CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
CSC 32 / CCEM 32

EXERCISE/EXERCICE NEW HORIZONS

Cyber Warfare: Issues and Defense Efforts of Republic of Korea

By /par Cdr Mingoo Lee

I. Introduction

In the past, the pattern of war was conducted very independently, which means that tanks, warships and fighters often had to engage their opponents with a single weapon system without being supported or helped by high technology. However, today in order to carry out the missions successfully using C4ISR or PGMs for example, we have to rely almost totally on computer systems and networks. Furthermore, it is clear that military and civilian information networks are becoming greatly interdependent.

Many countries have already prepared for the futuristic war, which destroys the enemy's IT system by spreading viruses through the internet and military networks. In many ways, the Third World War seems to have already started in cyberspace. Due to the development of the Internet and intra-nets, the issues today are not only how to protect the networks but also to attack them. These issues have been the focus in many countries; this is particularly so in South Korea as it has one of the fastest growing IT environments which in turn makes the country more vulnerable to cyber attacks from other countries or hostile groups.

As a matter of fact, there are numerous reports on the huge damage and loss from failure to defend against cyber attack. Due to the independence of the networks in the military arena, it would be reasonable to consider what cyber-warfare has different aspects. In addition I, as a Republic of Korea's (ROK) military officer, would like to examine the ROK's efforts to digitize its military and to defend from the threats from outside.

So, I'm going to argue that our military and civilian networks are vulnerable to cyber attackers and hackers who attempt to take a lot of information away from the

military and the national defence research institutions and how we should prepare for the critical vulnerabilities that we are exposed to by hackers and how to secure our IT networks in order to improve our national security.

To achieve the objectives of this report, the definition and concept of cyber warfare will be examined firstly in Chapter II. In Chapter III, the ROK's effort to digitize its military and the dependence on Networks will be discussed.

In detail, the aims of the digitization of the military and the IT environment and its infrastructure will be included in Chapter III as well. In addition, ROK battlefield and resource management information systems will be analyzed. In Chapter IV, the threat of ROK digitization and its efforts will be studied. The on going issues relevant to cyber warfare in North Korea, the Peoples Republic of China (PRC) and Japan will be also examined in this chapter. In the last Chapter, after short summary of the examined results, the ROK's ongoing efforts and their policies for the future are briefly mentioned.

II. Definition and Concept of Cyber Warfare

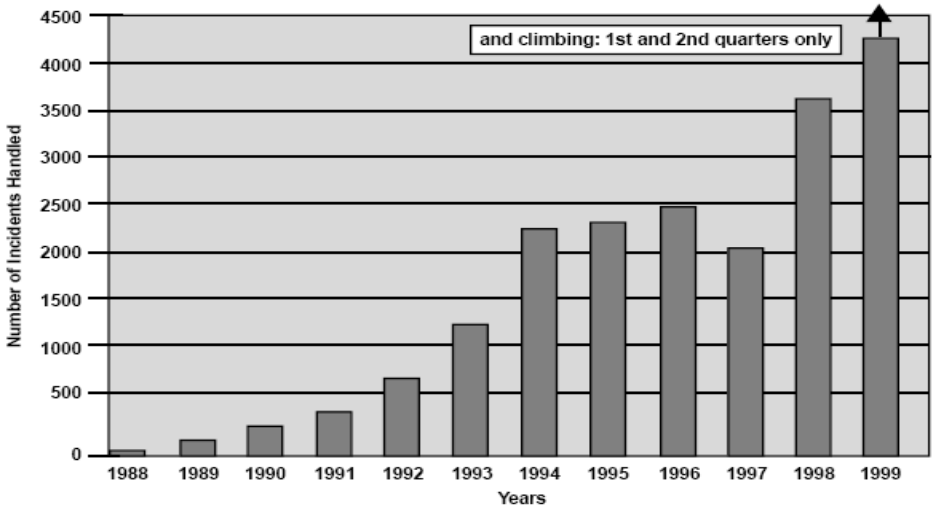
According to by Raymond C. Parks and David P. Duggan the definition of 'cyber warfare' is, "Cyber warfare is the sub-set of information warfare that involves actions taken within the cyber world."[1] On the one hand, Cyber warfare is a relatively new type of weaponry with various effects on the target. It doesn't have any limitations of use and can achieve most of the goals set.[2] The closest military definition of Cyber Warfare is a combination of computer network attack and computer network defence, and, possible

[1] Raymond C. Parks and David P. Duggan, "Principles of Cyber-warfare," Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June, 2001, 122.

