International Journal of Korean Unification Studies
Vol. 21, No. 2, 2012, 85–106

Cyber War and Policy Suggestions for South Korean Planners

Hyeong-Wook Boo & Kang-Kyu Lee

This paper aims to answer fundamental questions on cyber warfare. Conflicting perspectives regarding cyber war are introduced, and the critical issues of cyber deterrence and cyber security strategy are discussed. Then, they are followed by an assessment of North Korea's cyber warfare capabilities, which are main security concerns in South Korea. Finally, the authors will suggest the future direction of cyber war preparations for the South Korean Armed Forces. The authors argue that currently, the most viable agenda is focusing on defensive measures and using non-military assets, initiating cooperation with other domestic instruments or enhancing cooperation with other nations. This is attributed to the fact that kinetic countermeasures against North Korea's cyber attacks will not be effective from the perspective of the military's cost-effective analysis. Moreover, it may trigger an all-out war. Indeed, the use of armed forces against cyber attacks is still a controversial issue in the international community.

Key Words: cyber war, kinetic countermeasures, cyber security strategy, cyber deterrence, cyber threat

Introduction

Following the development of information and communication technology (ICT), cyber attacks against societal infrastructures can cause catastrophic effects on the people's everyday lives. It is especially true for a society that is heavily dependent on ICT. Many countries define cyberspace as the fifth domain of war in an effort to address the increasingly elaborate infiltration techniques used against various platforms and networks. In the case of the U.S., many people are becoming concerned about a potential "electronic Pearl Harbor attack."

The South Korean government is also apprehensive about North Korea's cyber threats and has adopted several policy measures against them.

In the meantime, recent developments in cyber security debates have raised critical questions. Is the cyber war approach appropriate in addressing cyberspace issues when non-military concepts can be used to manage cyber security?[1] Which theoretical approach is appropriate in addressing cyberspace and cyber war issues at this point? If South Korea adopts the cyber war approach, then has it carefully considered strategic issues, such as cyber deterrence? Does South Korea have the capability to face North Korean cyber threats?

This paper aims to seek answers to these fundamental questions. Then, they will be followed by an assessment of North Korea's cyber war capabilities, which are the main cyber security concerns in South Korea. Finally, policy suggestions regarding the future direction of the South Korean Armed Forces' cyber war preparations will follow.

Perspectives on Cyberspace and Cyber War

IR Theories and Cyberspace

Before diving into a full-blown discussion on cyber war, there is a need to think about what cyberspace is. However, defining cyberspace is not an easy task because of its characteristics; it is a newly emerging, intangible and evolving space.[2] An interesting aspect is that there are several different approaches to cyberspace even though people still

1. In general, cyber security against cyber threat has three pillars: cyber crime, cyber terrorism and cyber war. In this article, we will concentrate on discussing cyber war.
2. Sheldon (2011) suggests that the main characteristics of cyberspace are a reliance on the electromagnetic spectrum, the need to allow man-made objects to exit, the ability to be constantly replicated, relatively cheap entry costs and so on. John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly* (Summer 2011), pp. 95-112.

struggle to define it.[3] Cho (2012) categorizes two different approaches to cyberspace: the liberal approach vs. the realist approach.[4] Based on this categorization, Deibert (2010),[5] Nye (2011),[6] Singer & Schactman (2011)[7] represent the liberal approach while Clarke & Knake (2010)[8] and many planners in the Pentagon are realists.

The classification is mainly based on the traditional theories of international relations and extends their arguments into cyberspace. In addition, the approaches to cyberspace from the two schools of thought are based on assumptions of the real world.[9] To liberals,

---

3. Tabansky (2011) argues that cyberspace consists of the physical layer, software layer and data layer. Given those three layers, he defines cyberspace as "interconnected networks of information technology infrastructures, including the internet, telecommunication networks, mission-specific networks, computers and computer-embedded systems." Lior Tabansky, "Basic Concepts in Cyber Warfare," *Military and Strategic Affairs*, Vol. 3, No. 1 (May 2011), pp. 75-92.
4. Hyun-Suk Cho, "Cyber Security in the Era of Big Data," unpublished material, Seoul National University of Technology (January 2012).
5. Ronald Deibert, "Militarizing Cyberspace," *Technological Review* (MIT, 2010), http://www.technologyreview.com/notebook/419458/militarizing-cyberspace, accessed on May 4, 2012.
6. Joseph S. Nye, Jr., "Power and National Security in Cyberspace," in Kristin M. Lord and Travis Sharp (eds.), *America's Cyber Future: Security and Prosperity in the Information Age* (Vol. II) (Washington, DC: Center for a New American Security, 2011), pp. 5-23.
7. Peter W. Singer and Noah Schactman, "The Wrong War: The Insistence on Applying Cold War Metaphors to Cyber Security Is Misplaced and Counterproductive," Brookings Institute (August 2011), http://www.brookings.edu/research/articles/2011/08/15-cybersecurity-singer-shachtman, accessed on May 4, 2012.
8. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010).
9. As common knowledge, the realists, including neo-realists, generally assume that: 1) the state is the primary and unitary rational actor, 2) the state is always expanding its national interest, 3) the core values of the state are power and security, and security means national security and 4) the international system is essentially anarchy and the states act to secure their survival. On the other hand, liberals, including neo-liberals, endorse the core propositions in which: 1) the state is an important actor, but it is not the only actor and there are many non-state actors, including international organizations and individuals and 2)

