Analysis and Improvement Strategies for Korea's Cyber Security Systems Regulations and Policies

Park, Dong-Kyun* · Cho, Sung-Je** · Soung, Jea-Hyen***

<Contents>

Ⅰ. Introduction
Ⅱ. Korea's Cyber Security Laws and Policy Implementation
Ⅲ. Problems and Improvements of Cyber Security Systems
Ⅳ. Conclusion

<요 약>

Today, the rapid advance of scientific technologies has brought about fundamental changes to the types and levels of terrorism while the war against the world more than one thousand small and big terrorists and crime organizations has already begun.

A method highly likely to be employed by terrorist groups that are using 21st Century state of the art technology is cyber terrorism. In many instances, things that you could only imagine in reality could be made possible in the cyber space. An easy example would be to randomly alter a letter in the blood type of a terrorism subject in the health care data system, which could inflict harm to subjects and impact the overturning of the opponent's system or regime.

The CIH Virus Crisis which occurred on April 26, 1999 had significant implications in various aspects. A virus program made of just a few lines by Taiwanese college students without any specific objective ended up spreading widely throughout the Internet, causing damage to 30,000 PCs in Korea and over 2 billion won in monetary

* Professor, Department of Police Administration, Daegu Haany University, first author
** Professor, Department of Police Administration, Daegu Haany University, corresponding author
*** Lecturer, Department of Law, Hankuk University of Foreign Studies, co-author

damages in repairs and data recovery. Despite of such risks of cyber terrorism, a great number of Korean sites are employing loose security measures. In fact, there are many cases where a company with millions of subscribers has very slackened security systems. A nationwide preparation for cyber terrorism is called for. In this context, this research will analyze the current status of Korea's cyber security systems and its laws from a policy perspective, and move on to propose improvement strategies.

This research suggests the following solutions.

First, the National Cyber Security Management Act should be passed to have its effectiveness as the national cyber security management regulation. With the Act's establishment, a more efficient and proactive response to cyber security management will be made possible within a nationwide cyber security framework, and define its relationship with other related laws. The newly passed National Cyber Security Management Act will eliminate inefficiencies that are caused by functional redundancies dispersed across individual sectors in current legislation.

Second, to ensure efficient nationwide cyber security management, national cyber security standards and models should be proposed; while at the same time a national cyber security management organizational structure should be established to implement national cyber security policies at each government-agencies and social-components. The National Cyber Security Center must serve as the comprehensive collection, analysis and processing point for national cyber crisis related information, oversee each government agency, and build collaborative relations with the private sector. Also, national and comprehensive response system in which both the private and public sectors participate should be set up, for advance detection and prevention of cyber crisis risks and for a consolidated and timely response using national resources in times of crisis.

Key Words : Cyber Terrorism, Cyber Security Systems, Industrial Technology Protection, Information Communications Infrastructure Protection, National Cyber Security Center

I. Introduction

Since the collapse of the world order defined as the cold war, the terrorism has became a daily event in the international society attributed to a variety of disputes such as territorial conflicts from ethnic religions, the world struggling to come up with measures against terrorism.

Asia Pacific regions are outstanding in its strategic importance by the existence of U. S., Japan, China, Russia, etc, as well as in its economic dynamics, especially the Korean peninsula, the area of vital strategic importance, supposedly being put under considerable influences regarding its diplomatic standings in relations with its neighbours(Dong Kyun Park, Ik Ju Shin , 2007: 161).

What each nations in the world share in their efforts to fight against terrorism may come down to legislating against terrorism, organizing an exclusive institution for anti-terrorism, specializing the anti-terrorism agents and enhancing the security clearances at the airport(Seok Heon Jang, 2006: 89). Similarly, if late, Korea also needs to climb on the bandwagon by making a law to isolate the terrorism and establishing a special anti-terrorism institution, finally enhancing its counter-terrorism measures including to prevent, crackdown and research the terrorism and to promote campaigns against it.

