called "misinformation" or rumors in the South to signal its own position on or action in sensitive subjects.

In this author's judgment, the KPA Cyber Command (North Korean designator unknown) is probably not an independent service command on par with the KPA Army, Navy, Air and Anti-Air Forces, and Strategic Forces (formerly known as Strategic Rocket Forces). Nor is it a corps-level large combined unit under the Ministry of People's Armed Forces, as the North's media reporting would imply. But, it appears to be a division-level command unit subordinated to either the KPA General Reconnaissance Bureau, as it was speculated in some ROK and Western media reporting,[34,35] or to the Air and Anti-Air Command, as the North's uncharacteristically detailed description of the organizational evolution of the U.S. Cyber Command would imply.

Expanding KPA Cyber Unit Capabilities

According to South Korea's Defense Security Command (DSC), North Korea operates at least three cyber warfare units that specialize in hacking into South Korean and U.S. military computer networks, stealing classified information, and GPS jamming of ROK and USFK military communications.[36] KPA General Staff has been operating for years a 100-men strong "technology reconnaissance team" (a.k.a. Intelligence and Information Surveillance Unit) which is exclusively in charge of collecting information, establishing combat simulations, and disrupting military computer networks in South Korea and the U.S. [37] It also operates Enemy Attack Bureau No. 204, which is probably responsible for staging cyber attacks against ROK and Western targets.[38] The KPA Reconnaissance General Bureau operates Liaison Office No. 121, which may be responsible for KPA's GPS jamming operations.[39]

In addition, the State Security Department and WPK's Bureau 225 operate the specialized subunits responsible for the production of anti-South Korean multimedia content, which they disseminate among their operatives through the spy networks in China and Japan, according to *Chosun Ilbo*, South Korea's mainstream conservative daily.[40]

Training Cyber Warriors

Since the mid-1980s, the Korean People's Army has been reportedly engaged in systematic education and training of cyber war experts and operational officers for cyber operations. According to ROK government analysts, the number of cyber war experts in KPA has grown from approximately 100 in 2004[41] to 500-600 in 2009,[42] more than 3,000 in 2012,[43] and over 5,900 in mid-2014.[44]

The North Korean government selects talented children from students across the country and sends them for specialized training to computer classes at Kumsong No 1 Senior Middle School. Upon graduation, the best students are enrolled into Pyongyang University of Automation (formerly Mirim College), College of Information Science and Technology of Kim Ch'aek University of Technology, College of Computer Science of Kim Il Sung University, and Kim Hyŏng-gwŏn Military Academy of Communications Men, for advanced education in computer science and infor-

mation technology and training in sophisticated IT skills. Upon commencement, many of these graduates are recruited as cyber warfare officers of the IW units under the Ministry of People's Armed Forces or placed as communications officers in battalion-level military units.[45]

According to ROK media, Pyongyang University of Automation in Hyŏngjesan district is a five-year military university specializing in computer science, electronic information transmission, and code development.[46,47] It offers such programs as electronic warfare research, cyber warfare research, military IT system development, computer-based command and control systems, and information intelligence. According to ROK media, Kim Hyŏnggwŏn Military Academy of Communications Men in Hamhung is a three-year military academy training commanding officers in the field of military communications and electronic warfare.[48]

Key research institutes involved in developing core concepts and technologies for cyber operations for the KPA are reported to be Kusŏng Electronic Warfare Institute under KPA General Staff (R&D of EW concepts, methods, and equipment), Kanggye Institute (R&D on military electronics and guidance systems) and Research Institute No. 110 (R&D on cyber warfare capabilities), both under the Second Academy of Natural Sciences. Moreover, the December 1 Research Institute for Computer Programmer Training under the North's Ministry of Electronics Industry is probably responsible for training the computer hacker personnel who eventually may form the ranks of the so-called "patriotic hackers" or "cyber militia" in the ranks of the Worker-Peasant Red Guards.

Developing Core Cyber Technologies to Conduct Cyber Operations

The Korean People's Army reportedly prepares for a future cyber war of rather long duration by investigating expert hacking techniques and studying plans to paralyze the computerized networks of South Korea, United States, and Japan, as well as by developing software for disrupting the command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems of its major adversaries, according to the U.S. Army's Asian Studies Detachment (ASD). The KPA IW unit seeks "to gain control of South Korean and U.S. military information system by hacking into their computer networks and taking out classified data. When necessary, they may spread computer viruses to disrupt the networks."[49] The North Korean unit has also set up simulated cyber war training software and collected extensive data via "spyware" emails and various phishing schemes on USFK and South Korean high-ranking military personnel.[50]

The academic articles written by North Korean scientists—along with other research on network intrusion detection systems (NIDS) published in the DPRK—illustrate the DPRK's high level of interest in, and in the understanding of, hacking methods. For instance, the Kim Il Sung University Journal, *Natural Sciences*, published a number of scholarly articles by North Korean software programmers which illustrated their familiarity with hacking tools, network intrusion detection systems, and Defense Advanced Research Project Agency (DARPA)-sponsored research on the issue. In a December 2006 article published in *Natural Sciences* called "A Method to Improve Detection Rate in the Intrusion Detection by Neural Networks," the authors listed the following attack groups: Denial of Service (DOS),[51] User to Root (U2R),[52] Remote to User (R2L),[53] Probing (Prob)/Surveillance,[54] and Data Attacks.[55] In a May 2008 article titled "A Method of the Parameter Selection for Detection of the Portscan Attacks," the North Korean researchers mentioned the following eight types of widely used computer network attacks/tools, which they label "attack tool programs": Nmap,[56] Guest,[57] Back, Dict,[58] Portsweep,[59] Lpsweep, Satan,[60] and Nessus.[61] Although it was not clear whether they actually used any of the eight attacks/tools in their research, they appear to have a very good understanding of the features and applications of the attacks/tools listed above.