[2] http://www.security-gurus.de/papers/cyberwarfare.pdf

special information operations[3]. From the definition, Parks and Duggan argued that the cyber world is any virtual reality contained within a collection of computers and networks. Therefore, I would say that Cyber Warfare is the conduct of military operations according to information-related principles. Today, especially in military and civilian societies which live in the information age, one of the gravest dangers in Cyber Warfare is the destruction of, or interference with, information infrastructure in such a manner as to cause devastating economic harm to a country.[4] Actually, we recognize the huge role of computer operations in current military operations; more over I am sure military operations will be more seriously threatened in the future due to cyber attack.

According to Parks and Duggan, there are many cyber worlds, but the one most relevant to cyber-warfare is the Internet and related networks that share media with the Internet.[5] As we can see from Figure 1 below, the tendency for Cyber Warfare and the number of networked software systems that are under attack is increasing.



[3] Raymond C. Parks and David P. Duggan, op. cit. 122.
[4] CDR Vida M. Antolin-Jenkins, Naval Law Review *"Defining the Parameters of Cyber War Operations: Looking for Law in All the Wrong Places?*" Judge Advocate General of the Navy, VOL., 51, 2005, 132.

[5] Ibid.

Figure1. Number of CERT Incidents Handled[6]

The definition of Cyber Warfare has not been found in *Joint Doctrine for Information Operation* published by Department of Defence (DoD) in 1998. However, the closest military definition to this term is 'a combination of computer network attack, and possibly special information operations.' According to the definition by DoD, computer network attack is "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves."[7]

How is Cyber Warfare different from information warfare? According to the definition by DoD, 'Information Warfare' is "Information Operations conducted during a the time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."[8] The differences between Cyber Warfare and Information Warfare can be found in the definition in that it does not specify the place where the warfare is taking place, while the cyber warfare has its specific space, the 'cyber world.' It can be inferred from the definition of 'kinetic warfare,' the term used by Parks and Duggan, who argued that the warfare practiced in the 'real world' where all the tanks, ships, planes and soldiers of current militaries are the protagonists of the warfare.[9]

---

[6] Luinel D. Alford, Jr., Cyber Warfare: Protecting Military Systems, Acquisition Review Quarterly – Spring 2000, 103.

[7] Department of Defence Joint Publication 3-13, Joint Doctrine for Information Operation, 9 October 1998, p. I-9. According to DOD, 'Special information operations' are information operations that, by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the US, require a special review and approval process. The same source, I-11.

[8] Ibid.

[9] Raymond C. Parks and David P. Duggan, op. cit., 122.

Even though there is different definition of information warfare[10], it can be said that information warfare has existed throughout the history of warfare. Because of the importance of information in war, Clausewitz states "imperfect knowledge of the situation... can bring military action to a standstill."[11] In addition, as indicated by Sun Tzu in 500 B.C., it has been argued that information is inherent in war fighting.[12] In fact, the rapid develop in information technology has made information systems easier to use, less expensive, and more available to a wide spectrum of potential adversaries and true enemies.

III. The ROK's effort to digitize its military and the dependence on Networks

A. Its aims, IT environment and infrastructure

According to the ROK Defence White Paper 2004, the objective of defence digitization is "to create a ubiquitous-based elite intelligent force by building an integrated information system that enables the sharing of information and knowledge both in war and peace as well as real-time distribution/utilization of such information and knowledge."[13]

In detail, the defence digitization aims to establish an integrated defence information system ensuring interoperability between the battlefield management

[10] USAF has described information warfare as a rather new realm. It has defined information war as "any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own information operations." In this context, information warfare "views itself as both separate realm and lucrative target." Information Warfare: Pouring the Foundation, Draft, Headquarters USAF, Deputy Chief of Staff, Plans and Operations, 10 November 1994, i, 3.

[11] Carl von Clausewitz, On War, ed. and trans. *Michael Howard and Peter Paret* (Princeton, N.J.: Princeton University Press, 1984), 84.

[12] Sun Tzu, trans, Samuel B. Griffith, *The Art of War*(New York; Oxford University Press, 1971), 84.

[13] ROK *Defense White Paper 2004*, Section 5, 112.

information system and resource management information system in order that information can be distributed and used on a real-time basis in accordance with the defence digitization environment and information & communication infrastructure.[14] The ROK's defence digitization objectives and aims are shown in Table 1, and have been divided into three strategic stages.

