아태연구 제20권 제3호(2013)

Cyber Security for the Construction of Northeast Asian Community

이규영*·김유정**

| 목 차 |

| 논문요약 |

본 논문의 목적은 사이버 안보의 필요성과 중요성을 강조하고 사이버 안보와 관련하여 동북아 공동체 건설 및 정책협력을 위한 함의모색에 있다. 현재 제 국가들과 사회는 여러 측면에서 볼 때 정보통신기술의 발달로 이에 대한 의존도가 급격히 심화되고 있다. 나아가 인터넷은 사람, 정치와 상업 활동의 중추로서 상호 불가분의 관계로 접어들었다. 또한 국가안보 역시 사이버 공간으로부터 영향을 깊이 받으며, 동시에 국제무대에서 강력한 국가들 간 사이버 공간을 둘러싸고 무기 없는 군사전쟁이 이미 시작되었다.

이러한 변화와 더불어 최근 몇 년간 동북아에서도 안보환경이 매우 악화되고 치열해져 간다. 이는 무엇보다도 핵무기를 앞세운 통제되지 않는 도발에서 비롯되고, 나아가 북한의 잠재적 사이버 공격 가능성과 실제 사례로부터 크게 영향을 받기 때문이다. 이와 같이 사이버 안보문제는 해당 지역에서 핵 위협에 버금가는 군사력처럼 중요해진다.

* 서강대학교 국제대학원 교수
** 한국외대 강사

이러한 관점에서 본 논문은 사이버 공간에서 위협요소와 현상의 증가 원인 및 현상, 동북아시아에서 사이버 안보의 중요성 및 필요성, 이에 따른 동북아시아 공동체 건설을 구축하는 과정에서 사이버 안보를 통한 정책협력 가능성과 함의를 논술하고 있다. 본 논문은 총 5장, 즉, 1) 서론, 2) 동북아 안보환경의 변화양상 및 사이버 안보문제, 3) 실제적 동북아 안보환경과 사이버 안보구축의 필요성, 4) 동북아 공동체구성을 위한 제언 및 사이버 안보를 위한 다자적 정책협력, 5) 결론 등으로 구성되어 있다.

▪ 주제어: 사이버 안보, 아시아 공동체, 사이버 테러, 유럽연합, 북한

I. Introduction

Our society is entirely dependent upon computer networks. It touches many domains business, finance, control systems for power, gas, drinking water and other utilities, airport and air traffic control systems, logistical systems, health care, government services, and etc. In other words, cyber space affects nearly every part of our daily life and becomes essential components of our society.

Besides the connecting of cyber space to national security, the war without the use of guns has already started in cyber space among several states. Cyber space enables states to express power and pursue other state interests in new ways. In recent years, the American government has become particularly concerned with the security challenges from cyber attacks. In 2013, President Obama declared:

"Cyber threat is one of the most serious economic and national security challenges we face as a nation. America's economic prosperity in the 21st century will depend on cyber security."(National Security

Council 2013)

Obama also emphasized that the economic prosperity and security in the 21st century would rely on cyber security. The President has appointed Howard Schmidt to serve as the U.S. Cyber security Coordinator and created the Cyber security Office within the National Security Staff, which works closely with Federal Chief Information Officer Steven VanRoekel, Federal Chief Technology Officer Todd Park, and the National Economic Council(Cyber security 2013). It means that cyber security is widely regarded as an urgent and high-level problem that cannot be ignored.

This article aims to underline the necessity and importance of cyber security and try to search for the implications and suggestions for the construction of the Northeast Asian community and policy cooperation in this domain. In recent years, security environment in Northeast Asia has deteriorated. This is of course due to the naked provocations regarding nuclear weapons and also due to hidden cyber attacks from North Korea. In the face of an energy security crisis, cyber security is also getting more exposure as a considerable issue for the security of Northeast Asia. Nothing seems to be more important as the energy security agenda than cyber security.

The main discussion will be concerned with these emergent threats in cyber space, the necessity and importance of cyber security in Northeast Asian areas, and implications and suggestions for the construction of Northeast Asian community and policy cooperation in cyber security. Regarding this main aim of this article, we would like to discuss the following points of order: 1) Introduction; 2) The changing security environment and the cyber security in general; 3) Security environment and the cyber security in Northeast Asia; 4)

Suggestions for the construction of Northeast Asian community and multilateral policy cooperation in cyber security; and 5) Conclusion

Ⅱ. The Changing Security Environment and the Cyber security in general

During the Cold War when the identity of potential enemy between the two superpowers was very clear, the international security was concentrated in the sectors of military issues, such as nuclear strategy, weapons systems and arms control measures etc. Namely, the main concerns of strategists in this period were linked with preventing all-out nuclear war between U.S.A. and U.S.S.R. and establishing the superiority of weapons systems over the other, and minimizing one's own damage while imposing maximum damage to the other side.