The North has reportedly employed social engineering techniques for collecting on enemy states' militaries by taking advantage of "even a single percent of a loophole" and penetrating the human error of administrators, according to Dr. Kim Heungkwang, former professor of North Korea's Pyongyang College of Computer Science and now head of Seoul-based NK Intellectuals Solidarity. He explains, "North Korean hackers' main duty is to steal Internet protocols (IP), and it is a piece of cake for hacker unit members to hack the ROK military's Internet because they usually hack using the IPs from third countries, such as China and Japan."[62]

In 2011, North Korea revealed a particular interest in the technology the U.S. uses to build what it calls the "underground Internet" or "stealth Internet" not only because it wants to block it since it is designed "to provide information for impure elements who concoct anti-government conspiracies in anti-imperialist, independent countries," [63] but also because it can be instrumental in Pyongyang's own attempts "to break down the Internet

firewalls of other countries" (in particular, South Korea) and "to foster social disturbance and political instability and instill North Korean style ideology, culture, and way of life into the minds of the South Korean people."[64]

Exploiting Outside Resources to Conduct Cyber War

Given its backward information communication infrastructure, North Korea critically depends on outside resources for conducting cyber operations. The KPA may be using servers in a number of foreign countries on several continents for misattribution in conducting cyber operations, according to various streams of reporting. Pyongyang may also be involved in supply chain technical penetrations through its work in microelectronic circuit development and production.

North Korea runs forward cyber bases in China that conduct DDoS attacks against ROK websites, according to multiple reports from Western media. According to South Korea's Defense Security Command (DSC), most attacks by North Korean hackers take place via China, which has also been suspected of attempting to extract information from South Korean government computers.[65] At the seventh conference on the protection of national defense intelligence, hosted by the ROK Defense Security Command in mid-June 2009, the DSC estimated that South Korea's defense networks were attacked on average 95,000 times per day, with eleven percent of the attacks being "sophisticated attempts to extract military intelligence," while the rest being relatively easier to head off.[66] Hacking attempts amounted to 10,450 cases: 81,700 spread of viruses; 950 "denial-of-service (DoS)" attacks causing abnormal traffic; and 1,900 falsification of Internet homepages.[67]

According to ROK government sources, approximately 30 DPRK-affiliated software development companies in Dalian, China, work as subcontractors to produce China's logic bombs. A logic bomb is a cyber weapon that is installed as a program when making personal computer software, so it is more certain than a virus, and easier. The logic bomb is a cyber penetration to collect, monitor, or disrupt a host computer system. South Korea suspects that computer software and hardware originating in Dalian would be technically compromised.

According to *Seoul Daily* citing ROK intelligence authorities, North Korea has also been using South American-based servers since January 2009 to misattribute hacking activities, as well as routing through U.S. servers, to target the ROK and USFK.[68] E-mails with hidden hacking programs have been sent to ROK and USFK military generals and major ranking officials since January 2009. According to ROK military officials, "It is not easy to track these emails because they route via servers of third countries, but they are presumed to be acts of North Korean hackers." The hacking programs hidden in e-mails were designed to pilfer personal information and documents.

Finally, it is plausible to assume that North Korea may be active in the international cyber black market, including the cyber arms black market and cyber "zero-day" vulnerabilities market in which transnational criminal groups buy and sell specialized cyber capabilities. Also, Pyongyang may be scouting for foreign cyber talent to conduct cyber operations.

Challenges for the US-ROK Alliance

Stepping Up Cyber Deterrence

The attribution challenge renders classic deterrence strategies feeble in cyberspace. The U.S.-ROK alliance managers often find their response options limited in the absence of a clearly identifiable North Korean government source of cyber operations. Yet, it is beyond doubt that today North Korea conducts hostile cyber operations against the U.S.-ROK and U.S.-Japan alliances. The problem of "who" to deter and retaliate against in cyberspace is made even more difficult by a plethora of non-state actors who operate in the cyber environment, pursuing both their independent agendas and acting in support for North or South Korea and their allied states and their policy objectives. Often they act as proxies for these states. But, automatically presuming state sponsorship for non-state cyber operations can be misleading even in the case of North Korea.

A missile has a return address, a computer code does not. Sophisticated cyber warriors hide their tracks whereas users of kinetic weapons could not care less. It takes a lot of time and resources to do the cyber forensics and identify the source of a cyber attack, but even then the answer is rarely definitive. Thus, South Korea must do much more to strengthen its capability to improve attribution or, at least, to convince the international community that it has developed much better ways and means to pinpoint the real source of cyber attacks. Greater information sharing and dedicated public-private partnerships between the ROK's key government stakeholders and leading computer security firms may help to not only speed up tracing an attack, but also finding out who was operating a specific computer and his/her political agenda.

In addition to valid and reliable identification, another critical component of cyber deterrence is the commitment to retaliate in order to influence the enemy's calculations. A dilemma whether to match or escalate the use of force does not have easy answers. Judging by their public statements, the North Koreans already fear that in retaliation, the allies may not stop at proportionate cyber response and, instead, may go beyond the cyber realm to ensure the escalation dominance through the use of a mixture of cyber force and real-world kinetic force to put the North's hard assets at risk. In a way, U.S. official statements and forceful approach to cyber warfare may have already succeeded in reshaping what KPA cyber strategists think and deterring North Korea's most egregious offensive cyber operations.

Of particular importance is the growing realization in Washington and Seoul that they must strengthen their cooperation in the cyberspace domain to deter North Korean cyber attacks and to promote the resilience of critical infrastructure, including the security of information and computer systems. In this light, in 2012, the allies established the Cyber Cooperation Working Group which endeavors to strengthen cooperation in information sharing, cyber policy, strategy, doctrine, personnel, and exercise to improve their collective readiness against cyber threats. They held the second ROK-U.S. Cyber Policy Consultations in Washington D.C. in July 2013 and signed the initial Terms of References for the Cyber Cooperation Working Group on September 5, 2013.

But, to put real teeth into cyber deterrence and make their threat of overwhelming retaliation against North Korea's cyber attacks truly credible, Seoul and Washington may be well advised to study the latest cyber defense policy innovation at NATO and its possible applicability to the 1953 U.S.-ROK mutual defense treaty. On September 5, 2014, NATO leaders agreed that a large-scale cyber attack on a member country could be considered an attack on the entire U.S.-led alliance, potentially triggering a military response. The decision marks an expansion of the organization's mission, reflecting new threats that can disable critical infrastructure, financial systems and government without firing a shot. "Today we declare that cyber defense is part of NATO's core task of collective defense," NATO Secretary General Anders Fogh Rasmussen told a news conference.[69]

As NATO recognizes that cyber defense is part of NATO's core task of collective defense, the new policy confirms that NATO member states are able to invoke Article 5 of the North Atlantic Treaty on collective self-defense in case of a cyber attack with effects comparable to those of a traditional armed attack.[70] According to Jamie Shea, Deputy Assistant Secretary General for Emerging Security Challenges at NATO Headquarters, the policy does not set any detailed criteria for the activation of Article 5 which would have to be decided by the Allies on a case-by-case basis.[71] The U.S. and ROK should at least watch closely how this new mutual defense commitment will play out in practice.