Table 1 Strategies by Stage

Stage	Goal	Priority
Stage 1 (2005-2009)	Established of the Infrastructure/ Core System	• Build and information and communication network-centered infrastructure
Stage 2 (2010-2015)	Completion of the integrated information system	• Build a ubiquitous infrastructure - Upgrade application systems and integrate related systems - Create a full-fledged ubiquitous environment
Stage 3 (2016-2020)	Establishment of a next generation advanced system	• Establish an advanced intelligent information system

Source: ROK *Defence White Paper*, 2004, p. 113.

The components of the ROK defence digitization environment include relevant institutions and procedures, organizations and manpower, interoperability and standardization, and sustained civilian-administrative- military cooperative ties. ROK

[14] Now, the Korean Military network is separated from the national high-speed communication network, so hacking and viruses might not be so serious, however in that case of the military network and national high-speed network will be interface each other in the future, the damage would be more much serious than we had expected.

Defence digitization has been pursued in constant reflection of the IT technologies' development trend.

Firstly, guidelines regarding defence planning and acquisition management documents are formulated and revised to improve related institutions and procedures. In addition, the ROK military is improving digitization project assessment and supervision procedures, while developing and introducing up-to-date business management techniques and mechanisms. Secondly, the CIO (Chief Information Officer) system is promoted, and the organization/manpower for policy formulation/execution and technological research are efficiently reinforced. Thirdly, common operational and data sharing environments are set up to ensure the sharing and joint use of the defence information system and information resources by all the Services for the promotion of interoperability and standardization. With the C4I system at the center, the ROK military pursues interfacing with other weapons systems including surveillance and strike systems, and builds a certification system to guarantee interoperability. Lastly, launch of a consultative body to utilize the national information infrastructure to the utmost possible extent is pursued to sustain civilian-administrative-military cooperative ties. At the same time, such events as technological symposiums on defence digitization should be held to promote technological exchanges related to military digitization.[15]

The ROK's information and communication infrastructure consists of an information and communication network, computer systems and information protection systems.

[15] Ibid, 113. If the military C4I systems are connected through Internet and civilian computer network, it will be very vulnerable and will be primary targeted by cyber attacker.

Firstly, the ROK military have built an integrated network that ensures real-time sharing of information and distribution of large multimedia contents (voice, texts, images and so on). The information and communication network operated by the ROK military is divided into strategic and tactical communication systems. In consideration of the BCN (Broadband Convergence Network) [16] establishment plan and application system development, the military information and communication system is being built based on the following approach: design of, and subsequent shift to, the NGN (Next Generation Network) [17] , and ultimate establishment of a ubiquitous-based information and communication network.

Secondly, in alignment with the establishment of the Mega Center, the ROK military is concentrating its efforts on building an infrastructure that encompasses the host and personal computers. Establishment of the Mega Center is aimed at integrating the scattered information and communication offices and host computers of individual Services into 61 information and communication centers. One pilot center was set up for each Service with a view to completing establishment of the Mega Center in phases. In terms of the dissemination of computer systems, distribution of host computers is being pursued in line with the concept of the Mega Center. At the same time, personal computers are being disseminated under the goal of achieving "one personal computer for each military personnel in charge." As of 2004, the dissemination rate of personal and

[16] An integrated broadband backbone network combining wired and wireless communication, Internet and broadcasting media which enables large-scale multimedia data distribution.

[17] A next-generation defense information communication network that enables interpretation of multiple backbone networks including defense information and communication networks and microwave networks, and local networks set up in individual echelons.

host computers of the ROK military stands at 94% and 96%, respectively. The military intends to raise the rate to 100% by 2007.[18]

A. ROK Battlefield and Resource Management Information System

Battlefield Management Information System

Regarding ROK's battlefield management information system, a joint C4I system is being built to support timely decision-making in alignment and interface with surveillance and strike systems, which enables "detecting, making decisions, and striking in advance of the enemy." In addition, interface between the national contingency planning system and the combined C4I system is to be developed to support potential total war and ROK-US combined operations. In that case of the US military, military C4I systems are extremely vulnerable because they interconnect. Military C4I uses interfaces through the Internet, base and organizational Local Area Networks (LAN), modems, civilian and military communication systems, navigation systems, and radios in all frequency ranges.[19]

The Joint Chiefs of Staff (JCS) have operated the CPAS (Command Post Automation System), which was developed to automate command post functions of the JCS Headquarters and major strategic and operational units of the three Services and to enable transmission/receipt of telegraphic messages to and from tactical units under their command. Recently, the JCS completed a conceptual research on the development of the KJCCS (Korea Joint Command and Control System), an upgraded form of the CPAS. By

[18] Ibid, 113-115.