cyberspace is more akin to an open sea, while realists perceive it as a territory of sovereign states. Liberals consider the virtual world and the real world as irrelevant, whereas realists regard it as an extraterritorial site of real world power. As a result, Manjikian (2010) compared the liberal view on cyberspace to a global village and the realist view to a virtual battle space.[10] From the realist perspective, cyberspace is an "avenue for insurgents and national enemies to penetrate 'real' defenses."

Thus, it is reasonable that scholars have different perceptions of cyber war. Liberals argue that realists have a tendency to make attempts at nationalizing or militarizing cyberspace issues. In this context, liberals like Deibert (2010) bitterly criticize the realist approach, and it is somewhat provocative. The following is highlight of his argument:

> … many of the heralds of cyber war have a commercial stake in the cyber security market. Some may have more ulterior motives for ramping up fears, such as a desire to fan the flames of Sino-American rivalry or to diminish privacy on the Internet.[11]

The arguments from the two sides appear to be irreconcilable.[12] Moreover, neither side can establish a satisfying explanation of cyberspace and cyber war even though both emphasize cyberspace and cyber

---

they agree that the world system is anarchy, but they also believe that cooperation among actors can be achieved, even in the anarchy.

10. Mary McEvoy Manjikian, "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik," *International Studies Quarterly*, Vol. 54, Issue 2 (June 2010), pp. 381-401.
11. Ronald Deibert, "Militarizing Cyberspace."
12. Singer & Schactman (2011) of Brookings wrote that "...there is a massive amount of threat inflation going on in Washington's discussion of online dangers, most frequently by those with political or profit motives in hyping the threats. It's a new version of the old 'missile gap' hysteria." Peter W. Singer and Noah Schactman, "The Wrong War: The Insistence on Applying Cold War Metaphors to Cyber Security Is Misplaced and Counterproductive." Nye (2011) wrote "… narrower definition of cyber actions that have effects outside cyberspace that amplify or are equivalent to kinetic violence," Joseph S. Nye, Jr., "Power and National Security in Cyberspace."

war as a new challenge or threat to security.

Infinite Problems to Cyber War and a Pragmatic Approach

As discussed above, there are at least two conflicting views on cyber security strategy: the liberal perspective and the realist perspective. Although cyber security strategy must be grounded on specific technology and environmental differences, the realist approach to cyber security strategy is similar to that of nuclear deterrence. Many liberal scholars have warned that it can potentially be risky to apply Cold War metaphors to cyber security. Solomon (2011) insists that a probable strategy is cyber deterrence, but it should not simply adopt methods for nuclear deterrence.[13]

With regard to the differences between cyber deterrence and nuclear deterrence, Libicki's (2009) argument is quite convincing.[14] He claims that there are intrinsic problems in waging cyber war. First, an issue of recrimination; tracing cyber terrorists in a wired society is a very difficult task. One can launch a cyber attack anywhere in the world without leaving physical evidence. However, recrimination is not an issue in the case of nuclear war. Second, the prospect of damages cannot be guaranteed in cyber war; that is, it is not certain if real cyber attacks can bring about similar damages to those caused by *in vivo* tests. However, the prospects of damage are quite clear in the case of nuclear war. Third, the possibility of a repeated cyber attack; in the case of cyber attacks, there is no guarantee that a repeated attack can be as powerful as the first since the defending side's ability

13. Jonathan Solomon, "Cyber Deterrence between Nation-States: Plausible Strategy or a Pipe Dream?" *Strategic Studies Quarterly* (Spring 2011), pp. 1-25. On the other hand, James C. Mulvenon and Gregory J. Rattray (2012) claim that the ineffectiveness of cyber deterrence is due to the instability of cyberspace. James C. Mulvenon and Gregory J. Rattray (eds.), *Addressing Cyber Instability* (Executive Summary), Cyber Conflict Studies Association, 2012, http://www.cyberconflict.org/storage/CCSA%20-%20Addressing%20Cyber%20Instability.pdf, accessed on November 23, 2012.