"The Kim regime regards cyber warfare as an integral part of the asymmetric warfare aimed at bridging the growing gap in military capabilities, which exists between the DPRK and its enemies today."

Fortifying Cyber Defense

The Kim regime regards cyber warfare as an integral part of the asymmetric warfare aimed at bridging the growing gap in military capabilities, which exists between the DPRK and its enemies today. Since in cyberspace, the weak may have the advantage over the strong, cyberspace gives North Korea, the country with no critical infrastructure connected to the Internet, the kind of power over its much bigger and cyber-savvy adversaries that it could never dream of in the pre-digital age. South Korea, which is one of the most wired nations in the world, has countless vulnerabilities that a cyber-dwarf like North Korea can exploit to harm everything—from its civilian computer networks, communications, and data to critical infrastructure and military networks. South Korea's traditional strengths prove to be its cyber vulnerabilities. In cyberspace, power diffusion can potentially lead to power equalization.

North Korean cyber strategists appear to share the common assumption that cyber offense has the advantage over cyber defense. It stems from their general belief in the "cult of the offensive" and some pragmatic calculations. It is cheaper and easier to attack computer systems than to detect the cyber attacks and defend against them. Besides, they can choose the time and place of their attacks, whereas the defender must be ready to defend his or her assets everywhere.

That said, one of the recent trends in cybersecurity has been the re-evaluation of the importance of cyber defense in the offense-

defense balance. More and more cyber security experts come to the conclusion that "the best defense is actually a good defense." They recommend any and all measures that could help build up the resistance against cyber attacks and strengthen the resilience of systems and organizations by tightening the network security, employing common cyber defense tactics and techniques including firewalls, encryption, air gaps, and even hackbacks, and improving cyber forensics to track back attackers.

ROK defense planners recognize the growing complexity of cyber threats emanating from North Korea. Following a massive attack against the websites of South Korean government agencies in 2010, the ROK defense ministry established a 400-member Cyber Warfare Command to enhance the nation's cyber warfare capabilities. More recently, in a report to the National Assembly in October 2013, the ROK Joint Chiefs of Staff (JCS) said that it updated its contingency plan to classify North Korea's cyber threat as a "non-military provocation" and decided to establish in 2014 the Cyber Warfare Center (CWC) under the JCS, which is supposed to serve as the "control tower for cyber warfare missions," to protect military networks from the North's hacking attempts.[72] Although the specific missions of the JCS CWC remain unclear, it appears that the JCS's cyber team will be tasked with mainly protecting the military networks and will not have an offensive or defensive role in cyber warfare. It is good that the new unit will be required to share information with the related agencies, including the defense ministry's Cyber Warfare Command and the ROK National Intelligence Service, although it remains to be seen whether all these units will be able to develop smooth and effective inter-agency coordination. In addition, as Michael Raska, Research Fellow of S. Rajaratnam School of International Studies, Nanyang Technological University, recommends, the South Korean government should not hesitate to "engage the finest cyber professionals and team them up with strategic and defense experts, creating partnerships with cyber security firms to share commercial information and educate cyber personnel."[73]

If ROK government planners were serious about preventing the DPRK-inflicted Cyber Pearl Harbor, they should learn the lessons and methodology of and closely study the applicability of the operational concepts of Israel's Cyber Iron Dome. According to Michael Raska, "Israel is developing 'a national cyber defensive envelope' – a multi-layered cyber defense strategy leveraging automated computerized systems and highly-trained personnel that provide intelligence, early warning, passive and active defense, and offensive capabilities across civil-military networks."[74] Bearing in mind Marcus Noland's cautionary observation that "there are limitations to the applicability of Israeli lessons to the Korean case,"[75] South Koreans will be well advised to seriously examine the possible applications of the Iron Dome missile defense methodology in the cyber domain, especially its emphasis on the establishment and operation of the complete kill chain, including enemy analysis, passive detection, target list generation, early warning, active defense, overwhelming strike effort, area suppression, command and control, and, hopefully, cyber deterrence.

Preparing for Computer Network Attacks

Computer network operations (CNO) are the integral part of the U.S.-ROK planning, organization, preparation, and execution of cyber warfare. Although much of the allied CNOs are shrouded in secrecy, their aim is to "destroy, deny, degrade, disrupt and deceive" while defending against the enemy's persistent malicious cyber activity. It is plausible to assume that in accordance with the Presidential Policy Directive No. 20 on the U.S. Cyber Operations Policy issued in October 2012, they are engaged in the full spectrum of cyber operations from cyber collection to defensive cyber effects operations (DCEO) to offensive cyber effects operations (OCEO) against North Korean targets. In other words, they gather information about KPA cyber warfare capabilities, seek to infiltrate KPA C4 networks and identify their vulnerabilities, and contemplate to deploy their offensive cyber weapons aimed at North Korean assets even before the kinetic battle begins, establishing the conditions for both emergency cyber actions and the so-called "cyber operations with significant consequences."

