The Strategy to Secure Cyber Security in the Age of Cyber Crisis

Gi Geun Yang

Wonkwang University, South Korea

In this paper I seek to strategies to secure cyber security. First of all, In this paper I explore overview of strategies to secure cyber security in the U.S.. and in South Korea. The purpose of this article is to describe an ongoing cyber security policies that explores the analysis between U.S and Korea cyber security national preparedness. To achieve purpose of research, First, we examines the strategy of Cyber Security Research and Development Policies in the U.S. and then, this study makes several suggestions to improve cyber security in Korea.

Key Words: cyber security, cyber terrorism, critical infrastructures, cyber crisis management.

Ⅰ. Introduction

The IT infrastructure is highly vulnerable to premeditated attacks with potentially catastrophic effects. Thus, it is a prime target for cyber terrorism as well as criminal acts. The IT infrastructure encompasses not only the best-known uses of the public Internet – e-commerce, communication, and Web services – but also the less visible systems and connections of the Nation's critical infrastructures such as power grids, air traffic control systems, financial systems, and military and intelligence systems. The growing dependence of these critical infrastructures on the IT infrastructure means that the former cannot be secure if the latter is not(PITAC, 2005).[1)]

Sound national cyber security policy depends on understanding the problem, its solutions, and the nature of cyber conflicts from economic, behavioral, and political perspectives. Unfortunately, our understanding is currently quite limited. In such a circumstance, a sound policy would be to place high priority and urgency on gaining a deep understanding of all these areas.

Today hacking and virus get more and more burdensome in promoting safe Internet culture over the time in . Almost all systems connected to the super-high speed Internet network are attacked every several minutes or even every several seconds while users are not acknowledged. To cope with this, government has devoted its energy to effective countermeasures to hacking and viruses such as cyber attack countermeasure methodology and technical response to attack tools.

To prevent the infringement cases and minimize the

1) See http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

damage in Korea, Cyber Security Management System of Korea will take the lead in raising technical capability for protection of Critical Network Infrastructure Internet communication network and for reinforcement of prediction and alarm system.

This paper overview of the strategy to secure cyber security. The purpose of this article is to describe an ongoing cyber security policies that explores the analysis between U.S and Korea cyber security national preparedness. To achieve purpose of research, First, we examines the strategy of Cyber Security Research and Development Policies in the U.S. and then, this study makes several suggestions to improve cyber security in Korea.

II. Background

The information technology is a double edge sword, which can be used for destructive as well as constructive work. Thus, the fate of many ventures depends upon the benign or vice intentions, as the case may be, of the person dealing with and using the technology. For instance, a malicious intention forwarded in the form of hacking, data theft, virus attack, etc can bring only destructive results. These methods, however, may also be used for checking the authenticity, safety and security of one's technological device, which has been primarily relied upon and trusted for providing the security to a particular organization.

1. Threats to Critical Infrastructures

Dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often 24 hours a day, and electronic mail, Internet Web sites, and computer bulletin boards allow us to communicate quickly and easily with an unlimited number of individuals and groups(GAO, 2004: 3-4).[2)]

Table 1. Threats to Critical Infrastructures Observed by the FBI

Threat	Description
Criminal groups	There is an increased use of cyber intrusions by criminal groups who attack systems for monetary gain.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities.
Hackers	bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Information warfare	Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of Central Intelligence, can affect the daily lives of Americans across the country.
Insider threat	The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors.
Virus writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and ""worms"" have harmed files and hard drives, including the Melissa macro virus, the Explore. Zip worm, the CIH (Chernobyl) virus, Nimda, and Code Red.

Source: GAO(2004: 4). See www.gao.gov/cgi-bin/getrpt?GAO-04-628T. aPrepared statement of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, February 2, 2000.