14. Martin C. Libicki, *Cyber Deterrence and Cyber War* (RAND, 2009), http://www.rand.org/pubs/monographs/MG877.html.

to respond can make the difference. Fourth, there is the possibility of countering attacks through retaliation; however, cyber attacks are so cheap that one can launch attack anywhere with negligible costs. Thus, one cannot guarantee that retaliation will disarm the attackers, while nuclear retaliation guarantees that the attackers will be disarmed. Fifth, there is a third party issue; with the issue of recrimination, there are several potential opportunities to engage a third party in cyberspace. Since a third party often provides cyber infrastructure, this does not become an issue in nuclear war. Sixth, there is a risk of escalation; actions in cyberspace may spill over to real world conflicts. Seventh, there is the issue of thresholds; unlike a nuclear attack, it is very difficult to set a clear benchmark for cyber attack under which a state can find justifiable reasons to retaliate. Lastly, this is a liability issue; there are so many privately owned cyber infrastructures that publicly manifested and state-initiated retaliations may send the wrong messages to private companies. As a consequence, cyber attacks may result in lower liability due to the lack of investments in security.

Considering all these differences, waging cyber warfare may result in complicated problems. One example is that the ambiguous nature of recrimination causes a state suffering from cyber attacks to hesitate from launching a physical counterattack as retaliation. Then, what if a state launches a cyber attack with a traditionally armed attack? Many strategists argue that the cyber attacks also constitute as an act of war. What about incidents in which cyber attacks can cause physical damages to a state, including human casualties or extensive social turmoil? Many strategists argue that this can also be regarded as an act of war. However, the perception that cyber war is warfare in the fifth domain can be problematic. Cyber warfare should be held in a different regard than other warfare in the land, sea, air or space. That is, these four domains have emerged in the battlefield with the development of technology and instruments, so the domains have already been in existence. However, cyber warfare is conducted in cyberspace where everything has been newly created by the technological advancement. In this regard, people argue that cyber warfare is qualitatively different from the warfare in other domains. Thus, a

qualitatively different approach may be necessary in addressing cyber war. However, that has yet to be fully established in the field of strategic studies as well as the practice of waging cyber war.

Meanwhile, it is important to remember that there have been several unsettled arguments and competing approaches to cyber war and cyberspace. Indeed, analysts have been encountered theoretical conundrums, since every perspective has its own rationale. Also, such theoretical discussions have fallen behind reality. Analysts believe that this should be regarded seriously because cyberspace is still evolving and they have yet to develop an all-encompassing theory. Eriksson and Giacomello (2006) argue that there is a need to narrow the gap between the theory and practices of cyberspace issues.[15] They suggest adopting a "pragmatic approach." Since analysts believe that a pragmatic approach enables countries to adopt substantive measures for its national interests, they must first narrow the gap between theory and practice. The pursuit of theoretical adaptations, such as applying existing IR theories to cyberspace, will be the next step. Finally, they can exert our efforts in synthesizing theories and practices. Thus, an examination of cyber attacks will be an ideal starting point for a pragmatic approach. In the next section, we will review some cases of cyber attacks.

Recent Developments in Cyber Security

Cases of Cyber Attacks

Notable examples regarding cyber attacks include: (1) the cyber attack against the Iranian nuclear program in June 2009, (2) the Russian virus used to infiltrate into classified U.S. military networks in November 2008, (3) a brief cyber war between Georgia and Russia in

15. Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security and International Relations: (IR)relevant Theory?" *International Political Science Review*, Vol. 27, No. 3 (July 2006), pp. 221-244.

Table 1. Major Cyber Attack Cases

Cases	Estonia (2007)	Georgia (2008)	Iran (2009)
Actors	Individuals, organized crime, state support	Individuals, organized crime, state support/ involvement	State
Vectors	Botnet, simple technologies (inexpensive)	Botnet, simple technologies (inexpensive), military operations	Stuxnet, advanced technologies, significant financial support
Objectives	Government, media, banks, industrial websites	Government, media, banks, industrial websites	Nuclear facility, CII (critical information infrastructure)
Impacts	Increasing ethnic conflicts, strengthening NATO cyber security cooperation	Short-term operational effect, long-term strategic impact	Strategic impact, growing concerns about cyber security

2008, and (4) the cyber attack on Estonian banking and government websites in May 2007.[16] There are also other noteworthy examples, including the China Telecom case in April 2010, Operation Aurora in December 2009, the Pentagon network breach in 2008 and the DDoS attack in Myanmar in 2010. Among others, the Iranian case is the first instance in which Stuxnet was used on a specific target in a cyber attack. Cho (2012) examined some of these cases and he chose the following three cases and compared them with four aspects of cyber attacks.[17]

While many analyses can be conducted, there are at least two things that must be mentioned; very sophisticated technologies were

16. Several computers began to simultaneously attack target servers. As a result, government communication networks were limited to radio for some period of time.