[19] Lt Col. Lionel D. Alford, Jr., Cyber Warfare: Protecting Military Systems, 106.

pursuing the development of the KJCCS, the JCS intends to incorporate the system into force capabilities of related units.

In addition, the ROK military is pushing ahead with the establishment of an integrated military information processing system to allow real-time information sharing and distribution by all echelons through the joint C4I system. To attain the vision of a digitalized battlefield, the military seeks to set up a geographical information database management system by expressing its operational areas in numeric terms.

The ground-combat tactical C4I system aims to establish a combat command & control system based on real-time battlefield surveillance by automating the battlefield functions of tactical echelons of the corps or subordinate level. The system will provide a single corps first with targeting information, and then applied to all corps for its full-fledged incorporation into the military arsenal. The naval tactical C4I system, based on the existing Korean Naval Tactical Data System (KNTDS), will be built in a way that enables identification of maritime conditions on a real-time basis and command & control of integrated naval operations.

The air-combat tactical C4I system will serve as the core system that supports aerial operations including identification of current situation and decision-making by commanders and personnel of each operational echelon. It will be developed by 2007 in consideration of the interface and interoperability with the automated air defence system of the existing TACC and the MCRC (Master Control & Reporting Center).[20] Some personnel who experienced war in the past say almost half of the information delivered to commanders is false information. In particular, modern warfare is decided by how much exact information I have, and when we consider cyber war as a major means of war,

[20] Ibid, 117-118.

syntactic attacks and semantic attacks can be critical problems for a friendly side[21]. Because our command and control systems are rely heavily upon complicated computer networks, if any hacker aims at distorting or modifying the logic of the system, such as C4I, KJCCS, and puts malicious code into the system so as to be able to degrade decision-making, commanders will acquire false information and/or not use or trust the C2 system, with the consequence that their ability to control their sub units may be seriously compromised.

On the basis of its long-term vision to pursue the comprehensive development of modeling and simulation, the MND is building a simulation system that allows analysis of military principles, battlefield management concepts, unit structures, and operational plans appropriate for future warfare. Based on such effort, the MND is also setting up a decision-making and R&D simulation system that supports analysis and assessment for each stage of weapons system acquisition.

In addition, an education and training simulation system has been put into operation, based on the development of a model for each echelon including "Changjo 21", the training model for division and corps-level units of the ROK Army. In addition, the MND is to pursue the expansion of the training simulation system applicable to the JCS, individual Services, each echelon and each battlefield functions. The MND is also setting up the battalion-level Korean Army Advanced Combat Training Center (KCTC) to help troops with accumulated indirect warfare experience in simulated battlefield

[21] Syntactic attacks consists of modifying the logic of the system in order to introduce delays or to make the system unpredictable, on the other hand semantic attacks target not the computer's operation system but the accuracy of the information to which the computer user has access. CDR Vida M. Antolin-kenkins, Naval Law Review, 139.

environments to improve their capability to adapt to battlefield conditions as well as their tactical skills and capabilities.[22]

Now, a cyber situation room is running between DND and each service HQ, and it is able to conduct such operations as to being able to interrupt attempts at virus distribution and hacking, particularly as they relate to information missions. Meanwhile, DND planned to expand this system to brigade class units by 2005.[23]

Resource Management Information System

The MND is to pursue the establishment of the resource management information system to integrate resource management information mechanisms for efficient management of defence resources and improved execution of defence-related affairs. In addition, the MND aims to integrate the various resource management information systems in stages by 2013.[24]

IV. Threats of ROK Digitization and Its Defence Efforts

A. North Korea

Even though it has not been confirmed that South Korea's claims that Mirim or any other North Korean hacker academy even exists, there have been numerous reports which argue that North Korea has hacking capabilities.

According to the source from the Computer Crime Research Center, a military academy specializing in electronic warfare located in North Korea's mountainous

[22] Ibid, 118-119.

[23] www.segye.com/November 2, 2001.

[24] HR Information System, Mobilization Information System, Medical Information System, Logistics Information System, Electronic Procurement System, Facility Management System, Electronic Administration System.