However, this widespread interconnectivity poses significant risks to the government's and our nation's computer systems and, more important, to the critical operations and infrastructures they support. For

2) See www.gao.gov/cgi-bin/getrpt?GAO-04-628T.

example, telecommunications, power distribution systems, water supplies, public health services, national defense, law enforcement, government services, and emergency services all depend on the security of their computer operations. If they are not properly controlled, the speed and accessibility that create the enormous benefits of the computer age may allow individuals and organizations to eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage.

2. Cyber terrorism

Terrorism may be generally defined as politically motivated violence to coerce a government or civilian population. In the wake of the terrorist attacks on September 11, 2001, seven new national strategies were developed and published to help guide U.S. efforts to combat terrorism. Of these, five were newly published strategies that related to specific aspects of homeland security and combating terrorism, such as weapons of mass destruction, protecting physical infrastructure, and securing cyberspace(GAO, 2004: 4-5).[3)]

The most deadly and destructive consequence of this helplessness is the emergence of the concept of "cyber terrorism". The traditional concepts and methods of terrorism have taken new dimensions, which are more destructive and deadly in nature. In the age of information technology the terrorists have acquired an expertise to produce the most deadly combination of weapons and technology, which if not properly safeguarded in due course of time, will take its own toll. The damage so produced would be almost irreversible and most catastrophic in nature. In short, we are facing the worst form of terrorism popularly known as "Cyber Terrorism". The expression "cyber terrorism" includes an intentional negative and harmful use of the information technology for producing destructive and harmful effects to the property, whether tangible or intangible, of others. For instance, hacking of a computer system and then deleting the useful and valuable business information of the rival competitor is a part and parcel of cyber terrorism. The definition of "cyber terrorism" cannot be made exhaustive as the nature of crime is such that it must be left to be inclusive in nature. The nature of "cyberspace" is such that new methods and technologies are invented regularly; hence it is not advisable to put the definition in a straightjacket formula or pigeons hole. In fact, the first effort of the Courts should be to interpret the definition as liberally as possible so that the menace of cyber terrorism can be tackled stringently and with a punitive hand. The law dealing with cyber terrorism is, however, not adequate to meet the precarious intentions of these cyber terrorists and requires a rejuvenation in the light and context of the latest developments all over the world. The laws have to take care of the problems originating at the international level because the Internet, through which these terrorist activities are carried out, recognizes no boundaries. Thus, a cyber terrorist can collapse the economic structure of a country from a place with which a country may not have any reciprocal arrangements, including an "extradition treaty". The only safeguard in such a situation is to use the latest technology to counter these problems. Thus, a good combination of the latest security technology and a law dealing with cyber terrorism is the need of the hour(Computer Crime Research Center, 2006)[4)]

3. Dramatic Growth in Security Vulnerabilities

The Nation's IT infrastructure has undergone a dramatic transformation over the last decade. Explosive growth in the use of networks to connect

3) See www.gao.gov/cgi-bin/getrpt?GAO-04-408T.

4) See http://www.crime-research.org/articles/1873 (2008.5.14)

various IT systems has made it relatively easy to obtain information, to communicate, and to control these systems across great distances. Because of the tremendous productivity gains and new capabilities enabled by these networked systems, they have been incorporated into a vast number of civilian applications, including education, commerce, science and engineering, and entertainment. They have also been incorporated into virtually every sector of the Nation's critical infrastructure -including communications, utilities, finance, transportation, law enforcement, and defense. Indeed, these sectors are now critically reliant on the underlying IT infrastructure.

At the same time, this revolution in connectivity has also increased the potential of those who would do harm, giving them the capability to do so from afar while armed with only a computer and the knowledge needed to identify and exploit vulnerabilities. Today, it is possible for a malicious agent to penetrate millions of computers around the world in a matter of minutes, exploiting those machines to attack the Nation's critical infrastructure, penetrate sensitive systems, or steal valuable data. The growth in the number of attacks matches the tremendous growth in connectivity, and dealing with these attacks now costs the Nation billions of dollars annually. Moreover, we are rapidly losing ground to those who do harm, as is indicated by the steadily mounting numbers of compromised networks and resulting financial losses(PITAC, 2005: 1).