17. Hyun-Suk Cho, "Cyber Security in the Era of Big Data."

used in Iran. The Georgian case was prominent because a real military attack accompanied the cyber attack. With regard to the impact of these cases, Cho (2012) asserts that they triggered growing cyber security concerns and established the trend of nationalizing and/or militarizing cyber security.[18] Indeed, one can agree with Cho's argument by analyzing the recent development in the cyber security policy of major countries.

Other Nations' Responses against Cyber Threat

Many nations have shown a growing interest in cyber security. Some nations already developed cyber security strategies and established relevant organizations. The U.S. Army Cyber Command (ARCYBER) was created in 2009 and launched several cyber security policy initiatives. Last year, the U.S. government published two reports on cyberspace and cyber security, which are "International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World" and "Department of Defense Strategy for Operating in Cyberspace." These documents imply that the U.S. intends to take the initiative on developing international norms as legitimate countermeasures against cyber attacks.

Although Japan has not released its official cyber security strategy, the country boosted its efforts after the defense contractor, Mitsubishi Heavy Industries, was hacked and the employees at other arm firms received e-mails with viruses. As a result, Japan plans to establish a cyber defense unit by 2013. The United Kingdom has also instituted a national cyber security program and authorized the Office of Cyber Security and Information Assurance (OCSIA). Germany developed a comprehensive civilian approach to cyber security, which is considered a priority, and it is supplemented with "measures taken by the *Bundeswehr* (Armed Force) to protect its capabilities and measures based on mandates to make cyber security a part of Germany's preventive security strategy." China has also admitted the existence of cyber

18. Hyun-Suk Cho, *ibid*.

warriors, or the so-called "online blue army," in the People's Liberation Army.

By analyzing these countries' responses, one might raise fundamental questions about the appropriateness of initiating countermeasures for potential cyber attacks, since many countries do not have the opportunities to study cyber security strategy. One might argue that the U.S. and Germany have demonstrated countermeasures in practical manner. In particular, the U.S. has revealed its intent to use physical weapons against cyber attacks by invoking the right of self-defense, and they have been attempting to deter cyber deterrence with the use of real military power. However, following excerpt from Clarke's *Cyber War* is quite thought provoking, since he criticizes the approaches that many countries have already adopted.

> In the first decade of the twenty-first century, the U.S. developed and systematically deployed a new type of weapon, based on our new technologies, and we did so without a thoughtful strategy. We created a new military command to conduct a new kind of high-tech war, without public debate, media discussion, serious congressional oversight, academic analysis or international dialogue. Perhaps, then, we are at a time with some striking similarities to the 1950s. (referring nuclear war strategy) Perhaps, then, we need to stimulate learned discussion and rigorous analysis about that new kind of weapon, that new kind of war.

Korean Case

South Korea's Cyber Security Concerns

Among the cyber security issues in South Korea's infrastructures, North Korean cyber threats are regarded as the highest priority. Its efforts to harm South Korean cyber assets have increased. As previously mentioned, nations with well-developed ICT infrastructure are considerably exposed to the risks from cyber attacks. South Korea is no exception. Considering the South Koreans' impatience and love for ICT devices, they are more likely to quickly panic when a large-scale

cyber attack occurs. Therefore, it is safe to assume that South Korea is one of the most vulnerable countries against cyber threats.

After witnessing the Nonghyup (NH) Bank's computer system freeze on April 12, 2011, many South Koreans were surprised by North Korea's cyber warfare capabilities. South Koreans have taken the incident very seriously because the attack was qualitatively different from previous DDoS attacks in that DDoS attacks simply cause a flood of information traffic to target websites, which often lead to the shutdown of the websites. A DDoS attack is unwelcomed; however, the impact of the attack appears to be manageable in comparison to the case of internet banking system freeze. Following the April 12 cyber attack, many experts questioned whether North Korea has the capability of developing Stuxnet variants. If North Korea has such capacity, then it would be a "clear and present" security threat to South Korea.

Stuxnet development requires advanced technology and considerable costs. A substantial number of programmers and in-depth knowledge of target industrial or network processes are required. For these reasons, only Israel, the U.S. and other Western countries have attempted to develop Stuxnet and use it in real world operations. If North Korea has developed Stuxnet variants, as demonstrated in the case of April 12 attack, then South Korea must assume that the North is now capable of harming not only cyberspace assets, including government websites, but also operation of the real world infrastructure.

Meanwhile, the GPS (Global Positioning System) jamming in May 2012 also drew serious concern from South Koreans. Even though the point of origin was not clear, the Korea Communications Commission, which is responsible for broadcasting and ICT policy, claimed to have confirmed that the jamming signals affecting civilian flights came from the North. Many South Koreans took this incident seriously because it could endanger the lives of passengers.