Today, the rapid advance of scientific technologies has brought about fundamental changes to the types and levels of terrorism while the war against the world more than one thousand small and big terrorists and crime organizations has already begun.

A method highly likely to be employed by terrorist groups that are using 21st Century state of the art technology is cyber terrorism(Haugh, R.: 2003). In many instances, things that you could only imagine in reality could be made possible in the cyber space. An easy example would be to randomly alter a letter in the blood type of a terrorism subject in the health care data system,

which could inflict harm to subjects and impact the overturning of the opponent's system or regime.

Thus, terrorists prefer cyber terrorism over other physical terrorism methods because they may inflict greater harm with less cost. Unlike bombings or kidnapping hostages, cyber terrorist may invade their terror subjects anywhere anytime on the Internet(David F Forte, 1986).

With the North American Treaty Organization(NATO)'s misdirected shelling of the Chinese Embassy and its damage inflicted on China, a number of Chinese hacked into the White House and the U. S. Department of State web sites. This caused the web site of the White House to show various Chinese and English character scribblings, rending it inaccessible for an extended time(Edward A. Lynch, 1987).

In June of 1998, immediately following India's nuclear testing, Dutch and British university students posted a mushroom image that symbolized nuclear weapons on the web site of the Nuclear Weapons Research Institute of India. In September of 1998, Portuguese hackers invaded the systems of some 40 regions in Indonesia and created hyper links to a web site that criticized the human rights conditions in Indonesia.

The CIH Virus Crisis which occurred on April 26, 1999 had significant implications in various aspects. A virus program made of just a few lines by Taiwanese college students without any specific objective ended up spreading widely throughout the Internet, causing damage to 30,000 PCs in Korea and over 2 billion won in monetary damages in repairs and data recovery(Dong Kyun Park, Ik Ju Shin , 2007: 161).

Despite of such risks of cyber terrorism, a great number of Korean sites are employing loose security measures. In fact, there are many cases where a company with millions of subscribers has very slackened security systems. A nationwide preparation for cyber terrorism is called for. In this context, this research will analyze the current status of Korea's cyber security systems and its laws from a policy perspective, and move on to propose improvement strategies.

Ⅱ. Korea's Cyber Security Laws and Policy Implementation

Korea's cyber security systems are governed based on the National Cyber Security Management Act(Executive Instructional Order 222), the Information Technology Infrastructure Protection Act(Code No. 8852), Information Technology Network Use Promulgation and Information Protection Act(Code No. 8867), Industrial Technology Information Security and Protection Act(Code No. 8900), Software Industry Promotion Act(Code No. 8852), etc. However, Korea lacks an integrated and systematic national cyber security policy, and policies are scattered throughout laws and regulations of various sectors such as those related to the national core infrastructure protection, information communication networks, industrial technology information, private sector software industry information, etc. As a result, cyber security organizations are also dispersed throughout various sectors and form the national cyber crisis management organizational structure, This includes the National Cyber Security Center, the Information Communication Infrastructure Protection Commission, the Private Information Conflict Mediation Commission, the Industrial Technology Protection Commission, the Software Business Conflict Mediation Commission. This current state requires a more systematic policy approach.

An analysis on Korea's current status of cyber security in the legal and policy perspective will be elaborated, based upon which derivative problems and future improvement strategies will be discussed.