However in the 1990s when the East European Communist regimes collapsed and the threat from Communist countries was reduced to almost nothing, a new international environment emerged. The bipolar system gave way to a new international order led by the unipolar system and the possibility of nuclear war was reduced. But with the decentralization and regionalization of the international system, the global security environment has become more complicated and fluid than the 1990s.

1. The changing of security concept between traditional and non-traditional security environment

Since the post-Cold War period, the overall global security

environment was confronted with new threats ranging from traditional challenges to non-traditional threats. This evolution led to a search for a new security doctrine. Furthermore, this new concept of security was opening new spaces for theorizing about the world politics(Buzan et al. 1998).[1] During this period, attention is being paid to non-traditional security threats, namely: economic security, food security, health security, environmental security, personal security, community security, energy security, cyber security, and etc. In such new circumstances, cyber attacks and crimes crossing the boundaries of public and private sectors are very serious. As Michael Sussmann explicitly states:

"Because everything from banks to phone systems to air traffic control to our military relies so heavily on networked computers, few individuals and institutions are impervious to this new and threatening criminal activity."(Sussmann 1999, 452)

The web in the modern society came into its own as a critical medium for governance, commercial exchange and social interaction. Although it has only been viably standard in the post-1990 period, this development has produced not only meaningful results, but also generated significant challenges to state security. By improving technological utilization, it opened a new generation of threats that have increased in magnitude as the web has expanded.

2. Cyber security as a new concept in international security environment

1) They argue that security should cover not only military but also other non-military matters and call themselves widener and their approach a new concept or widening interpretation.

With the changing environment of society, security perceptions and concepts were greatly shifting. Especially, since the 9·11 terrorist attacks in the U.S.A, protection and security in the United States and Europe have been faced with a variety of new terrorisms (primarily non-state extremist terrorism). One of the new and important issues to be considered is the concern with cyber terrorism(Elmusharaf 2004).[2] The more society is dependent on computer networks, the more cyber terrorism is becoming one of the bigger challenges to modern military technology. Consequently, cyber security is becoming an important national security and crisis management agenda item. Recently, the director of National Intelligence James Clapper said that:

"America's biggest national security threat could come not from bullets or bombs in a terrorist attack, but from a computer keyboard."(Martinez 2013)

Therefore, these new threats require new types of responses. Traditional categories of security might be not adequately adopted for the response against the emerging challenge of threats, attacks and terrors in cyber space(Dorothy 2013).[3] For that reason cyber security (security within and from cyber space) is a much broader problem for individuals, businesses, public and private organizations, governments,

2) Cyber terrorism is new concept of military strategy that the FBI defined it as the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub-national groups or clandestine agents.

3) Cyber threats are characterized by an attacker, a target system, a set of actions against the target, and the consequences resulting from the attack, including damages to the target, direct and indirect losses to victims, and impact to third parties. The nature and mission of the attacker often classify threats. There are six major categories: hackers, insiders, corporate spies, criminals, terrorists, and nation states.

and international organizations. There is a need to acknowledge the importance and necessity of cyber security and to search for the appropriate cooperation policy.

Ⅲ. Security environment and the Cyber security in Northeast Asia

Northeast Asia has considerably developed the field of economy of Internet Technology (IT). States such as Japan, South Korea and China are markedly advanced in this domain. Cyber space has become, thus, essential components of their societies. Nowadays, it seems difficult to imagine a major business or organization that does not rely on advanced IT in these countries. The need to respond to this security challenge, also, seems to be seen more outstandingly in these areas. Lately, cyber crimes were remarkably increased and cannot be turned to the blind-eye. In Japan, for example, the number of cyber crimes uncovered by police in 2004 increased 13 percent from the previous year to 2,081 with the figure more than doubling over the past five years. The following year reports of cyber crimes in Japan being increased to 52 percent from 3,161 reported incidences. A similar trend can be seen in South Korea where, in 2002, the number of internet-based criminal cases increased to 60,000 up from 121 in 1997. By 2006 it had increased to 70,545 instances, with identity fraud and hacking being the two most prevalent crime types(Asian Security 2013).

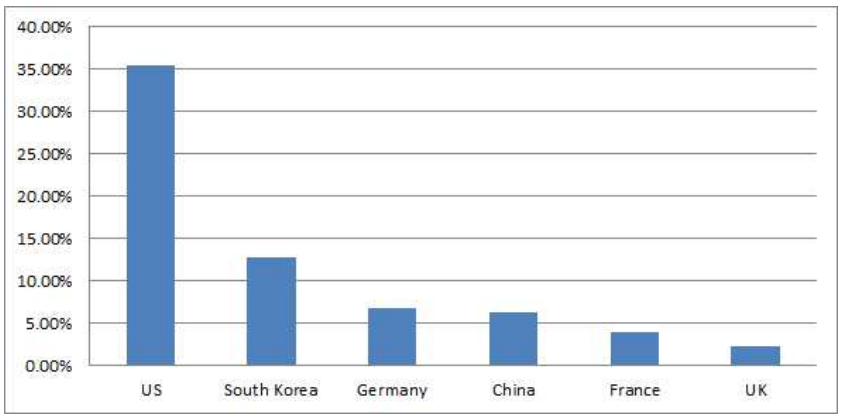
Such as in Japan and South Korea, exceptionally, connections to the web are commonplace and there is a rapid adoption of new

technologies. Such a tremendous circumstance of computers stimulated criminals and terrorists to make it their preferred tool for attacking their targets. Particularly, in Northeast Asia, computer network attacks have been rising steadily with the prevalence of computer viruses and worms since 2002.