Hyungsan region, (which is located in North-western North Korea), has been churning out 100 cyber-soldiers every year for nearly two decades. Graduates from the elite hacking program at Mirim College are very specialized in everything from writing computer viruses to penetrating network defences and programming weapon guidance systems.[25]

Even North Korea is believed to have paid some attention to the development of a range of military IW capabilities. The North Korean government claims that the country's communications network has been upgraded using fiber-optic cables; that the use of computers is being expanded; and that the computer networks of a number of the country's ministries and agencies, as well as its military units, are being increasingly connected. North Korea is also beginning to show interests in developing an indigenous computing capability and attempts to possess a large-scale computer production capability. These developments are thought to have led to an improvement in Pyongyang's hacking and virus insertion capabilities. Pyongyang believes that by using information technology, it will be able to catch up, and eventually surpass, more developed countries, not only in the commercial, but also in the military sphere.[26]

In 2005, according to a defence expert, there is another assessment of the North Korean cyber-warfare capability that allegedly reaches to a level capable of seriously disrupting the U.S. military. The expert argued that "a series of cyber simulations have

[25] *Hackers or cyber-soldiers?* Date: September 28, 2004 Source: Computer Crime Research Center By: Dmitri Kramarenko Dr. Vladimir Golubev, CCRC Director was interviewed by Mr. Bernhard Warner, European Internet Correspondent for Reuters. www.crime-research.org

[26] Damon Bristow, "Asia: grasping information warfare?" *Jane's Intelligence Review*, DEC. 01, 2000.

proven that North Korea's increased hacking capabilities could disrupt command and control elements of the U.S. Pacific Command.''[27]

In addition, North Korea currently runs a hacking unit of some 600 elite soldiers. Its military academy has been producing 100 cyber-soldiers every year since 1981. Graduates from the Mirim College, as mentioned above and also known as the Pyongyang Automated Warfare Institute[28], are skilled in everything from writing computer viruses to penetrate network defences and program weapon guidance systems. Though it has not been elaborated for security reasons, North Korea is allegedly also collecting information from South Korean institutions and research facilities through a total of 39 wiretapping devices, while waging a cyber war against other countries, including the U.S.[29]

B. Peoples Republic of China and Japan

According to the US Department of Defence (DoD), the PRC's offensive IW program is in the early stages of research. The DoD believes that China is studying offensive employment of IW against foreign economic, logistics, and command, control, communications, computers and intelligence (C4I) systems. Specifically, it is striving to

[27] In an annual conference on cyber security at Korea University in Seoul, Byun Jae-jung, a researcher at the Agency for Defence Development (ADD), said Pyongyang's computer hacking capabilities have reached the level of those of the U.S. Central Intelligence Agency (CIA). The Defence Information Security Conference was co-organized by the Defence Security Command, Korea Information Security Agency (KISA) and Korea University. *The Korea Times*, June 02, 2005. Also, it is known as the US DoD assessed that North Korea's computer hacking capability is reached to same level of CIA. www.segye.com, May 27, 2001.

[28] North Korea changed the institute's name to "Kim Il Military University" in the early 1990s and opened a computer college at Kim Il-sung University in 1998.

[29] *The Korea Times*, June 02, 2005. For example, North Korea has accessed the most numerous times to the US Army internet homepage for years and the information which was collected will be accumulated for cyber terror or cyber war. Jung Kyeong soo, The research on Korea's strategies against Cyber War (Seoul, Chosun University: 2003), 30.

establish a competence in attacking other countries' computers and researching methods to insert computer viruses into foreign military and civilian computer networks.

The People's Liberation Army (PLA) is working hard to put these technologies to practical use. Since 1997, the PLA has held a number of exercises in which it has attempted to interrupt, paralyze or destroy enemy broadcasting and military communications. China is also pursuing the concept of a Net Force (Battalion size), which would consist of a strong reserve force of computer experts trained at a number of universities, academies, and training centres.[30] Furthermore, at the October 2000 meeting of the Chinese Communist Party Central Committee in Beijing, it was believed that plans were adopted to streamline the military and introduce many of the technologies outlined above. New capabilities, including combined EW-armoured artillery divisions, are expected to be added to the PLA's existing 24 Group Armies[31] and China also considered establishing the 4th organization with exclusive responsibility for information warfare.[32] According to the US House of Representative in 1997, China has judged that Cyber Warfare is more effective strategically than nuclear war.[33]

Japan's susceptibility to IW attack has been highlighted by a series of attacks on government websites. In January 16, 2000, sixteen Japanese government websites including those of the Science and Technology Agency and the Mainichi Shimbum newspaper were hacked. Their content was erased and replaced with a Chinese message criticising Japan's role during the Nanjing massacre. Interestingly, in response to these

[30] Steven A. Hildreth, CRS Report for Congress, *"Cyber Warfare"* (Washington, Congress Library: 2001), 12.