The number of malicious attacks has increased with the growing number of vulnerabilities[5]in U.S. In 2000, the Software Engineering Institute's CERT® Coordination Center(CERT/CC)[6] received 1,090 reports of security vulnerabilities. By 2005, this number had more than quadrupled to 5,990. Figure 1 illustrates the number of security reported from 1995 through 2005(GAO, 2006: 5-6).

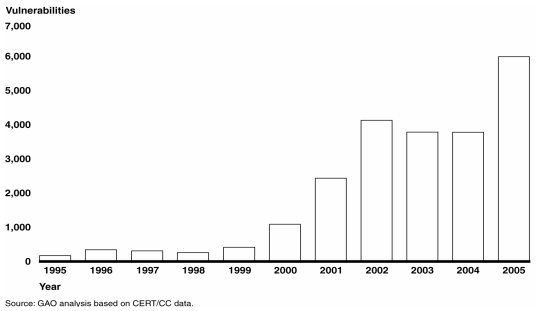


Figure 1. Security Vulnerabilities, 1995-2005

The violations came on the heels of the Korean largest hacking incident, in which Internet Auction, the biggest online shopping mall, was found to have mistakenly leaked the data of almost 11 million customers. All this indicates how lax the nation's laws and regulations are on cyber privacy and how fatally generous society is with identify thieves and fraudsters(The Korea Times, 2008.4.25)[7].

III. Overview of Cyber Security Research and Development Policies in the U.S.[8]

Recently, U.S. selected cyber security as one of the most important area in national R&D priorities. Because of increases in security vulnerabilities, protecting both the public and private systems that support critical operations and infrastructures of the federal government has never more important. Federal law and policy call for critical infrastructure protection activities to enhance the cyber and physical security of

5) A vulnerability is a flaw or weakness in hardware or software that can be exploited, resulting in a violation of an implicit or explicit security policy.

6) The CERT®/CC is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

7) See http://www.koreatimes.co.kr/www/news/opinon/2008/04/197_23164.html (2008.5.17)

8) GAO(2006). 「Information Security: Coordination of Federal Cyber Security Research and Development」. GAO-06-811(Washington, D.C.: Sept. 29, 2006).

the infrastructure that are essential to national security, national economic security, and national public health and safety.

1. Cyber Security R&D Policies, Organizations and Fund

The National Strategy for Homeland Security sets out a plan to improve homeland security through the cooperation and partnering of federal, state, local, and private sector organizations on an array of functions.[9] The strategy organizes these functions into six critical mission areas:[10] Intelligence and Warning, Border and Transportation Security, Domestic Counterterrorism, Protecting Critical Infrastructure and Key Assets, Defending Against Catastrophic Threats, and Emergency Preparedness and Response. The strategy also identifies the major initiatives to be addressed within each of these six mission areas(GAO, 2005: 4-5).[11]

Over the years, the federal government has taken these and other actions to improve cyber security efforts:

First, publishing best practices and guidelines that assist in the planning, selection, and implementation of cyber security technologies;

Second, partnering with private sector counterparts to assess vulnerabilities and develop plans to eliminate those vulnerabilities; and

Third, awarding grants to support cyber security R&D.

1) Federal Cyber Security Research and Development Policies

Research associated with enhancing the cyber security of critical infrastructures has been reinforced through federal requirements aimed at improving the nation's cyber security posture. Additional requirements for research can be found in legislation that establishes agency responsibilities. For example, the act that establishes the Office of Science and Technology Policy gives the office the responsibility of assisting the President in providing general leadership and coordination of the research programs of the federal government.[12] To provide a historical perspective, table 2 summarizes the key federal cyber security R&D actions that have shaped the development of the federal government's cyber security R&D policies.