The second half of the year 2002 showed that the most dangerous nation for originating malicious cyber attacks is the U.S. with 35.4% of the cases down from 40% for the first half of the same year. South Korea came next with 12.8%, followed by China 6.2 % then Germany 6.7%, then France 4%. The UK came number 9 with 2.2%(Sunny Lee 2011). As demonstrated by <Figure 1>, South Korea is the second most dangerous country in terms of cyber attacks.

<Figure 1>

Most Dangerous Nation for Originating Malicious Cyber Attacks



1. Bilateral Cooperation between U.S.A. and Northeast Asia for cyber security

In the United States, improving the security of cyber space more

generally received greater attention within the Administration and Congress of Obama. Its focus is toward cooperative effort with some strong countries in IT. Washington is pursuing collective cyber security with its allies. This strategy has a symbolic meaning for the alliances to show the strong will to counter cyber threats collaboratively. The U.S. government would appreciate information-sharing about the defense industry, given the series of cyber espionage targeting American, Japanese, Chinese and South Korean defense contractors. Also, Washington is expanding an information-sharing framework this year, based on the cooperative mechanism of the defense industrial base under the Executive Order to improve critical infrastructure's cyber security.

(1) U.S.A.-Japan

Following the increase in cyber attacks in Japan, the Japanese government has thus strengthened its National Information Security Center (NISC). The office was established in 2005 with officials on loan from several ministries and made significant policy changes in Japan. The Japanese government issued the policy of Information Security Strategy for Protecting the Nation on May 11, 2010, as it realized that the large-scale cyber attacks in the United States and South Korea particularly alerted Japan and could be a threat to national security. In Japan, there is the National Police Agency, Ministry of Defense, Cabinet intelligence Research Office (CIRO), and the previously mentioned National Information Security Center (NISC).

Lately, the Japanese government adopted the Cyber security Strategy to replace the Information Security Strategy for Protecting the Nation. This is the first time for Tokyo to employ the word cyber security, in its strategy to deal with information security issues and cyber threats to its national interests. The country is also trying to

raise a Japan-U.S. alliance in terms of cyber security. Tokyo and Washington are currently discussing the revision of their bilateral defense-cooperation guidelines and the modification cover cyber security for the first time.

U.S. President Barack Obama and Japan's conservative Prime Minister Shinzo Abe discussed the issues in their bilateral meeting at the White House on February 22, 2013. The following Friday Obama said the U.S. and Japan are committed to strong actions in response to North Korea's provocations as he welcomed Japan's premier to the White House. In this meeting, Tokyo and Washington formally talked about cyber security for the first time.

(2) U.S.A.-China

The latest Obama-Xi summit referred cyber security in their bilateral meeting at the Annenberg Retreat at Sunnylands in Rancho Mirage, California, on June 7, 2013. The talks between the two leaders in this country will be followed by a July meeting between the U.S. and Chinese officials focusing on cyber espionage, along with other strategic and economic issues. Certainly, Obama needs China's help in stemming nuclear threats from North Korea.

Furthermore, Obama is trying to establish a policy of cooperation between the two states in cyber security. The situation for China was that President Jiang Zemin was badly positioned for both the U.S. and North Korea. However, Xi has recently taken a more stern tone with North Korea. He has told North Korea to return to formal nuclear talks with the U.S. and other world powers. In addition, he has warned Kim Jung-Un that no country should be allowed to throw a region and even the whole world into chaos for selfish gain.

The U.S. long has pushed China to take more aggressive action against North Korea and welcomed Xi's comments. However, China is

North Korea's strongest ally and biggest trading partner. This point is very significant for solving the problem of cyber attacks from North Korea. The leader of China is in the position to mediate North Korea's nuclear threats, which can bring about the policy of cooperation among the countries in the world that may help to search the new way of peace.

(3) U.S.A.-South Korea

In South Korea, the economy, commerce and every aspect of daily life is deeply dependent on the internet. Recent massive cyber attacks that paralyzed computer networks at several South Korean banks and broadcasts led South Korea to acknowledge the risk of cyber attacks. But North Korea's cyber attacks not only centered on South Korea but also the United States. According to several news agencies' reports, a series of attacks on computer networks in South Korea and the U.S. was apparently the work of a North Korean hacker. North Korea attacked the White House, the Pentagon, and the Washington Post. Apparently, South Korea and U.S. governments both should prepare to block such cyber terror activities and cooperate against these new attacks. Recently, according to Kwon Kihyeon, a spokesperson at South Korea's Ministry of National Defense, said that U.S. and South Korean militaries would cooperate to develop diverse deterrence scenarios against hacking attacks and increase anti-cyber warfare forces to over 1,000 to better deal with emerging threats from countries like North Korea. Most of all, it seems to be important and pressing to estimate exactly the capability of North Korea's cyber attacks, through the mutual cooperation between the South Korean and U.S. governments.