[31] Damon Bristow, *op. cit*

[32] www.segye.com/May 27, 2001.

[33] www.donga.com/Jan 2, 2003.

attacks, the Tokyo Metropolitan Police Department announced that 12 of the e-mails had come through servers in the PRC. This prompted Raisuke Miyawaki, a former public relations advisor to former Prime Minister Yasuhiro Nakasone, to complain that these attacks clearly demonstrated the failure of Japanese government officials and business executives to "understand the latest technology involving information and communication using computers." However, this is not just a civil problem, because the military and civilian computer network systems are very closely connected.

For those reasons, the Japanese Defence Agency (JDA) was aware of the potential threat posed to Japan from cyber and other IW attacks. Japan's *Defence White Paper*, *The Defence of Japan 2000*, referred for the first time to the threat posed by IW. The paper stated that Japan was in the process of studying ways in which it should respond to attacks on its computer networks and JSDA should be able to establish a cyber-warfare unit to assess the threat from attack between 2001 through 2006.

However, in a frank admission of the degree to which Japan lagged behind in embracing the information revolution, the then Japanese Prime Minister, Yoshiro Mori, had promised that he would make Japan an advanced IT nation within five years. More specifically, Mori stated his intention to draw up a national IT strategy, the 'e-Japan plan', as soon as possible.[34]

In the *Japan's Defence White Paper 2005*, Japan reacts to the information technology revolution as follows:

[34] Mori also committed the government to creating an advanced online network in Japan to lower the costs of the country's Internet services, take steps to improve education in the area of IT and remove or ease current legislation that was hindering the spread of e-commerce in the country. Although little had officially been written on the subject, it was thought that, with its efforts to improve its information-gathering capabilities through the acquisition of observation satellites and airborne early warning aircraft, the JSDA was also developing a limited IW capability. Japan has already acquired electronic attack and electronic protection capabilities. Ibid.

● Creation of an Advanced Network Environment;

● Enhancing Command, Control, Communications, and Intelligence Functions; and

● Assurance of Information Security.

To protect the intelligence and communication infrastructure of the Defence Agency and the SDF that utilizes computers from cyber attacks, the Defence Agency is carrying out the following actions:

● Improvement in safety characteristics of the system itself (e.g. firewall);

● Improvement in protection capability of the system (e.g. constant surveillance by the protection unit);

● Improvement in rules to control and utilize the system;

● Enhancement of the capability of the system administrator, user etc;

● Sharing, etc. of security information with organs concerned; and

● Investigation and research of technology to react toward the most recent cyber issues.[35]

Along with the above, the Defence Agency actively contributes to the activities of the government including the sending off of personnel to the Cabinet Secretariat' National Information Security Center (NISC), and supporting the Cryptography Research & Evaluation Committees (CRYPTREC) mandated to the Ministry of Internal Affairs and Communications; and the Ministry of Economy, Trade and Industry.

C. ROK Defence Vulnerability to Cyber Warfare

Due to the efforts to digitize their national capabilities in Northeast Asian countries, South Korea is highly vulnerable to the crime of Cyber warfare and must be

[35] Japan *Defense White Paper 2005*, 77.

able to defend itself aggressively. For instance in 2000, it was reported that hacking attacks on high-profile commercial and government websites rose, between January and October of that year by up to 1,238.[36] Because of its highly wired broadband Internet infrastructure, South Korea is, ironically, rapidly emerging as one of the targets of international cyber attacks.