North Korea's Cyber Warfare Capabilities

As many experts have argued, North Korea may have capability to freeze South Korea's financial networks, presumably through the use of malware similar to Stuxnet.[19] Since the mid-1980s, North Korea has enhanced its cyber attack capacity by training professional hackers. Many news sources report that Kim Jong-il himself stressed the ability to wage cyber war. For example, he said, "the wars of the 20th century were those of oil and bullets, but the wars of the 21st century are information wars." Experts believe that North Korea's notion of information war includes cyber warfare, since the Korean People's Army has tried to enhance its cyber warfare capability under the concept of "electronic intelligence warfare" which encompasses the disruption of networks, destruction of infrastructure and freeze of the enemy's military command and control systems.

Recent news sources have found that North Korea established Mirim College in 1986 for the purpose of improving cyber attack capabilities. This school is closely related to the People's Armed Forces and allegedly educates about 100 professional hackers every year. They are considered to be top-class hackers and are appointed to hacking units as military officials after graduation. The hacking units,

---

19. Some experts even estimate that North Korea's cyber warfare abilities are almost equal to that of the CIA. Here is an excerpt from a newspaper, *The Korea Times*, May 18, 2011, http://www.koreatimes.co.kr/www/news/nation/2011/05/113_87191.html, accessed on December 4, 2012. According to the report, "South Korea's intelligence agencies now believe that North Korea has the capability to 'paralyze the U.S. Pacific Command and cause extensive damage to defense networks inside the United States,' Fox News reported Tuesday. Among the most frequent visitors to U.S. military websites, according to the U.S. Defense Department, are computers traced to North Korea, the report said. According to estimates from Washington and Seoul, their abilities rival those of the CIA, it said."; Even though it may sound like a worst-case scenario, Lim Jong-In, a professor at Korea University, has argued that major infrastructures in South Korea will be compromised in only five minutes if North Korea launched a full-blown cyber attack by applying time-bombs with Stuxnet. *The Dong-A Ilbo*, May 7, 2012, http://news.donga.com/3/all/20120506/46047415/1, accessed on December 4, 2012.

similar to the 121 office, are under the General Bureau of Reconnaissance of the People's Armed Forces. South Korea's Prosecution Service determined that it was a major suspect in the April 12 attack of the Nonghyup banking system. As mentioned earlier, this kind of attacks require highly developed technology and it appears that North Korea has reached a very advanced level to even develop Stuxnet-variants malwares. Many people perceive this situation to be very urgent.

North Korea's Intent: Why Did North Korea Diligently Pursue Advanced Cyber Warfare Capabilities?

It has to do with North Korea's asymmetric warfare strategy. Chemical weapons and biological weapons are often called the poor man's nuclear weapon because they require low development costs and create catastrophic results. North Korea perceives cyber warfare capabilities as means of waging asymmetric warfare. In fact, cyber threats have become synonymous to asymmetric threats. It enables poor countries with the chance to harm the wealthy nation's ICT assets at low costs. If a nation is highly wired with advanced ICT networks, then the attacks against targeted infrastructures can create pandemonium. For this reason, North Korea has desperately invested in the enhancement of cyber attack capabilities. In only several clicks, North Korean hackers can initiate a cyber attack.

Another reason for North Korea's interest in enhancing cyber warfare capability is that it can be useful to its anti-South Korean espionage department. In other words, cyber warfare resources can be used in peace time as well as wartime operations. From the perspective of the North Korean espionage team, cyberspace is ideal for their activities. There is no need for any physical weapons to eliminate anti-government thought or foster pro-North Korea sentiments in South Korea, especially among the young generation. This might be an everyday task of well-trained cyber warriors, who are stationed in Chinese border cities. They may also try to acquire valuable information, including classified documents, through online means. Needless to say, the data can be used to plan the next blow against South Korea.

Meanwhile, it is challenging as well as costly to ensure resilience from an attack for the defending side. Considering these facts and contexts, we cannot deny the burgeoning fact that North Korea's cyber war capabilities are no less than that of China or the U.S., and we must admit that North Korea's cyber warfare capabilities are advanced enough to pose a serious threat to South Korea's security.

Future Direction

Current South Korean Response against Cyber Threat

South Korea's perception regarding cyber security is dire and most discussions are framed as national security issues due to North Korea's threats. Although there are conflicting perspectives, as in the case of the liberal approach toward cyberspace issues, many people simply cannot promote such approaches, considering the security environment in the two Koreas. Thus, one can argue that there is a tendency to nationalize or militarize cyber security in South Korea.