9) There were several other related national strategies issued subsequent to the National Strategy for Homeland Security. These include the National Money Laundering Strategy, the National Security Strategy, the National Strategy to Combat Weapons of Mass Destruction, the National Strategy for Combating Terrorism, the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, and the National Strategy to Secure Cyberspace. For our analysis of all of these strategies, see www.gao.gov/cgi-bin/getrpt?GAO-04-408T.

10) The strategy also includes a discussion of ""foundations,"" which we did not identify separately in our analysis. The strategy describes these foundations as unique American strengths that cut across all sectors of society, such as law, science and technology, information sharing and systems, and international cooperation. The discussion of these foundations overlaps with the six mission areas. For example, the initiative to improve international shipping security is covered by both the mission area of Border and Transportation Security as well as the foundation of international cooperation. To some extent, our discussion of crosscutting issues also acknowledges issues that cut across all sectors.

11) See www.gao.gov/cgi-bin/getrpt?GAO-05-33.

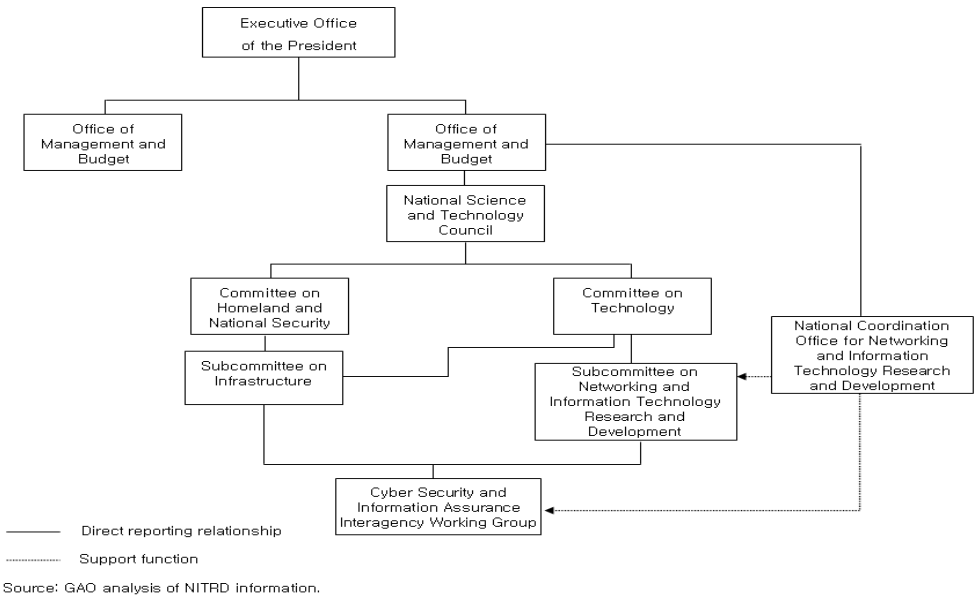
12) Pub. L. 94-282, Presidential Science and Technology Advisory Organization Act, May 11, 1976.

Table 2. Key Federal Government Actions on Cyber Security R&D

Actions	Date	Description
Cyber Security Research and Development Acta	November 2002	Enacted to enhance cyber security research efforts. Authorizes the National Science Foundation and the National Institute of Standards and Technology to award grants and establish programs aimed at enhancing computer security and related research partnerships. Defines the responsibility of the Director of the Office of Science and Technology Policy in working with the directors of the National Science Foundation and the National Institute of Standards and Technology to ensure programs authorized by the act are accounted for in governmentwide cyber security research efforts.
National Strategy to Secure Cyberspace	February 2003	Provides direction to the federal government's departments and agencies that have roles in cyberspace security and outlines an initial framework for both organizing and prioritizing efforts. It identifies five national priorities, one of which includes reducing cyberspace threats and vulnerabilities. As part of this priority, the Director of the Office of Science and Technology Policy is to coordinate the development, and update on an annual basis, a federal government R&D agenda for cyber security.
President's Information Technology Advisory Committee report	February 2005	The President's Information Technology Advisory Committee is a federally chartered advisory committee operating under the Federal Advisory Committee Actb whose members were appointed by the President to provide independent, expert advice on advanced information technology issues. It conducted a review of the focus, balance, and effectiveness of federally funded cyber security R&D projects. The results of the review were published in a February 2005 reportc that recommends several changes in the federal government's cyber security R&D portfolio. One of the report's recommendations was to strengthen coordination and oversight of federal cyber security efforts.