However, these cases of bilateral cooperation between the U.S. and the major three states of Northeast Asia have some limitations on the

ability of not only solving the problem against the cyber attacks from North Korea, but also creating the idea of the construction of the Northeast Asian community. This is due to the challenge posed by cyber threats which becomes more complex and transnational. We need to create a fundamentally new way to approach this issue.

2. Potentials and Threats of Cyber Terrors from North Korea

Military tensions not only in the Korean peninsula but also in Northeast Asia in general have escalated dramatically since North Korea conducted its third nuclear test in March of 2013. North Korea threatened war on the peninsula with nuclear weapons in order to leverage their goals and interests. In reality, North Korea continues to issue serious attacks in cyber space simultaneously. In short, North Korea is continuing to stoke tensions with a fourth nuclear missile test, which comes as the regime may be looking to carry out war on a different battle fieldthe internet. Consequently, there is a need to pay attention to North Korea's new form of terrorism and their ability and reinforcement of the capability of cyber terrorism as much as their ability to use nuclear power.

Contemporarily, North Korea is the one of the worst cyber terrorist countries in the international society. North Korea is in a very challenging status after China(US-China Economic and Security Review Commission 2008)[4] and Russia in Northeast Asia. North Korea's cyber threats are getting worse as it is reinforcing its training system.

---

4) China's intentions and capabilities often feature prominently in analysis of this sort. According to a recent US Congress policy review panel, "China is aggressively developing its power to wage cyber warfare and is now in a position to delay or disrupt the deployment of America's military forces around the world, potentially giving it the upper hand in any conflict."

<Figure 2>
Cyber Threat Matrix

Country	Estimated Military Spending	Intent	Estimated Threat	Current Capabilities	Basic Data	Intermediate Data Weapons	Advanced Data Weapons
China	$55.90	5.1	High	4.2	Yes	Yes	Yes
Iran	$9.70	4.0	Elevated	3.4	Yes	Limited	No
Libya	$1.30	3.0	Moderate	2.5	Yes	No	No
North Korea	$5.20	3.0	Elevated	2.8	Yes	Limited	No
Russia	$44.30	5.0	High	4.0	Yes	Yes	Yes
Syria	$8.90	3.0	Moderate	2.2	Yes	No	No

Estimated Military Spending is in Billions of U.S. Dollars
Rating Scale: 1=Low 2=Limited 3=Moderate 4=High 5=Significant
※ Source: Cyber Threat Matrix (Sunny Lee 2011)[5)]

North Korea has been training a team of computer-savvy cyber warriors. According to Won Sei-Hoon, then chief of South Korea's National Intelligence Service, North Korea has a large elite force of cyber warfare experts of about 3,000. North Korean students were recruited to the nation's top science schools to become "cyber warriors. They were trained as future hackers at a university in the industrial North Korean city of Hamhung. Some of them also were sent to study abroad in China and Russia(North Korea training teams … 2013).

The government of South Korea estimates that North Korea has enough power to threaten South Korea and the U.S. with such organizations from North Korea's unit that operate and originate from these educational institutions related to cyber terrorism. Five major

5) Technolytics(The Technolytics Institute) created a cyber threat matrix by the international standard in 2007. It measured intent and capabilities of six potential adversaries of the U.S. that North Korea is in very challenging status after China and Russia in Northeast Asia.

universities have trained cyber hackers each year. Specifically, Mirim University concentrates on training cyber warfare tactics by Russian professors. This university, affiliated with the Ministry of the People's Armed Forces, educates some 100 world-class hackers every year and appoints them as military officials to hacking units under the General Bureau of Reconnaissance of the Ministry of the People's Armed Forces.

<Figure 3>
North Korea's Cyber Warfare Training Status

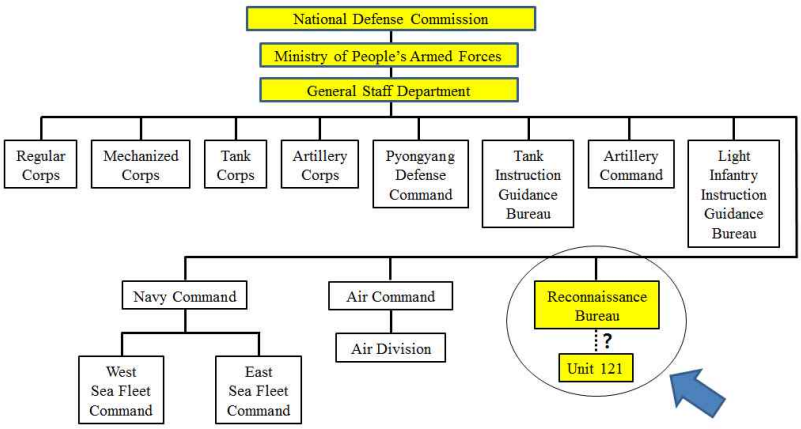
Institute	Training	Faculty
Mirim University (Pyongyang Automation University)	- electronic warfare tactics - a hundred hackers every year	25 Russian professors from the Frunze Military Academy
Amrokgang college of Military Engineering	Hackers	
The National Defense University	Hackers	
The Air Force Academy	Hackers	
The Naval University	Hackers	