In reflection, the ROK government released the National Cyber Security Master Plan last year, and it can be viewed as the foundation to guide the nation's cyber security strategy. The master plan holds five action plans; "establishing a joint response system among private, public and military sectors, strengthening the security of critical infrastructure and enhancing protection, detection and blockage of cyber attacks at the national level, establishing deterrence through international cooperation and building cyber security infrastructure."[20] In addition, the ROK Armed Forces instituted the Cyber Command, attempting to recruit competent cyber warriors. However, it seems that there are many things that must be accomplished before South Korea is fully prepared for North Korean cyber threats.

For example, the assignment of roles among the government

---

20. "National Cyber Security Master Plan," http://service1.nis.go.kr/eng/120802_masterplan_eng.pdf, accessed on August 20, 2011.

agencies is not distinct. According to the Cyber Security Master Plan, the nexus over cyber security is mainly National Intelligence Service. Although it is appropriate for the intelligence agency to tackle cyber security problems in the peacetime, it does not reflect the concept of cyber war as an independent act of war.

South Korea's responses against cyber threats have not been based on extensive discussions and strategic thought. Even though South Korea has over 1,000 military personnel in Cyber Command within MND,[21] nothing has been clearly manifested by the government or military in regard to the many fundamental issues of cyber countermeasures: 1) recrimination issues, 2) prospects of damage, 3) possibility of repeated application of cyber attacks, 4) possibility of disarming attackers through retaliation, 5) third party issues, 6) risks of escalation, 7) threshold issues and 8) liability issues.

Then What? Raising Fundamental Questions Again

If we have to define the current situation of cyber war preparation, one might use the metaphor of installing outdated or inappropriate software for high-end machinery. In many countries, instruments relevant to cyber war have been instituted without prudent consideration of their effective use. South Korea's situation is more dramatic, since North Korea is attempting to take advantage by waging cyber war. As we have learned from history, late comers often outperform predecessors by adopting and adapting strategies; it was an American military strategist who discovered that an airplane could sink a ship, but it was the Japanese military that dramatically launched the plan in combat situations. The same can apply in cyberspace. North Korea, a country with outdated technology and poor infrastructure, is now boldly preparing cyber warfare.

---

21. The Cyber Command was established in 2010, and reorganized in 2011. The main roles involve planning cyber war, conducting cyber war, educating cyber warriors, training for the cyber war and cooperating with the relevant departments.

What can be done to respond to North Korea's cyber war threat? We have to raise fundamental questions with a pragmatic approach: 1) Can we retaliate North Korea's cyber attack with kinetic means? 2) Is it appropriate? 3) Are there any reliable means to retaliate North Korea's cyber attack in cyberspace? 4) And some analysts argue that South Korea must "prepare a preemptive strike" against North Korea's WMD assets. Are these applicable to North Korea's cyber threat? All of these questions bring us back to the enduring problems in cyber war that we discussed previously. For now, tentative answer for those questions is "yes" in mind but "no" in reality. Suppose South Korea receives serious cyber attacks from North Korea and the intelligence analysts uncover the origin, thus addressing recrimination issues. It is not effective to launch cyber attacks against the Hermit Kingdom because North Korea does not have a well-established cyber infrastructure. Compared to South Korean damages sustained from cyber attacks, North Korea will suffer considerably less than its southern counterparts.

Against this backdrop, it is rational to wage physical attacks, such as missiles, in order to destroy North Korean facilities. However, this kind of countermeasure can lead to all-out war. The use of armed forces against cyber attacks is still a controversial issue in the international community.

We have to focus on what the rational choice is for ROK Armed Forces. Cornish (2010) tried to tackle the strategic problem of cyber warfare in three respects: ends, methods and means. In short, South Korea must invest and prepare of defensive measures rather than offensive options. Furthermore, South Korea must delve into non-military options first because there are inherent limitations of countering cyber attacks by employing military assets. Thus, enhancing multi-national cooperation and establishing solid inter-organizational cooperation in the domestic level should be considered since others may fall in the realm of technology.

The Chinese famous strategist Sun Tzu wrote in his book, *The Art of War*, "the supreme art of war is to subdue the enemy without fighting." This maxim is more suited to North Korea than South

Korea because South Korea cannot internalize its fatal vulnerability on an advanced network. Thus, a focus on defensive measures and the use of non-military assets, initiating inter-agency cooperation in a nation or enhancing cooperation with other nations are viable measures.

Establishing Solid Inter-Organizational Cooperation

South Korea instituted the aforementioned Cyber Security Master Plan last year. However, many people argue that the plan should be elaborated. Cyber strategy must be integrated into the national strategy, since countermeasures for cyber threats involve entire governmental agencies. In fact, responding cyber threats calls for a comprehensive response, ranging from government to private sectors.