According to the National Police Agency, from August 2001 to March 2002, the country received a total of 4,376 reports on security breaches and hacker attacks in computer servers, accounting for 39 percent of worldwide online attacks. The US, China, and Taiwan ranked second, third and fourth, respectively.[37] The country's network security proved to be vulnerable again July 2005, when 250 computers in 10 government organizations were attacked through large-scale hacking, suspected to have originated in China. The National Police Agency, the National Assembly, state-run think tank the Korea Institute for Defence Analyses (KIDA) and the Agency for Defence Development (ADD) and US Forces Korea (USFK) were among the organizations whose websites were hacked.[38] In October 2005, the military's cyber security was tested again when personal information was stolen by computer hackers from the website of the MND HoGuk Foundation, an organization affiliated to the Defence Ministry.[39]

To overcome this vulnerability, in 2000 the South Korean MND and the National Intelligence Services issued reports advising not only that the country's armed forces

---

[36] Damon Bristow, *op. cit.*

[37] *The Korea Times,* May 25, 2003.

[38] www.segye.com/June 20, 2004. ADD and KIDA which was exposed to hacker in 2004 is the highest think tank in Korea that state-run. The major purpose of two organizations are to establish for national defence and research and development for high-tech weapons.

[39] *The Korea Herald*, March 23, 2006.

should "prepare for cyber warfare in the future from enemy countries," but also that they should consider establishing "specialist units for cyber warfare".[40] In the same year, the ROK government has also sent out an appeal to the country's universities asking for the assistance of hacker groups in dealing with the problem of cyber attacks and allocated $226,000 to fund the project.[41]

In its 2000 annual report, South Korea's Ministry of National Defence said a 5 percent budget increase was allocated mainly for projects such as "the build-up of the core capability needed for coping with advanced scientific and information warfare." The report also revealed that South Korea's military has 177 "computer training facilities" and had trained more than 200,000 "information technicians."[42]

In the *ROK Defence White Paper 2004*, the ROK revealed the Construction of the Cyber-War Platform. Saying that the evolution of computerization, information network and various accompanying services has brought about consequences along the way, the ROK MND acknowledging that such that negative developments may trigger a cyber-war, established cyber-war doctrines to formulate a cyber-war platform, and formed a master plan to protect information and improve intelligence capabilities.

More widely, while it has erected an integrated security control system at the corps level or above, a single anti-virus system across all the forces, and a MND authentication system, it also continues to train cyber-war specialists, maintain

[40] Damon Bristow, op. cit.

[41] Ibid.

[42] Dmitri Kramarenko, op. cit.

collaborative and cooperative relationships with external institutions and provides improved training on INFOCON to gear up for encroachment through the cyber world.[43]

Under the ROK defence information protection system, the Computer Emergency Response Team (CERT) continues to be operated by the MND and individual Services. Based on the establishment of an integrated security control system for units at the level of a command or higher and a single anti-virus system for all the Services, the ROK military is tackling possible threats to its information systems including hacking and viruses on a real-time basis. In addition, it is reinforcing its exercises according to the INFOCON to gear up for potential enemy infiltrations for cyber warfare. Currently, cyber attacks including hacking against government agencies are on a gradual rise, inflicting substantial damage. To brace for such cyber attacks, close civilian-government-military cooperation is being promoted to promptly activate a response system of the agencies concerned in the event of an emergency.[44]

As one of academic circles' efforts to increase cyber warfare capabilities, in 2005, Byun, a researcher at the Agency for Defence Development, called on the government to increase the budget for the build-up of the core capability needed to cope with advanced scientific and information warfare, especially for the protection of information.[45]

In 2006, the ROK military has launched plans to revise defence laws relating to cyber warfare in a move to cope with this newly emerging dimension of national defence. Military authorities have assessed the cyber warfare capabilities of neighboring countries

[43] ROK *Defence White Paper 2004*, 189.

[44] Ibid, 116.

[45] *The Korea Times,* May 25, 2003.

such as China, Japan and North Korea as threatening, and recognized the necessity of such measures.

Speaking on the condition of anonymity, an official said "To combat cyber attacks in the event of war, (We are) planning to revise related laws including the integrated defence law and martial law, and enact new laws by June."

The revisions are mainly aimed at establishing the legal grounds to sufficiently mobilize manpower, equipment and budget in countering possible cyber attacks from enemy states against the country's defence computer systems or the government's communication networks. The military also plans to improve the ability of its cyber teams to counter an attack through improvements in organization and personnel training.[46]

V. Conclusion: Cyber-warfare

How can we imagine the impact on national security and the economy if an electric or nuclear power plant is prevented from operating by cyber attacker aimed at cyber warfare for a certain period, such as just one day or one week? It would clearly be an unpredictable situation.

The definition of the cyber world is any virtual reality contained huge amounts of information within a collection of computers and networks. There are many cyber worlds, but the one most relevant to cyber-warfare is the Internet and related networks that share media with the Internet. This is where the information stays, exchanges, and recreates its own values.