※ Source: North Korea's Cyber Warfare Training Status (Sunny Lee 2011)

In fact, North Korea has been building up a hacking squad since 1986. Kim Jong-Il got the isolated nation to reinforce itself towards electronic warfare tactics all the more since economic hardships during the '90s led to difficulties in expanding its conventional weapons arsenal. North Korea's General Bureau of Reconnaissance started to conduct cyber terrorism projects as the center of such terrorism(Sunny Lee 2011). Kim Jong-Il told his military, Modern war is electronic warfare. After the Kosovo war, he commented frequently, The war of the 20th century was a war of oil and bullets, but the war of the 21st century is one of intelligence.

North Korean hackers are becoming increasingly sophisticated in their attacks on the computer control systems of South Korean government agencies, financial institutions, news media and other organizations. In 2011, the young leader of North Korea, Kim Jong-Un, raised the status of its cyber warfare unit under the Reconnaissance General Bureau and increased the number of troops in the unit from 500 to about 3,000(Urgency needed … 2013).

<Figure 4>
North Korean Armed Forces Command Structure



?: Unit 121 is reportedly subordinate to the Reconnaissance Bureau according to open source and media reports
※ Sources: Sunny Lee 2011

Traditionally, North Korea has conducted terrorism by the way of organizing fear and disrupting physical destruction and even death. However, as the past two decades and the increase in recent activity shows, there is now a new wide range of network attacks.

North Korea's cyber terrorism is a new challenge on top of military terrorism. Even though North Korea announced that it possess nuclear weapons and conducted nuclear tests, it is not easy to consider its overall military capability. However, recently North Korea's military

cyber terrorism seems more dangerous in cyber warfare in advanced cyber techniques. In effect, it is more difficult to predict the exact targets or impacts of future activity. North Korea will strive to reinforce to take advantage of actual cyber war.

3. North Korea's Real Cyber attacks

In 2009, the massive scale of cyber attacks was recorded in the U.S. and South Korea. Such targets included the Department of Defense (DOD), the U.S. Congress, the Treasury, the Department of Homeland Security (DHS), Federal Trade Commission (FTC), New York Stock Exchange (NYSE), Washington Post, and among others. Servers slowed down during the attacks(U.S. eyes N. Korea for massive cyber attacks 2013). These attacks are known as BOTNET Attacks. Owners of the servers had no idea that their servers were used to attack other computers.

In 2012, North Korea conducted a hacking incident that disabled the news production system at the South Korean newspaper JoongAngIlbo. In April of the same year, South Korea's agricultural cooperative known as Nonghyup Bank was paralyzed by a computer virus attack. Clients could not use ATM's and online services during this period. These cyber attacks have raised fears about North Korea's cyber terrorism capabilities.

In 2013, North Korea is widening its targets, as we have seen in the March 20 case that involved television broadcasters and financial institutions. Also, cyber attacks were launched against South Korean banks and TV broadcasters and paralyzed business operations. The main pursuits of cyber attacks from North Korea are:

- Physical Damage to Infrastructures, Utilities, and Premises
- Financial Damage or Theft

- Psychological Damage or Demonstration
- Virtual Damage (Not Recognized, but Serious)

In sum, the major goals of cyber attacks from North Korea are to not only affect national prosperity and security, but also destroy the societal stability in South Korea. This can be achieved by disrupting national transport systems, stealing bank details for financial crime or accessing personal information for fraud. In fact, in 2009, North Korea launched a series of cyber attacks that resulted in the forced shut down of nearly 50,000 computers and servers at South Korean broadcasters and banks. Yet, officially North Korea has denied involvement in such cyber attacks against their South Korean brethren(NKorea denies … 2013).

Cyber attacks can be carried out for comparatively little cost, with widely available equipment and minimal risk. Also, it could be confidently acted, unrecognized, but very serious. Most of the time, it is difficult to identify who the real attackers are. North Korea prefers using the following cyber attack methods:

- Facility: from anywhere in the world.
- Comparatively low cost with catastrophic results: cheaper than traditional methods but affecting a large number of people or countries in war.
- Concealment: hiding personalities and location.

Thurman, commander of the U.S. forces in South Korea, said that cyber attacks are ideal for North Korea because they can take place relatively anonymously(NKorea denies … 2013). A cyber attack can deal a great amount of damage to South Korea's vital infrastructure at a low cost. As such, the South's online infrastructure needs greater

protection. But neither the public sector nor the private one is vigilant enough against North Korea's cyber terrorists. The great risk to South Korea's society poses a serious threat but countermeasures are so far unreliable at best.