Operation Orchard is an example of successful "computer network operations" including the cyber collection effort followed up by the offensive cyber effects operation with a kinetic outcome. First, the United States and Israel were able to exploit the inadequate computer security of a key Syrian WMD official to discover and trace North Korean involvement in the Syrian nuclear program in general and the construction of the Al Kibar nuclear facility in particular. Then, the allies succeeded in penetrating the Syrian military's computer networks, directing their own data streams into its air defense networks and effectively misleading Syrian radars and turning off its air defenses at the time of the Israeli air raid leveling the Al Khibar nuclear facility on September 6, 2007.[76]

Although originally the ROK Cyber Defense Command put a much greater emphasis on psychological warfare operations against Pyongyang's propaganda and slandering in cyberspace, in February 2014, the ROK Ministry of National Defense (MND) unveiled a revised long-term cyber warfare strategy, which out-

lined the vision for the expansion of comprehensive cyber warfare missions and called for the development of offensive cyber weapons like Stuxnet, a computer virus that damaged Iran's uranium enrichment facility, in order to cripple North Korea's missile and nuclear facilities, according to Yonhap.[77] The new strategy also called for augmenting the nation's EIW capabilities in order to suppress the origins of cyber attacks and for setting up a task force in charge of conducting war exercises.[78]

In October 2014, the ROK MND reiterated its new cyber operations posture favoring cyber offense. According to Yonhap, whereas in the past, the ROK military was preoccupied with the monitoring-based operations to deter the North's hacking attempts, now its cyber units are tasked with proactively detecting the hosts of such attacks online and launching preemptive strikes to prevent them from striking at the South from the outset.[79] Bearing in mind the rapid growth of mobile telecommunications networks in the North, the South also plans to expand the scope of its cyber operations to cover mobile and all types of online-based equipment, according to Yonhap.

ROK government pronouncements make it clear that the Cyber Defense Command will strive to damage the North's ability to build nuclear weapons by targeting its facilities for enriching uranium and reprocessing plutonium, and it will attempt to disrupt the KPA's ability to launch a nuclear-tipped ICBM at the time of crisis. This author agrees with Zachary Keck's assessment that "even simply delaying North Korea's ability to launch a nuclear missile could be crucial when paired with South Korea's evolving precision-strike capabilities, which could be used to preemptively destroy these facilities before a nuclear attack could be launched."[80] In this sense, the ROK's shift to cyber offense could be part of an asymmetric warfare strategy aimed at using non-nuclear means to preemptively destroy DPRK's nuclear arms.

That said, Seoul's unprecedented public admission of its intended cyber targets raised eyebrows among many foreign observers, who understood that it was driven by the considerations of cyber deterrence but questioned its wisdom on legal, political, and military grounds.[81] Because the South's announcement was the statement of official intent, the North now claims that it has the right to preemptively strike any ROK facilities and units that are involved in preparations of a potential cyber attack against the DPRK on the basis of the anticipatory self-defense – the same legal argument the United States used to justify its war on terror. Some scholars believe that the use of Stuxnet malware during Operation "Olympic Games" represents an unlawful use of force, and, therefore, the threat to use a similar weapon is also unlawful. Others fear that the North may react in a wildly disproportionate and indiscriminate way, going beyond what one might consider the legitimate targets in a cyber war and striking not only at the military personnel responsible for launching the virus, but also at the software developers working for private companies who help develop the virus, as well as the communications networks used to transmit information about the virus, etc. One should keep in mind that in retaliation for the Stuxnet attack, Iran launched cyber attacks against U.S. financial institutions (Operation Ababil) and deployed the Shamoon malware against Saudi Arabia's national oil company, Saudi Aramco, and Qatar's RasGas.

It is a worthwhile objective to try to compromise the enemy's weapons systems and military industrial facilities, especially if one can "persuade" them to do the opposite of what their owners intended. Moreover, if such attacks succeed, they can have a debilitating psychological impact on the minds of the users of the computer networks under attack, who may start doubting any information coming from the computers. Such offensive cyber operations may not only cause destruction and loss of life in the enemy camp, but also may open up new possibilities in disruption of the enemy's operations, co-optation of its weapons platforms and industrial systems, and "persuasion" of the enemy forces. However, all these objectives must be kept secret. In my judgment, the ROK government's public announcement about its cyber offense designs went too far in its explicit details; it is unlikely to enhance South Korea's cyber security and probably will undermine the nation's military security and moral and legal standings in the international community.

Waging Proxy Wars in Cyber Space

Pyongyang is very adept at waging proxy wars in cyber space. It often employs private citizens and non-state actors of other countries to do its bidding. Often, it is very hard to attribute the conduct of these individuals and groups to the North Korean state because it is difficult to ascertain that they are either acting "on the instructions" of that state or acting under its "direction or control."[82]

For instance, North Korean patriotic hackers based in China and disguised as Chinese citizens are known to disseminate pro-North propaganda praising the Kim Jong-un regime and anti-South propaganda slandering the ROK government and its policies in cyberspace. Last year, they posted over 14,000 comments praising North Korea on Facebook, Twitter and YouTube. They also post malicious comments on all sorts of publications related to

South Korea on Chinese websites and on China's social networking sites including Weibo, according to ROK daily *Chosun Ilbo*.[83] But, it is a real challenge to prove that they receive their orders from the North or that the North Korean government provides them with cyber weapons or other technical support or that the United Front Department of the Workers Party of Korea Central Committee (WPK CC) directly controls their activities. Obviously, Pyongyang has never acknowledged or adopted their conduct as its own, which could have served as an additional basis for attribution of a non-state actor's cyber operations, according to the evolving international law of attribution.[84]

South Korea should clearly articulate its position on the matter whenever it can establish that the North has resorted to a proxy to conduct harmful cyber operations; otherwise, Pyongyang will interpret silence as acquiescence. In addition, pursuant to the law of state responsibility, the South may be justified to demand reparations or pursue countermeasures if it succeeds in ascertaining that Pyongyang either instructed the actors to mount the cyber operations or exercised effective control over them.

Furthermore, Seoul should seek to expand cyber cooperation with China, the North's biggest benefactor. As Martin Libicki, noting the importance of tackling fast-growing cyber threats from Pyongyang, pointed out, "The best leverage that South Korea might offer would have to work through China—convincing China that the risks of a North Korean collapse are tolerable compared to all the other risks that might exist from not tamping down on North Korea"[85]

Advocating Cyber Arms Control and Confidence Building Measures in Cyber Space

Although current policies of the two Koreas are not conducive to any dialogue or cooperation on the peninsula, resumption of inter-Korean collaboration in the future may open the possibility for promoting cyber peace. At present, neither the South nor the North is interested in cyber disarmament or even cyber détente. They do not have the capacity to disrupt or regulate international cyber weapons trade. Each country is left to its own ways and means to deal with growing cyber threats.

But, once inter-Korean dialogue is reopened, and the two militaries resume their contacts, Seoul should engage Pyongyang in a cyber arms control discussion, focusing initially on common terms and definitions. Hopefully, the two Koreas will be able to come up with some shared understandings that they can use to create new norms to shape each other's cyber behavior in the future. A viable inter-Korean cyber weapons treaty may not be possible, but such cyber dialogue might be able to serve as a useful mechanism to clear some fog in cyberspace and lower cyber tensions on the peninsula.