With respect to the Cyber Command of the Ministry of National Defense, it should have a clear role and specific mandates. These are closely related to the Cyber Command's position in cyber war. More concretely, it has to be a nexus for the Army, the Air Force, the Navy and the Marines. Cyber threat is characterized by its broadness, and in a wired society, it can cover almost every aspect of civilian life. It is very likely that many government agencies have overlapping jurisdiction regarding the preparation and response to cyber threats. Given the importance of prompt responses to cyber attacks, policymakers should impose specific mandates for the Cyber Command and establish effective cooperation among governmental institutions and non-governmental organizations.

Policy planners must note that governments should not try to take on responsibilities beyond their scope. Hyping cyber threats is not helpful as well. If a state pursues an overly proactive role in cyber security, then the public may take it for granted. In other words, civilians may spare little effort in cyber security and instead, expect state action. Thus, state-level actions should be designed to reflect many important aspects in respects to the arrangement and/or facilitation of inter-organizational cooperation.

Enhancing Multi-National Cooperation

Responding to cyber threats requires a comprehensive response. On the international level, multi-national cooperation may be considered. Cyberspace goes beyond national borders, and thus, security encourages nations to cooperate with one another. Currently, the South Korean government's main concern is North Korean threats, but it cannot ignore threats posed by other sources, including China, Russia and international hacking groups.

In addressing the threat from those countries, efforts have been made to establish cyber security cooperation amongst South Korea, the United States and Japan. For example, the South Korean Defense Minister and the U.S. Secretary of Defense agreed to strengthen bilateral cyber security cooperation in the 43rd SCM. However, South Korea must expand such efforts into a trilateral agreement. Governments and militaries of these three nations must closely cooperate with both the private sectors and other nations.

In the case of establishing multi-national cooperation system, unified efforts must be pursued. Coordination of multi-organizational and multi-national efforts must be carefully considered. Working with international non-profit organizations, such as the International Multilateral Partnership against Cyber Threats (IMPACT), is highly recommended.

In the meantime, costs for establishing countermeasures to cyber threats may be considerable. In this respect, a multi-national cyber defense initiative may save costs and enhance multi-national cooperation for information exchange, cooperation in research and pool procurement. In addition, it is extremely important to prepare for a joint seed funding.

In order to realize the Multi-National Cyber Defense Initiative, commitment from each nation is required. For example, in May 2011, President Obama and Prime Minister Cameron demonstrated their commitment to bilateral cyber security cooperation. They articulated six key areas of bilateral cooperation: 1) a shared vision for the future of cyberspace, 2) building consensus on responsible behavior, 3) pro-

tecting citizens and building the rule of law, 4) partnering with industry, 5) expanding the reach of networked technologies and 6) sharing responsibility for cyber security.

In the pursuit of multi-national cooperation, "how can South Korea position herself between the U.S. and China?" This is highly debated topic because some commentators perceive conflicts between the U.S. and China to be a diplomatic dilemma for South Korea. This conflict should be carefully considered in future studies.

Building Up Resilience of Cyberspace

The core of cyber defense is to make networks resilient to attacks. In the real world, it takes time to restore damaged equipment and facilities destroyed by armed attacks. Sufficient stock of weapons and resources are critical in conducting war. In contrast, cyberspace is intangible and can possess resilience against attacks. Networks can be partly destroyed or disrupted, but cyberspace as a whole does not disappear because it is not a substantial material. This resistance can act as deterrence itself because enemies will realize that cyber attacks are ineffective.

In this sense, resilience is completely defensive, but it also has strong deterrence. It can be achieved through three pillars: software, hardware and human resources. Software and hardware can be viewed as supplies, and it is essential to secure a sufficient supply of goods and their updates. More importantly, a workforce management is necessary to sustain high resilience.

Conclusion

In this article, we explored IR theoretical perspective on cyberspace and cyber war, typical examples of cyber attacks, major countries' response to cyber threats and the South Korean approach to cyber security. Cyberspace is continuously evolving. Initially, few agencies and organizations took notice of cyberspace as a possible threat to security, but it has evolved into a strategic arena.

Strategy for cyber war must be taken in two directions. The first is to secure cyberspace with cyber deterrence based on the current networks environment. At this stage, we argue that defensive measures must be adopted. The second is to astutely predict the transformation of cyberspace and cyber war and the need to initiate proactive measures.

■ **Article Received: 8/2** ■ **Reviewed: 11/14** ■ **Revised: 12/6** ■ **Accepted: 12/17**

Bibliography

Bae, Dal-hyong. "Direction for Coping with Cyber Threats of North Korea in the Level of National Military Strategy." *Strategic Studies*, Vol. 52 (2011), pp. 147-172.

Boo, Hyeong-Wook. "North Korea's Cyber Warfare Capabilities and Need for Multi-National Cyber Defense Initiative." Paper presented at the 8th KIDA-INSS-NIDS Trilateral Workshop. December 2011.