Ⅳ. Suggestions for the construction of Northeast Asian community and multilateral policy cooperation in cyber security

Meeting the challenge of cyber security crossing boundaries, there is a need for international cooperation against increasing cyber terror attacks in Northeast Asia. The reason for this is because cyber attacks frequently cross national borders as attackers hack one system after another, using each to launch an attack against the next. North Korea's cyber terrorism is not only focused on South Korea but also on the other countries. Thus, it is urgent to prepare the response and require cooperation from every country involved. Three ideas of shouldering the collective burden could be:

- Sharing the consciousness of risk of cyber terrors and cyber challenges.
- Sharing the necessity of collective effort to response against cyber terrors.
- Sharing information on threats and vulnerabilities of cyber attacks.

In practice, several governments have already come together in

several forums, including the G8, Council of Europe (CoE), and European Union to address the problems associated with international attacks and facilitate international cooperation(Denning 2013). Such organizations, the Council of Europe Convention on Cyber Crime, which is the first international treaty for fighting against computer crime, consists of 45 member and non-member countries including Japan, USA, and Canada. Also, Interpol, with its 178 member countries, has fought against cyber terrorism. In addition, the European Police Office('Europol') is established under the Europol Convention of 1995 to enable the European Union's police authorities to cooperate more effectively in combating specific types of serious international crime, including drug trafficking, forgery of money, trafficking in human beings, trafficking in radioactive or nuclear substances and child pornography.

This organization has the aim to provide for police cooperation between member states to combat terrorism, drug trafficking and other international crime. In reality, it facilitates the exchange of data between members; provides expertise, technical support and advice; generates strategic reports and provides operational analysis in support of Member States' operations(Elmusharaf 2004).[6] A good starting point is information-sharing with these international organizations on threats and vulnerabilities of cyber attacks. In short, governments of Northeast Asia should address these issues through cross-sector cooperation and actively seek collective intelligence beyond the parameters of a traditional security approach.

6) Recently, the association of South East Asia nations (ASEAN) has set plans for sharing information on computer security.

1. Implications from the European Experiences: approach of functionalism

A good beginning effort is building a common consciousness of crisis facing the recently growing cyber attacks in Northeast Asia. According to Jean Monnet, who led the negotiation of community of ECSC in 1952 and better known as the Father of Europe said Europe is the result from the crisis of Europe for solving the problem facing the present risk(Monnet 1976, 488). Feeling the crisis and consciousness of the danger may stimulate the Northeast Asia to get the necessity for the cooperation policy in cyber security and the construction of Northeast Asia in peace.

It is acceptable for the construction of Northeast Asia to implement the pragmatic idea like the process of European Unification in the past 60 years. On the other hand, the cooperation in the domain of economy, technology, and science may easily help to organize the collective effort in security. Functionalism, one of the theories of European Integration, might be a realistic method of approach for the construction of the Northeast Asian Community(Groom 1978, 140-152).[7] In other words, a functional need or technological change could call for the cooperation among the states of Northeast Asia.

Facing the common threats as the result of cyber terrors, Northeast Asian countries must hold a large number of high-level sectorial

7) The integration theory has developed under three major approaches: functionalism, neo-functionalism, and federalism. First, functionalism is based the hypothesis that national loyalties can be diffused and redirected into a framework for international cooperation in place of national competition and war. Second, unlike functionalism which stresses functional needs or technological changes in the study of international political integration, Neo-functionalism, which is provided by Ernst Hass, has turned its analytical attention to the influences of political factors, such as interest groups, political parties, governments and international organizations.

dialogues on issue of security. Sectorial and technological communications involving officials and experts on cyber security will give a possibility toward the feasible cooperation of security policy in this area.

2. Establishment of 'Asianpol'

Lessons from Europe for the cooperation policy and the construction of a Northeast Asian security community, such as 'Europol'(Kyu Young LEE 2007), are a good example of where to begin. We can perhaps suggest establishing an organization like 'Asianpol' that might be specialized to the region of Northeast Asia to tackle a cross-border crime like those that occur in cyber space. Like Europol, this organization ought to provide police cooperation between countries in Northeast Asia to combat terrorism, in the way of:

- Facilitating the exchange of information between Northeast Asia states.
- Providing operational analysis in support of operations.
- Generating strategic reports (e.g. threat assessments) and crime analysis on the basis of information and intelligence
- Providing expertise and technical support for investigations and operations carried out within the states involved, under the supervision and the legal responsibility of the member states concerned.
- Promoting crime analysis and harmonization of investigative techniques.

Without sharing information about crime in cyber space, it brings about low possibility of real cooperation and the dearth of solutions to the crisis of cyber attacks; we are doomed to be repeat victims. With

proper handling of criminal intelligence in cyber space, the effectiveness and cooperation between the member states could be significantly improved.