Appendix 1. List of High Profile Cyber Attacks Attributed to North Korea

Date	Target	Type of Attack	Resources Employed
From May 19 to September 16, 2014[86,87]	Approximately 20,000 smartphones in ROK	Installation of malicious smartphone apps enabling eavesdropping and clandestine videotaping	NK hackers deployed malware disguised in mobile gaming apps on ROK websites for free downloading
June 25, 2013[88]	ROK Ministry of Unification, The Sejong Institute, Korea Institute for Defense Analyses, Hyundai Merchant Marine, and the ROK organizations belonging to "The supporters of Korean Unification" (http://www.unihope.kr/)	The "Kimsuky" Operation: cyber espionage, using the early stage malware most often delivered by spear-phishing e-mails	Korean compilers alongside Bulgarian e-mail command-and-control communications
June 9, 2012	ROK *JoongAng* Daily	DDoS	n.a.
April 12, 2011[89,90]	ROK National Agricultural Cooperatives Federation (Nonghyup)	DDoS	300,000 zombie PCs
January 17, 2011[91]	Website of Free North Korea Radio	DDoS	Direct NK attack without using a proxy server as a punishment for ROK's hacking of NK website "Uriminzokkiri" on January 8-9, 2011[92,93]

Date	Target	Type of Attack	Resources Employed
March 3, 4 (10:00 a.m. and 6:30 p.m.) and March 5 (10:45 a.m.), 2011[94,95,96,97]	30 ROK government agencies and financial institutions, including ROK Blue House, MND, NIS, National Assembly	The DDoS attack reportedly came from all the computers connected to the zombie PCs executing game programs provided by the illegal game sites whose servers were based in China.[98]	30 overseas servers in 18 countries (including U.S., Russia, Italy, Mexico, Israel, and Hong Kong) ordering 34,000 zombie PCs in ROK and 100,000 PCs abroad to carry out DDoS attacks[99]
July 7, 2010 (6:00 p.m.)[100]	ROK Blue House, MOFA, Korea Exchange Bank, Naver	DDoS	Smaller scale than in July 2009
July 7, 2009 (6:50 p.m.)[101]	26 U.S. and ROK websites, including those of the U.S. White House, U.S. treasury, U.S. Secret Service, Blue House, ROK MND, ROK National Assembly, Sinhan Bank, Korea Exchange Bank	DDoS[102]	442 overseas servers ordering attacks[103] to some 12,000 PCs in ROK and 8,000 PCs abroad
March 5, 2007[104]	Third Army Command and Center for Chemical Safety Management under ROK National Institute of Environmental Research	By stealing the [user] certificate password that enables the Third Army Command to enter the National Institute of Environmental Research's Center for Chemical Safety Management under the Ministry of Environment, the North Korean hacker unit stole the information in the "Chemical Accident Response Information System" (CARIS), including data on around 700 enterprises and organizations that manufacture toxic chemical substances, and the information on around 1,350 types of toxic chemical substances and [information on] weather.	
April-June 2004[105]	A total of 314 PCs were hacked, including 235 servers at national institutions, including Korea Coast Guard, National Assembly, Korea Atomic Energy Research Institute, Korea Institute for Defense Analyses, Agency for Defense Development, Air Force University, [former] Ministry of Maritime Affairs and Fisheries, Small and Medium Business Administration, and Education Center for Unification, and 79 servers at enterprises and universities.	DDoS	Hundreds of PCs in China

Endnotes

[1] Eric Schmidt' blog, *Google Plus*, 20 January 2013, https://plus.google.com/+EricSchmidt/posts/UZnAUzpszHX

[2] Dave Lee, "North Korea 'makes home-grown' Arirang smartphone," *BBC News*, 13 August 2013, http://www.bbc.co.uk/news/technology-23681261#sa-ns_mchannel=rss&ns_source=PublicRSS20-sa.

[3] AFP, Hong Kong in English, 0536 GMT 07, June 2012.

[4] James Lewis, "Speak Loudly and Carry a Small Stick: The North Korean Cyber Menace," *38 North*, 7 September 2010, http://38north.org/2010/09/speak-loudly-and-carry-a-small-stick-the-north-korean-cyber-menace/.

[5] Mark Clayton, "In cyberarms race, North Korea emerging as a power, not a pushover," *The Christian Science Monitor*, 19 October 2013, http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover.

[6] Egle Murauskaite, "North Korea's Cyber Capabilities: Deterrence and Stability in a Changing Strategic Environment," *38 North*, 12 September 2014, http://38north.org/2014/09/emurauskaite091214/.

[7] "Profiling an enigma: The mystery of North Korea's cyber threat landscape," HP Security Briefing Episode 16, *HP Security Research*, August 2014, http://h30499.www3.hp.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf.

[8] A well-known U.S. cyber strategist Martin Libicki distinguishes cyber warfare from cyber war. In his thinking, "cyber warfare, like warfare itself, is about the conduct of war, carried out inevitably to further the performance of combat in the physical domain (it can also be considered operational or instrumental cyber war). Cyber war is undertaken to affect the will of the adversary directly (it can also be considered tantamount to strategic cyber war)." See "Why Cyber War Will Not and Should Not Have Its Grand Strategist," Martin C. Linicki, *Strategic Studies Quarterly*, Spring 2014, p. 29.

[9] Kim Nam-hyŏk, "Let Us Heighten Vigilance Against the US Imperialists' Psychological Strategic Warfare -- The 'Shock and Awe' Operation the United States Perpetrated in Iraq," *Rodong Sinmun* (in Korean), 4 July 2003, p. 6.

[10] "N. Korea Boosting Cyber Warfare Capabilities," *Chosun Ilbo*, 5 November 2013, http://english.chosun.com/site/data/html_dir/2013/11/05/2013110501790.html.

[11] Ri Ok-chu, "Cyberspace Appears as New Battlefield," *Minju Joson* (electronic edition, in Korean), 19 July 2011.

[12] Full text of press statement by a spokesperson for the Ministry of the People's Armed Forces under the DPRK National Defense Commission: "Bad Habit of Finding Fault With Others Must Be Relinquished." *Pyongyang Korean Central Broadcasting Station* (in Korean), 0811 GMT, 10 May 2011.