[46] *The Korea Herald*, March 23, 2006.

As I am interested in cyber-warfare, the relevant parts in the ROK Defence White Paper 2004 have been examined. If the ROK is to be able to defend itself in the age of cyber warfare, it needs to pursue defence digitization, with the objective of creating an ubiquitous-based elite intelligent force, and by building an integrated information system that enables the sharing of information and knowledge both in war and peace as well as real-time distribution/utilization of such information and knowledge.

The components of the ROK defence digitization environment include relevant institutions and procedures, organizations and manpower, interoperability and standardization, and sustained civilian-government-military cooperative ties. ROK Defence digitization has been pursued and may be seen as a constant reflection of the IT technologies' development trend.

As to the assessment of cyber threat from North Korea, the PRC and Japan, it has been assessed that North Korea has the capability for cyber warfare. Due to some antagonism between China and Japan, there are growing concerns about possible conflicts in the cyber worlds. In reality, there are many hacking records between those countries.

Since security in virtual reality is no less crucial than that on the ground or in the air, it is reasonable for countries to be prepared for possible nightmare scenarios in which power supplies, communications and financial infrastructure can be severely disrupted by an attack in cyberspace.

In this regard, I would say that the ROK Ministry of Information and Communications and other governmental and civilian authorities should learn lessons from other countries which have moved far ahead in gearing up for cyber war.

In real war, computer technology can play an ingenious part in a classical strategy for information operations by destroying communication infrastructures or leaking wrong messages. At the same time, even the so-called smart bombs used by US armed forces in Iraq are considered to be cutting-edge weaponry with the capacity to knock out electricity supplies when detonated. However, they to maybe vulnerable to hacking attacks which could render them unusable.

As one of the most densely wired countries in the world, South Korea is among the most vulnerable to the risks of cyber war. Thorough and ongoing assessments are still necessary in order to determine the need to build cyber warfare platforms that will make a country secure from cyber warfare threats and attacks. It is becoming increasingly evident that information security is one of the major keys to success in today's conflicts and wars. So Cyber Warfare is becoming more and more powerful in today's battlefield both during peace and war and when we use it effectively, we can have superiority against adversaries threatening our country.

Biography

Raymond C. Parks and David P. Duggan, "Principles of Cyber-warfare," Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June, 2001.

CDR Vida M. Antolin-Jenkins, Naval Law Review *"Defining the Parameters of Cyber War Operations: Looking for Law in All the Wrong Places?*" Judge Advocate General of the Navy, VOL., 51, 2005.

Luinel D. Alford, Jr., Cyber Warfare: Protecting Military Systems, Acquisition Review Quarterly – Spring 2000.

Department of Defence Joint Publication 3-13, Joint Doctrine for Information Operation, 9 October 1998.

Information Warfare: Pouring the Foundation, Draft, Headquarters USAF, Deputy Chief of Staff, Plans and Operations, 10 November 1994.

Carl von Clausewitz, On War, ed. and trans. *Michael Howard and Peter Paret* (Princeton, N.J.: Princeton University Press, 1984).

Sun Tzu, trans, Samuel B. Griffith, *The Art of War* (New York; Oxford University Press, 1971).

Lt Col. Lionel D. Alford, Jr., Cyber Warfare: Protecting Military Systems

ROK *Defense White Paper 2004*, Section 5.

Japan *Defense White Paper 2005*, 77

Damon Bristow, "Asia: grasping information warfare?" *Jane's Intelligence Review,* DEC. 01, 2000.

Jung kyeong-soo, The research on Korea's strategies against Cyber Warfare (Seoul, Chosun University: 2003)

Steven A. Hildreth, CRS Report for Congress, *"Cyber Warfare"* (Washington, Congress Library: 2001).

Maj. Beaton, Exercise New Horizon "The sovereign nature of cyber warfare" (Toronto, CFC: 2003)

Others

www.segye.com/May 27, 2001.

www.segye.com, May 27, 2001.

www.segye.com/June 20, 2004.

www.segye.com/November 2, 2001.

www.security-gurus.de/papers/cyberwarfare.pdf

www.donga.com/Jan 2, 2003.

www.crime-research.org

www.endtimesreport.com/NK_cyber-war.htm

The Korea Times, May 25, 2003.

The Korea Times, June 02, 2005.

The Korea Herald, March 23, 2006.