Source: GAO analysis of federal policy documents and report. aPub. L. 107-305, Cyber Security Research and Development Act, November 27, 2002. bPub. L. 92-463, Federal Advisory Committee Act, October 6, 1972. cPresident's Information Technology Advisory Committee, Cyber Security: A Crisis of Prioritization (Washington, D.C.: Feb. 28, 2005).

2) Federal Structure for Oversight and Coordination of Cyber Security Research and Development



Source: GAO analysis of NITRD information.

Figure 2. Organization of Federal Cyber Security R&D Oversight and Coordination

Numerous entities are involved in federal cyber security research and development. The Office of Science and Technology Policy(OST) and Office of Management and Budget(OMB), both in the Executive Office of the President, provide high-level oversight of federal R&D, including cyber

security(GAO, 2006: 8-9). The Office of Science and Technology Policy oversees the National Science and Technology Council, which prepares R&D strategies that are coordinated across federal agencies. The council operates through its committees, subcommittees, and interagency working groups. The Subcommittee on NITRD and the Interagency Working Group on Cyber Security and Information Assurance are the key entities responsible for coordinating cyber security R&D activities among federal agencies. The organization chart in figure 2 depicts the federal organizations involved.

While this chart illustrates that several organizations are involved, much of the coordination for cyber security research is actually accomplished at lower level working groups and subcommittees.

2. Key Agencies Fund and Conduct Cyber Security Research

While there are multiple agencies involved, three agencies fund and conduct much of cyber security R&D: the National Science Foundation and the Department of Homeland Security and Defense.

In 2004, he National Science Foundation established the Cyber Trust program to complement ongoing cyber security investments in each of its core research areas: computer and networked systems, computing and communication foundations, information and intelligence systems, shared cyber infrastructure, and information technology research. In accordance with the Cyber Security Research and Development act, the National science Foundation awards Cyber Trust grants for three projects. Recent Cyber Trust grants include research in areas such as approaches to Internet security, system behavior monitoring, and information security risk management architecture. The President's budget for fiscal year 2006 provides about $94 million to the National Science Foundation for cyber security research, education, and training.

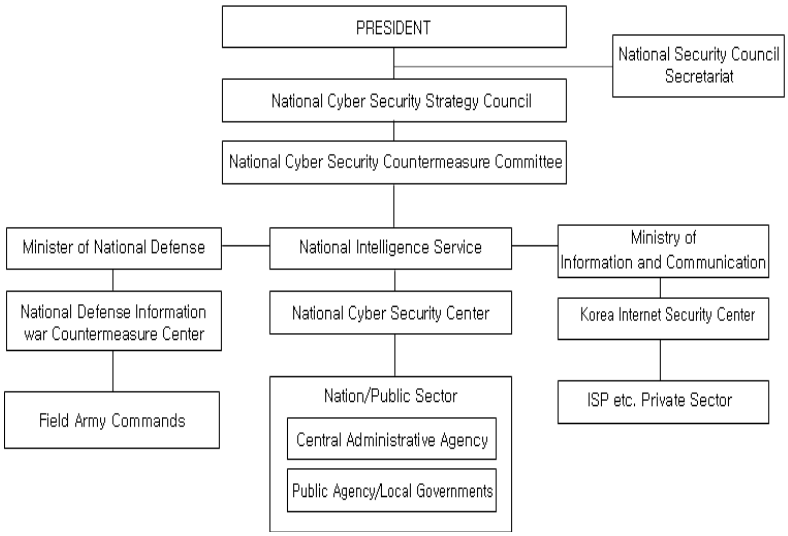
The Department of Homeland Security's cyber security R&D program resides in the agency's Science and Technology Directorate. According to GAO's report(2006), Department of Homeland Security's cyber security R&D program was funded with approximately $10 million in fiscal year 2004, $18 million in fiscal 2005, and $17 million in fiscal 2006.