[13] Cho Sŏng-ch'ŏl, "An Impure Conspiracy Seen on 'Underground Internet,'" *Rodong Sinmun* (electronic edition, in Korean), 25 July 2011.

[14] Ri Ok-chu, "Cyberspace Appears as New Battlefield," *Minju Joson* (electronic edition, in Korean), 19 July 2011.

[15] Ra Myŏng-sŏng, "Cyber Warfare That Draws International Concerns," *Rodong Sinmun* (electronic edition, in Korean), 29 September 2011.

[16] Cho Sŏng-ch'ŏl, "An Impure Conspiracy Seen on 'Underground Internet,'" *Rodong Sinmun* (electronic edition, in Korean), 25 July 2011.

[17] "Resilient Military Systems and the Advanced Cyber Threat," *Defense Science Board*, Washington: Department of Defense, January 2013, ES-1.

[18] "민주조선 미국의 싸이버공격전략의 엄중성을 폭로"("Minju Joson Exposes Danger of U.S. Cyber Attack Strategy"), KCNA, 10 August 2013, http://www.kcna.co.jp/calendar/2013/08/08-10/2013-0810-007.html.

[19] Ra Myŏng-sŏng, "Cyber Warfare That Draws International Concerns," *Rodong Sinmun* (electronic edition, in Korean), 29 September 2011.

[20] Cho Sŏng-ch'ŏl, "An Impure Conspiracy Seen on 'Underground Internet,'" *Rodong Sinmun* (electronic edition, in Korean), 25 July 2011.

[21] "North Korea Ramps Up Cybersecurity," *Korea Real Time*, 3 June 2014, http://blogs.wsj.com/korearealtime/2014/06/03/north-korea-ramps-up-cybersecurity/?mg=blogs-wsj&url=http%253A%252F%252Fblogs.wsj.com%252Fkorearealtime%252F2014%252F06%252F03%252Fnorth-korea-ramps-up-cybersecurity.

[22] "S. Korea Accused of Plotting to Stamp Out Progressive Forces," *KCNA*, 11 April 2013.

[23] "CPRK Secretariat Blasts S. Korea for Cyber-attack on DPRK's Websites," *KCNA*, 20 April 2013.

[24] "조선중앙통신사 론평《어나니머스》싸이버공격은 망상" (KCNA Commentary Terms Int'l Hackers' Plot Barking of Rabid Dogs), *KCNA*, 21 June 2013, http://www.kcna.co.jp/calendar/2013/06/06-21/2013-0621-028.html.

[25] Ibid.

[26] Cho Sŏng-ch'ŏl, "An Impure Conspiracy Seen on 'Underground Internet,'" *Rodong Sinmun* (electronic edition, in Korean), 25 July 2011.

[27] Ibid.

[28] "S. Korean Authorities' Anti-DPRK Racket Slammed," *KCNA*, 16 August 2011.

[29] "What Snowden Incident Shows?" *Rodong Sinmun* (electronic edition, in Korean), 6 July 2013, http://www.rodong.rep.kp/en/index.php?strPageID=SF01_02_01&newsID=2013-07-06-0016&chAction=T.

[30] Ri Hak-nam, "No Real Friend for U.S.," *Rodong Sinmun* (electronic edition, in Korean), 16 July 2013, http://www.rodong.rep.kp/en/index.php?strPageID=SF01_02_01&newsID=2013-07-16-0008&chAction=T.

[31] "DPRK Delegate Clarifies Principled Stand on U.S. Electronic Espionage," *KCNA*, 30 November 2014.

[32] "Minju Chosun Discloses Danger of U.S. Cyber Strategy," *KCNA*, 13 June 2012.

[33] "S. Korean Puppets' Move to Participate in U.S.-led Cyber Storm Exercises Blasted," *KCNA* (in English), 1125 GMT, 27 June 2009.

[34] "ROK's Intelligence Agency Says Group or State Behind Cyber Attacks," Yonhap (in English), 0629 GMT, 8 July 2009.

[35] "North Korea Increases Cyber War Personnel by Doubling it: Report," *SPAMfighter News*, 14 July 2014, http://www.spamfighter.com/News-19077-North-Korea-Increases-Cyber-War-Personnel-by-Doubling-it-Report.htm.

[36] "ROK's Intelligence Agency Says Group or State Behind Cyber Attacks," Yonhap (in English), 0629 GMT, 8 July 2009.

[37] "ROK's Intelligence Agency Says Group or State Behind Cyber Attacks," Yonhap (in English), 0629 GMT, 8 July 2009.

[38] "Organization Chart of KPA Cyber IW and Cooperative Organizations," Seoul: ROK Ministry of National Defense, May 2006.

[39] Hyŏn Kŏn, "Kim Cho'ng-u'n [Kim Jong Un] Is Behind North Korea's Electronic Warfare," *Yo'llin Pukhan Pangsong* (in Korean) 0212 GMT, 8 March 2011.

[40] "N. Korea Boosting Cyber Warfare Capabilities," *Chosun Ilbo*, November 5, 2013, http://english.chosun.com/site/data/html_dir/2013/11/05/2013110501790.html.

[41] Ko Sŏng-p'yo, "There Is a 'CIA-Class' Hacker Group in North Korea's Ministry of People's Armed Forces -- The World Is Currently at Cyber War," *JoongAng Ilbo Online* (in Korean), 20 April 2009.

[42] Ko Sŏng-p'yo, "There Is a 'CIA-Class' Hacker Group in North Korea's Ministry of People's Armed Forces -- The World Is Currently at Cyber War," *JoongAng Ilbo Online* (in Korean), 20 April 2009.

[43] Hong Kong *AFP* (in English), 0536 GMT, 7 June 2012.

[44] "North Korea Increases Cyber War Personnel by Doubling it," Yonhap, 14 July 2014, http://www.spamfighter.com/News-19077-North-Korea-Increases-Cyber-War-Personnel-by-Doubling-it-Report.htm.

[45] Ko Sŏng-p'yo, "There Is a 'CIA-Class' Hacker Group in North Korea's Ministry of People's Armed Forces -- The World Is Currently at Cyber War," *JoongAng Ilbo Online* (in Korean), 20 April 2009.