3. Idea of the 'Cyber silk-road' by Kim Dae-Jung for the cooperation between Europe and Asia

Cooperation in cyber space between the EU and Northeast Asia is both desirable and feasible. Even though the EU does not have military alliance in North East Asia, the EU has already begun to cooperate on space technology and satellite navigation with some of Asia's major space powers. The EU signed an agreement for the joint development of Galileo (the EU-led global navigation satellite system) with China in 2003 and with South Korea in 2006 (renewing the accord in 2011). The satellite network's ground stations are currently being developed across the Asia-Pacific in the EU territories (mainly the French Polynesia) while discussions are underway with the Asian partners in the Galileo project for building joint ground stations and receivers(Haines 2006). This form of cooperation allows the two sides to establish the crucial relationship related to the security implications.

In addition, we can't ignore the idea from former Korean president Kim Dae-Jung that of the construction of high-speed information network for the cooperation between the EU and Asia. On December, 11, 2001, during a speech at the European Parliament in Strasbourg, France, he suggested the Cyber Silk Road, so as to create an 'e-EurAsia,' under the Trans-Eurasian Information Network project. Kim Dae-Jung states:

"The information revolution is inevitably linked with accelerating

openness and globalization. Territorial boundaries are becoming practically meaningless as enormous amounts of information are spreading throughout the world almost instantaneously. […] Thus, enhanced information capabilities and globalization could also threaten global peace in the 21st century. […] Now I would like to touch on the future of Korea and the EU. I proposed the construction of a high-speed information network at the Asia-Europe summit meeting in Seoul last year. I am pleased to remind you that the leaders of all the member nations gave it their active support. Under this project, we are envisaging the creation of a "Cyber Silk Road" linking Asia and Europe. It is a project for the new millennium aimed at furthering the exchanges between Asia and Europe by setting in place an 'e-EurAsia'."(Adress by Kim Dae Jung 2001)

On the same day, he suggested another project, such as the construction of an "Iron Silk Road", directly linking Korea with Europe by land, which would greatly promote exchanges between Europe and Asia. Thus, one of the things that must be done is the linking of the railway between South and North Korea. This railway has been severed at the Demilitarized Zone for the past 50 years. Besides, when the trans-Korean railway (TKR) is linked with the trans-China or the trans-Siberia railways, a train leaving London could reach Seoul and Busan via Paris, Eastern Europe, Central Asia and Siberia or China. Then, goods could be shipped to all parts of the Pacific region, and beyond, from Busan, which also happens to be the third largest container port in the world. Transportation costs would be cut by 30% and time shortened by one third(Addressed by Kim Dae Jung 2001).

According to the message of Kim Dae-Jung, technological and economical approach for the cooperation between EU and Asia

contribute to achieve the construction of cooperative partnership and also the establishment of peace in Northeast Asia. He also insisted that:

"The EU has been taking part in the Korean Peninsula Energy Development Organization (KEDO) and has offered a range of humanitarian and economic assistance to North Korea. It is also pursuing an array of diverse activities, including technological assistance and training programmes, for the North Koreans. [...] The EU is an important supporter of peace on the Korean Peninsula and exchanges and cooperation between the South and North. You, the Members of the European Parliament are genuine friends of the Korean people. I earnestly hope that your unsparing support will continue until the day when peace is settled and the first ray of unification shines over the Korean Peninsula."(Address by Kim Dae Jung 2001)

Briefly, he believed that technological cooperation and expansion of economic activities between two sides would practically bring about the establishment of peace not only in the Korean Peninsula but also in Asia.

Ⅴ. Conclusion

This article has approached the topic of cyber security, focusing on the recently increasing cyber attacks from North Korea. Because the character of cyber terrorism crossing national borders, above all else, it is urgent to have a collective effort and cooperative policy to respond against these transnational threats. We have discussed in

detail about the threats that are present in cyber space. These problems are already global and there is indeed a limit to approach these kinds of terrorist acts only with a concerted effort from a group of nations. In other words, nationalism or a single national capability can't solve the increasing problem of cyber terrors. We should have a new way of cooperation in cyber security.

However, Northeast Asia truly lacks a sense of common security. Historically, Northeast Asia has never endeavored to cooperate for a collective security. In contrast to Europe, Northeast Asia is still under the circumstance of competitive nationalism and there is resulting national conflict amongst them. Therefore, the experiences and cases of the collective efforts in Europe are meaningful for the construction of Northeast Asia community, especially in cyber security. For example, Europol could be a good reference for the Northeast Asia in terms of its cyber security.