Several agencies within the Department of Defense have cyber security R&D program. According to Department of Defense officials, its cyber security research programs totaled about $150 million in fiscal year 2005. Although the Department of Defense's research organizations have cyber security programs, the largest investments within its cyber security program are with the Defense Advanced research Agency Projects Agency and the National Security Agency. The Defense Advanced Research Projects Agency is the central R&D organization of the Department of Defense. And the National Security Agency also performs extensive cyber security research.

IV. The Strategy to Secure Cyber Security in Korea

1. Cyber Security Management System of Korea

With growing importance of cyber security, Government established National Cyber Security Management Regulation - Presidential Direction No. 141- for cyber security management. Numerous national agencies and organizations are involved in nationally funded cyber security policies and countermeasures. The National cyber Security Strategy Council provides national-level oversight of cyber security policies. The organization chart in figure 3 depicts the national organizations involved.



Source: National Cyber Security Center(http://www.ncsc.go.kr/eng/ ; 2008.5.15)

Figure 3. Comprehensive System for Cyber Security Management

2. Findings and Implications in Cyber Security R&D Policies of U.S.

In this study on Cyber Security R&D Policies of U.S., we have found a few key findings. First, the cyber security budget of U.S. has kept increasing. This is thanks to laws and regulations such as Cyber Security Research and Development Act of 2002 (CSRDA) that promotes cyber security investment indirectly and effectively. Second, the policies emphasize cooperation between public sector and private sector. Third, cyber security laws and organizations are amended and newly established.

3. Policy Proposals for Further Development in Korea

First, we must gradually increase the share of information security R&D in national. We are recommending that korea establish firm timelines for the completion of national cyber security R&D agenda.

Second, with the entry into a ubiquitous society, they are reinforcing research on solutions related to social engineering and non-technological means rather than solutions focused on technologies. On the report "Cyber Security: A Crisis of Priortization" by PITAC, US raised the necessity of research and development on non-technological issues which cannot be addressed by network and software engineering.

Third, we have to establish governance network for building public-private partnerships. Recently the terms "governance" and "good governance" are being increasingly used. What is good governance? The concept of "governance" is not new. It is as old as human civilization. Simply put "governance" means: the process of decision-making and the process by which decisions are implemented or not implemented. So, we can describe public-private governance as a subset discipline of Corporate Governance focused on cyber risk management. As an example, see CSRDC in U.S. The Cyber Security R&D Center(CSRDC) was established by the Department of Homeland Security in 2004 to develop security technology for protection of the U.S. cyber infrastructure. The Center conducts its work through partnerships between government and private industry, the venture capital community, and

the research community.[13]

Fourth, in accordance with the cyber crisis, government enacts internet laws for cyber security. Today Cyber Terror Protection Act being discussed in korea. I think that this is a good chance in the ongoing cyber trust society.

Fifth, international cooperation is indispensable to the effective protection of cyber crisis Management. The problems associated with the cyber crisis are not peculiar to any particular country as the menace is global in nature. The countries all over the world are facing this problem and are trying their level best to eliminate this problem. The problem, however, cannot be effectively curbed unless popular public support and a vigilant judiciary back it. The legislature cannot enact a law against the general public opinion of the nation at large. Thus, first a public support has to be obtained not only at the national level but at the international level as well.