[46] "평양 자동화 대학, 최고두뇌 뽑아 전자전 장교 육성," *Donga Ilbo*, Seoul, 29 April 2001, http://news.donga.com/3/all/20010429/7682787/1.

[47] "北, 해킹부대 통해 남한정보 수집"…기무사 첫확인, *Donga Ilbo*, Seoul, 27 May 2004, http://hanbitkorea.com/technote7/board.php?board=freeboard&page=71&sort=hit&command=body&no=1909.

[48] "김정일총비서 김형권통신병군관학교시찰," *KCNA*, Pyongyang, 17 November 1998, http://www.kcna.co.jp/item2/1998/9811/news11/17.htm.

[49] "ROK's Intelligence Agency Says Group or State Behind Cyber Attacks," Yonhap (in English), 0629 GMT, 8 July 2009.

[50] An Tong-hwan, "North Korean Hackers Distribute Hacking Mails Targeting Generals of [ROK] Military and US Forces in Korea," *Seoul Sinmun Online* (in Korean), 17 June 2009.

[51] DOS is a class of attacks where an attacker causes a computing or memory resource to be too busy or full to handle legitimate requests. The result is that legitimate users access to a computer system is denied (e.g., Syn-flood).

[52] U2R exploits are a class of attacks whereby an attacker starts out with access to a normal user account on the system and is able to exploit vulnerability to gain root access to that system—that is, the attacker gains unauthorized access to local super user (root) privileges (e.g., various "buffer overflow" attacks).

[53] R2L attack is a class of attacks where an attacker sends "packets" to a target computer over a network and exploits a target machine's vulnerability to illegally gain local access as a user—that is, an attacker gains unauthorized access from a remote machine (e.g., guessing password).

[54] Prob is a class of attacks whereby an attacker scans a computer network to gather information or find known vulnerabilities, in order to survey and to conduct other probing (e.g., port scanning).

[55] Data Attacks involve someone—user or administrator—performing some action that is unauthorized on a given computer system. Often, these attacks involve transferring "secret" data files to or from sources where they do not belong (e.g., secret).

[56] Nmap is a general-purpose network-scanning tool that discovers hosts and services on a computer network.

[57] The Guest attack is a variant of the Dict attack. On badly configured systems, guest accounts are often left with no password or with an easy to guess password. Because most operating systems ship with the guest account activated by default, this is one of the first and simplest vulnerabilities an attacker will attempt to exploit.

[58] This is an attack where an intruder uses a program that tries every possible word in the dictionary. Dictionary attacks can be done either by repeatedly logging into systems or by collecting encrypted passwords and attempting to find a match by similarly encrypting all the passwords in the dictionary. Intruders usually use an English-language dictionary as well as foreign language dictionaries for this purpose.

[59] These are probing attacks that conduct a surveillance sweep to determine which hosts are listening on a network.

[60] Satan is a Security Administrator Tool for Analyzing Networks that gathers as much information about remote hosts and networks as possible.

[61] Nessus is a network vulnerability assessment tool that detects potential vulnerabilities on a computer network.

[62] O Tong-yong, "Military Internet Network, Vastly Penetrated by DPRK Hacking Unit -- Exclusively Obtains 'Details of CARIS Leakage to North Korea' Drafted by Diplomacy and Security Policy Office of the [ROK] Prime Minister's Office," *Monthly Chosun* (in Korean), 1 November 2009, pp 62-69.

[63] Cho Sŏng-ch'ŏl, "An Impure Conspiracy Seen on 'Underground Internet,'" *Rodong Sinmun* (electronic edition, in Korean), 25 July 2011.

[64] Ibid.

[65] "ROK's Intelligence Agency Says Group or State Behind Cyber Attacks," Yonhap (in English), 0629 GMT, 8 July 2009.

[66] Ibid.

[67] An Tong-hwan, "North Korean Hackers Distribute Hacking Mails Targeting Generals of [ROK] Military and US Forces in Korea," *Seoul Sinmun Online* (in Korean), 17 June 2009.

[68] Ibid.

[69] "NATO agrees cyberattack could trigger military response," *Reuters*, September 5, 2014, http://www.cnbc.com/id/101974720.

[70] Steve Jordan, "NATO updates cyber defense policy as digital attacks become a standard part of conflict," *ZDNet*, 30 June 2014, http://www.zdnet.com/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict-7000031064/.

[71] "NATO Summit to Update Cyber Defense Policy," *International Cyber Developments Review (INCYDER)*, 2014 Q2, https://www.ccdcoe.org/sites/default/files/publications/articles/INCYDER%202014Q2.pdf.

[72] Kim Eun-jung, "S. Korean military to launch cyber warfare center next year," Yonhap, October 22, 2013, http://english.yonhapnews.co.kr/full/2013/10/22/46/1200000000AEN20131022004200315F.html.

[73] "North Korea Increases Cyber War Personnel by Doubling it: Report," *SPAMfighter News*, 14 July 2014, http://www.spamfighter.com/News-19077-North-Korea-Increases-Cyber-War-Personnel-by-Doubling-it-Report.htm.

[74] Michael Raska, "Building A Cyber Iron Dome: Israel's Cyber Defensive Envelope – Analysis," *Eurasia Review*, October 2, 2014, http://www.eurasiareview.com/02102014-building-cyber-iron-dome-israels-cyber-defensive-envelope-analysis/?utm_source=getresponse&utm_medium=email&utm_campaign=rsis_publications&utm_content=RSIS+Fortnightly+Summary+%28Issue+88%29.

[75] Marcus Noland, "Iron Cyber Dome?," Peterson Institute for International Economics, October 15, 2014, http://blogs.piie.com/nk/?p=13548.

[76] P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), pp. 126-129.

[77] Kim Eun-jung, "S. Korea pushes to develop offensive cyberwarfare tools,", Yonhap, February 19, 2014, http://www.globalpost.com/dispatch/news/yonhap-news-agency/140218/s-korea-pushes-develop-offensive-cyberwarfare-tools.

[78] Ibid.

[79] "S. Korea to get proactive in cyber warfare," Yonhap, October 8, 2014, http://english.yonhapnews.co.kr/full/2014/10/08/82/1200000000AEN20141008011400315F.html.