Finally, in regard to the solution to the increasing problem of cyber terrors, the construction of peace in Northeast Asia serves as the viable purpose. This can be achieved by sharing the consciousness of risk of cyber terrors and cyber challenges, sharing the information on threats and vulnerabilities of cyber attacks, and sharing the necessity of collective effort to respond against cyber terrors.

| 참고문헌 |

"Address by Mr Kim Dae Jung, President of the Republic of Korea (2001)." http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20011211&secondRef=ITEM-016&format=XML&language=EN. (accessed on June 20, 2013)

"Asian Security(2013)." www.tandfonline.com/loi/fasi20. (accessed on June 15, 2013)

"NKorea denies cyber attack on SKorean companies(2013)." http://www.huffingtonpost.com/2013/04/13/north-korea-denies-cyber-n_3076603.html. (accessed on June 20, 2013)

"North Korea training teams of 'cyber warriors' to conduct attacks (2013)." http://www.onenewspage.com/n/Front+Page/74vr1vhc2/North-Korea-training-teams-of-cyber-warriors-to.htm. (accessed on June 19, 2013)

"U.S. eyes N. Korea for 'massive cyber attacks'(2013)." http://www.nbcnews.com/id/31789294/ns/technology_and_science-security/t/us-eyes-n-korea-massive-cyber-attacks/#.UcvFeOuWG8g. (accessed on June 20, 2013)

"Urgency needed to deal with N Korea's cyber attacks (2013)." http://www.nationmultimedia.com/opinion/Urgency-needed-to-deal-with-N-Koreas-cyber-attacks-30204047.html. (accessed on June 19, 2013)

Buzan, Barry et al(1998). *Security: a New Framework for Analysis*. Colorado: Lynne Rienner Publishers, Inc.

Denning, Dorothy E.(2013). "Cyber Security as an Emergent Infrastructure." http://faculty.nps.edu/dedennin/publications/cyber%20security%20as%20emergent%20infrastructure.pdf. (accessed on June 20, 2013)

Elmusharaf, Mudawi Mukhtar(2004). "Cyber Terrorism: The new kind

of Terrorism." Computer Crime Research Center. April 08, 2004. http://www.crime-research.org/articles/cyber_terrorism_new_kind_terrorism. (accessed on June 21, 2013)

Groom, A.J.R.(1978). "Integration." Groom, A.J.R. and Mitchell, C.R. (eds.). *International Relations theory.* London: Francis Printer.

Haines, Lester(2013). "South Korea joins Galileo." http://www.theregister.co.uk/2006/01/12/korea_galileo. (accessed on June 20, 2013)

LEE, Kyu Young(2007). "European Intelligence Environment and Community in Post-Cold War Era." *National Strategy.* Vol. 13. No. 1, pp. 33-59. (in Korean)

Lee, Sunny(2011). "U.S. Security Strategy toward North Korea's Cyber Terrorism." Paper presented at 2011 Dupont Summit. Carnegie Institution for Science. Washington, DC. Dec. 2nd, 2011. http://www.ikupd.org/2013/34.pdf. (accessed on June 20, 2013)

Martinez, Luis(2013). "Intel Heads Now Fear Cyber Attack More Than Terror." http://abcnews.go.com/Blotter/intel-heads-now-fear-cyber-attack-terror/story?id=18719593#.UcB6RaWsa8g. (accessed on June 17, 2013)

Monnet, Jean(1976). *Memoires.* Paris: Fayard.

National Security Council(2013). "Cyber security." http://www.whitehouse.gov/cybersecurity. (accessed on June 15, 2013)

Sussmann, Michael(1999). "The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium." *Duke Journal of Comparative and International Law.* Vol. 9. No. 45.

US-China Economic and Security Review Commission(2008). "2008 Report to Congress. cited in China winning cyber war, Congress warned." *The Guardian* (online). 20 November 2008. http://www.guardian.co.uk/technology/2008/nov/20/china-us-mil

itary-hacking. (accessed on June 25, 2013)

| **논문투고일** : 2013년 11월 21일 |
| **논문심사일** : 2013년 11월 22일 |
| **게재확정일** : 2013년 12월 16일 |

ABSTRACT
Journal of Asia-Pacific Studies, Vol. 20. No. 3 (2013)

Cyber Security for the Construction of Northeast Asian Community

Kyu-Young LEE
(Graduate School of International Studies, Sogang Univ.)
Yoo-Joung KIM
(Department of History, Hankuk Univ. of Foreign Studies)

The article aims at underlining the necessity and importance of cyber security and try to search for implications and suggestions for the construction of the Northeast Asian community and policy cooperation regarding cyber security. In every aspect, society is becoming increasingly dependent upon information and communications technology (ICT). As a hub of personal, political and commercial activity, the internet has become indelibly important. In addition, connecting cyber space with national security, a militaristic war without guns has already started in cyber space among the most powerful states in the world.

In recent years, the security climate in Northeast Asia has deteriorated. This is of course due in part to the naked provocations of nuclear weapons and also due to hidden cyber attacks from North Korea. However, the energy security agenda is not as important as cyber security. In short cyber security is also gaining consideration, such as the military power of nuclear threat in these areas.

The main discussion will be concerned with these emergent threats in cyber space, the necessity and importance of cyber security in Northeast Asian areas, and the implications and suggestions for the

construction of Northeast Asian community and policy cooperation in cyber security. Focusing on these principal aims, this presentation consists of four major chapters: 1) Introduction; 2) The changing security environment and the cyber security in general; 3) Security environment and the cyber security in Northeast Asia; 4) Suggestions for the construction of the Northeast Asian community and multilateral policy cooperation in cyber security; and 5) Conclusion.

Key words: Cyber Security, Asian Community, Cyber Terror, European Union, North Korea