Finally, is it true that cyber crisis recur? From an academic perspective, focused research can improve our understanding of how to make lesson learning work well. If we don't learn past lessons, we failed to fix the problems that injured cyber world the last time. Thus, at all levels of government to give serious attention to the goal of inculcating a culture of learning from past cyber terrorism to prevent future losses.

V. Conclusions: For Cyber Trust

From the above discussion it should be clear that cyber trust is very dangerous and security vulnerabilities have increased. We cannot emphasis too about the cyber security. Information Technology(IT) is a rich repository of natural economic growth for our future. The IT infrastructure of all country today is essential to the functioning of government, private enterprise, and civil society, including its critical systems for water, energy, transportation, and public safety.

In other words, cyber trust is very important in the age of cyber crisis. So, Nations is both warranted and needed to encourage development of long-term goals and technical strategies for improving the overall security of this vital national interest.

However, as we have seen, this paper is based on literature review only. Thus, this study has many limits. I will go on study of cyber crisis and cyber security.

13) See http://www.cyber.st.dhs.gov/

<References>

▷ Amy K. Donahue and Robert V. Tuohy. 2006. Lessons We Don't Learn: A Study of the Lessons of Disasters, Why We Repeat Them, and How We Can Learn Them. *Homeland Security Affairs*. 2(2); http://www.hsaj.org.

▷ Interagency Working Group (IWG) on Cyber Security and Information Assurance. 2006. Federal Plan for Cyber Security and Information Assurance Research and Development. *National Science and Technology Council*; http://www.nitrd.gov/pubs/csia /csia_federal_plan.pdf

▷ National Information Society Agency. 2007. Information Security Research and Development of Advanced Countries in 2007. *NIA I-RER-07043(Seoul: December, 2007)*; http://www.nia.or.kr/.

▷ President's Information Technology Advisory Committee. 2005. *Cyber Security: A Crisis of Prioritization*(Washington, D.C.: Feb. 28, 2005). http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/ cybersecurity.pdf.

▷ U.S. General Accounting Office. 2004. Combating Terrorism : Evaluation of Selected Characteristics in National Strategies Related to Terrorism. *GAO-06-811(Washington, D.C.: Feb. 3, 2004)*; www.gao.gov/cgi-bin/getrpt?GAO-04-408T.

▷ U.S. General Accounting Office. 2004. Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems. *GAO-04-628T(Washington, D.C.: March 30, 2004)*; www.gao.gov/cgi-bin/getrpt?GAO-04-628T.

▷ U.S. General Accounting Office. 2005. Homeland Security Agency Plans: Implementation, and Challenges Regarding the National Strategy for Homeland Security. *GAO-05-33 (Washington, D.C.: January 14, 2005)*; www.gao.gov/cgi-bin/getrpt?GAO-05-33.

▷ U.S. General Accounting Office. 2006. Information Security: Coordination of Federal Cyber Security Research and Development. *GAO-06-811(Washington, D.C.: Sept. 29, 2006)*; www.gao.gov/cgi-bin/getrpt?GAO-06-811.

한국위기관리논집 제4권 제2호 2008. 12 104~114쪽

▷ http://dhs.gov/
▷ http://www.crime-research.org/articles/1873
▷ http://www.dhs.gov/index.shtm
▷ http://www.fema.gov/
▷ http://www.koreatimes.co.kr/www/news/opinon/ 2008/04/197_23164.html
▷ http://www.ncsc.go.kr/
▷ http://www.nitrd.gov/
▷ http://www.nitrd.gov/subcommittee/csia.php
▷ http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

Gi Geun Yang: He received the Ph.D. in Public Administration from Kyunghee University, Korea in 2004. Since 2008, he has been with the Division of Fire Service Administration. His main research interests include Crisis Management and Fire Policy(withgg@wku.ac.kr).

접수번호: #081030-02
접수일자: 2008. 10. 30.
심사완료: 2008. 12. 15.