_____. "North Korea's Cyber Warfare Capability and the Republic of Korea's Policy Options." *RINSA Forum*, Vol. 18. KNDU. September 2011.

Chang, Noh-Soon. "A Comparative Study on Cyber and Nuclear Threats by Transnational Actors in terms of the Stability of International System." *Korean Political Science Review*, Vol. 39, Issue 5 (2005), pp. 263-281.

Cho, Hyun-Suk. "Cyber Security in the Era of Big Data." Unpublished material. Seoul National University of Technology. January 2012.

Clarke, Richard Alan and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: HarperCollins. 2010.

Cornish, Paul, David Livingstone, Dave Clemente and Claire Yorke. "On Cyber Warfare." A Chatham House Report. November 2010.

Deibert, Ronald. "Militarizing Cyberspace." *Technological Review*. MIT. 2010, http://www.technologyreview.com/notebook/419458/militarizing-cyberspace, accessed on May 4, 2012.

Dougherty, Jamed E. and Robert L. Pfalzgraff. *Contending Theories of International Relations: A Comprehensive Survey*. London: Longman. 2000.

Eriksson, Johan and Giampiero Giacomello. "The Information Revolution, Security and International Relations: (IR)relevant Theory?" *International Political*

Science Review, Vol. 27, No. 3 (July 2006), pp. 221-244.

Federal Ministry of the Interior. "Cyber Security Strategy for Germany." 2011, http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile, accessed on August 20, 2011.

Geer, Daniel E. Jr. "Cyber Security and National Policy." *Harvard National Security Journal*, Vol. 1 (2010), pp. 203-215.

Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security*, Vol. 4, Issue 2 (2011), pp. 1-24.

Krekel, Bryan et al. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation." Prepared for the U.S.-China Economic and Security Review Commission. McLean, VA: Northrop Grumman Corporation. 2009.

Libicki, Martin C. *Cyber Deterrence and Cyber War*. RAND. 2009.

Mahnken, Thomas G. "Cyber War and Cyber Warfare." In Kristin M. Lord and Travis Sharp, eds. *America's Cyber Future: Security and Prosperity in the Information Age* (Vol. II). Washington, DC: Center for a New American Security. 2011, pp. 55-64.

Manjikian, Mary McEvoy. "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik." *International Studies Quarterly*, Vol. 54, Issue 2, June 2010, pp. 381-401.

Mulvenon, James C. and Gregory J. Rattray, eds. *Addressing Cyber Instability* (Executive Summary). Cyber Conflict Studies Association. 2012, http://www.cyberconflict.org/storage/CCSA%20-%20Addressing%20Cyber%20Instability.pdf, accessed on November 23, 2012.

Nye, Joseph S. Jr. "Power and National Security in Cyberspace." In Kristin M. Lord and Travis Sharp, eds. *America's Cyber Future: Security and Prosperity in the Information Age* (Vol. II). Washington, DC: Center for a New American Security. 2011, pp. 5-23.

Sheldon, John B. "Deciphering Cyberpower: Strategic Purpose in Peace and War." *Strategic Studies Quarterly* (Summer 2011), pp. 95-112.

Singer, Peter W. and Noah Schactman. "The Wrong War: The Insistence on Applying Cold War Metaphors to Cyber Security Is Misplaced and Counterproductive." Brookings Institute. August 2011, http://www.brookings.edu/research/articles/2011/08/15-cybersecurity-singer-shachtman, accessed on May 4, 2012.

Solomon, Jonathan. "Cyber Deterrence between Nation-States: Plausible Strategy or a Pipe Dream?" *Strategic Studies Quarterly* (Spring 2011), pp. 1-25.

Son, Tae-Jong and Insoo Choi. "Threats to Cyber Security and its Countermeasures in the ROK." Paper presented at the 7th KIDA-IDA-NIDS Trilateral Workshop. September 2011.

Tabansky, Lior. "Basic Concepts in Cyber Warfare." *Military and Strategic Affairs*, Vol. 3, No. 1 (May 2011), pp. 75-92.

Viotti, Paul R. and Mark V. Kauppi. *International Relations Theory: Realism, Pluralism, Globalism and Beyond*. Needham Heights: Allyn and Bacon. 1999.

Waxman, Matthew C. "Cyber Attacks and the Use of Force: Back to the Future of Article 2(4)." *The Yale Journal of International Law*, Vol. 36 (2011), pp. 421-459.

Whitehouse. "International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World," http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, accessed on May 30, 2011.

Wu, Timothy S. "Cyberspace Sovereignty? The Internet and the International System." *Harvard Journal of Law & Technology*, Vol. 10, No. 3 (Summer 1997), pp. 647-666.

Yoon, Kyu-Sik. "North Korea's Cyber Warfare Capability and Threat." *Military Review [Gunsanondan]*, Vol. 68, 2011, pp. 64-95.