[80] Zachary Keck, "S. Korea Seeks Cyber Weapons to Target North Korea's Nukes," *The Diplomat*, February 21, 2014, http://thediplomat.com/2014/02/s-korea-seeks-cyber-weapons-to-target-north-koreas-nukes/.

[81] Joe Boyle, "South Korea's strange cyberwar admission," *BBC News*, March 2, 2014, http://www.bbc.co.uk/news/world-asia-26330816.

[82] M. Schmitt and L. Vihul, "Proxy Wars in Cyberspace. The Evolving International Law of Attribution," *Fletcher Security Review*, Vol. I, Issue II, 2014, p 55-73, http://media.wix.com/ugd/c28a64_2fdf4e7945e9455cb8f8548c9d328ebe.pdf.

[83] "N. Korean Agents Badmouth S. Korea in Chinese Cyberspace," *Chosun Ilbo*, November 27, 2013, http://english.chosun.com/site/data/html_dir/2013/11/27/2013112701629.html.

[84] M. Schmitt and L. Vihul, "Proxy Wars in Cyberspace. The Evolving International Law of Attribution," *Fletcher Security Review*, Vol. I, Issue II, 2014, p 55-73, http://media.wix.com/ugd/c28a64_2fdf4e7945e9455cb8f8548c9d328ebe.pdf.

[85] "N.K. cyber aggression has no parallel," *The Korea Herald*, 20 July 2014, http://www.koreaherald.com/view.php?ud=20140720000130.

[86] "N. Korea Hacks 20,000 S.Korean Smartphones," *Chosun Ilbo*, 29 October 2014, http://english.chosun.com/site/data/html_dir/2014/10/29/2014102901755.html

[87] "South Korea Spy Agency Says North Hacking Smartphones," AFP, 29 October 2014, http://www.securityweek.com/south-korea-spy-agency-says-north-hacking-smartphones

[88] Dmitry Tarakanov, "The "Kimsuky" Operation: A North Korean APT?" *SecureList*, 11 September 2013, http://securelist.com/analysis/57915/the-kimsuky-operation-a-north-korean-apt/.

[89] "Will S. Korea Refer NK`s Hacking of Nonghyup to UN?," *Dong-A Ilbo Online* (in English), 0029 GMT, 5 May 2011.

[90] Full text of press statement by a spokesperson for the Ministry of the People's Armed Forces under the DPRK National Defense Commission: "Bad Habit of Finding Fault With Others Must Be Relinquished," *Korean Central Broadcasting Station* (in Korean), 0811 GMT, 10 May 2011.

[91] Kim Ŭn-ho, "Pyongyang Directly Accesses Free North Korea Radio Website," *Free North Korea (FNK) Radio* (in Korean), 18 January 2011.

[92] "True Character of Hacking Crime Which Is Being Exposed With Each Passing Day," Article by reporter Kim Ch'ŏl-hyŏk, Pyongyang *Uriminjokkkiri* in Korean, 11 January 2011

[93] U Min-il, "Foolish Rash Act of Trying To Blur the Image of Our Home Page," *Uriminjokkkiri* (in Korean), 11 January 2011.

[94] "Zombie Computers in DDoS Attack Begin To Destroy Own Hard Drives," Yonhap (in English), 1414 GMT, 6 March 2011.

[95] On Chong-rim, "North Korean Figure, '[North Korea] Beat South Korea With 100,000 Zombie Computers,'" *NewDaily* (in Korean), 0045 GMT, 7 March 2011.

[96] "S. Korean Web Sites Hit By New DDoS Attack, No Damages Reported," Yonhap (in English), 0620 GMT, 5 March 2011.

[97] "South Korea hit by cyber attacks," *BBC*, 4 March 2011, http://www.bbc.co.uk/news/technology-12646052.

[98] On Chong-rim, "North Korean Figure, '[North Korea] Beat South Korea With 100,000 Zombie Computers,'" *NewDaily* (in Korean), 0045 GMT, 7 March 2011.

[99] "S. Korean Web Sites Hit By New DDoS Attack, No Damages Reported," Yonhap (in English), 0620 GMT, 5 March 2011.

[100] "Fresh Cyber Attack Marks Anniversary of Hacking Disaster," *Chosun Ilbo Online* (in English), 0348 GMT, 8 July 2010.

[101] Sam Kim, "S Korea's Intelligence Agency Says Group Behind Cyber Attacks" Yonhap (in English), 0629 GMT, 8 July 2009.

[102] DDoS are the so-called distributed denial-of-service attacks that involve hacking into personal computers and using them to jam Web sites by increasing data traffic beyond their capacity.

[103] "S. Korean Web Sites Hit By New DDoS Attack, No Damages Reported," Yonhap (in English), 0620 GMT, 5 March 2011.

[104] O Tong-yong, "Military Internet Network, Vastly Penetrated by DPRK Hacking Unit -- Exclusively Obtains 'Details of CARIS Leakage to North Korea' Drafted by Diplomacy and Security Policy Office of the [ROK] Prime Minister's Office," *Monthly Chosun* (in Korean), 1 November 2009, pp 62-69.

[105] Ko Sŏng-p'yo, "There Is a 'CIA-Class' Hacker Group in North Korea's Ministry of People's Armed Forces -- The World Is Currently at Cyber War," *JoongAng Ilbo Online* (in Korean), 20 April 2009.

KEI Editorial Board

KEI Editor: Nicholas Hamisevicz | **Contract Editor:** Gimga Group | **Design:** Gimga Group

The Korea Economic Institute of America (KEI) is a not-for-profit policy and educational outreach organization focused on promoting dialogue and understanding between the United States and Korea. Established in 1982, KEI covers all aspects of the alliance, including economic, trade, national security, and broader regional issues through publications, forums, and conferences across North America. KEI is an affiliate with the Korea Institute for International Economic Policy, a public research institute in the Republic of Korea.

The views expressed in this publication are those of the authors. While this paper is part of the overall program of the Korea Economic Institute of America endorsed by its Officers, Board of Directors, and Advisory Council, its contents do not necessarily reflect the views of individual members of the Board or of the Advisory Council.

Printed in the United States of America.

KEI KOREA ECONOMIC INSTITUTE OF AMERICA | 한미경제연구소
1800 K St. NW, Suite 1010 | Washington, DC 20006
T.202.464.1982 | F.202.464.1987 | www.keia.org