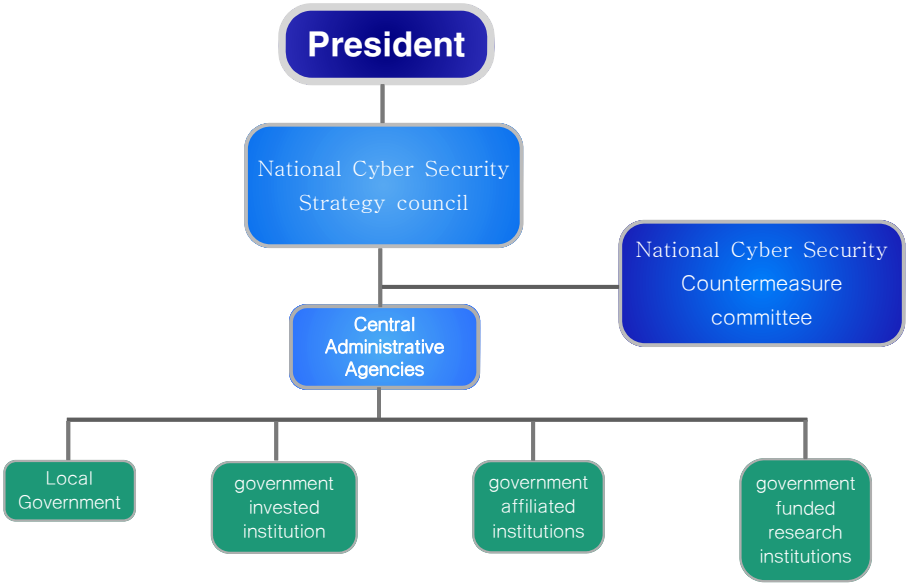
1. Status of Korea's Cyber Security Management System

The National Cyber Security Strategy Council was set up to discuss important issues such as the institution and improvement of a national cyber security management system, establishment of policies and interagency coordination, and the National Cyber Security Task force Council was

established for efficient operations of this National Cyber Security Strategy Council for national cyber security management and countermeasures. In addition, for a comprehensive and systematic national approach to cyber attacks the National Cyber Security Center of the National Intelligence Service was appointed to oversee national cyber security policy making; cyber risk information collection, analysis and dissemination; cyber attack incident investigations and recovery support; and national information communication network security verification. Central government agencies have been assigned to establish and implement cyber security measures for information communication network security enhancements.

In addition, a collaboration system was founded for inter-organizational cyber attack information sharing and a reporting mandates to the National Intelligence Service whenever incidents occur or risks are discovered. In the break out of a wide-span incident, the National Intelligence Service is to form and operate a joint governmental investigation team and a recovery support team. Cyber security technology development has been delegated to the National Security Technology Research Center(http://www.ncsc.go.kr).

<PICTURE 1> National Cyber Security Control System



2. The National Cyber Security Strategy Council and the National Cyber Security Task force Committee

In Korea, the National Cyber Security Strategy Council was established for deliberation of important issues on national cyber security, and the Strategy Council is chaired by the Head of the National Intelligence Service. The Strategy Council members consists of the Deputy Ministers of the Ministry of Education, Science and Technology, the Ministry of Foreign Affairs and Trade, the Ministry of Justice, the Ministry of National Defense, the Ministry of Public Administration and Security, the Ministry of Knowledge and Economy, the Ministry for Health, Welfare and Family Affairs, the Ministry of Land, Transport and Maritime Affairs, as well as the President's Office Diplomacy and Security Chief of Staff, the Korea Communication Commission Standing Committee Member, the Financial Supervisory Commission Deputy Chair, and a deputy minister-level public official of a central government agency designated by the Strategy Council Chair.

The Strategy Council will discuss: ① establishment and improvement of the national cyber security system, ② national cyber security related policies and interagency coordination, ③ implementation measures for executive directives related to national cyber security, and ④ other matters raised by the Strategy Council Chair (National Cyber Security Management Code No. 6). In addition, for efficient operations of the Strategy Council, the council is mandated to retain a National Cyber Security Task force Committee. The Task force Committee Chair is to be the Deputy Chief of cyber security affairs for the National Intelligence Service, and Committee members consists of section head public officials of each Strategy Council member's ministries. The Task force Committee shall discuss: ① National Cyber Security Management and Counter measures, ② implementation measures of Strategy Council decisions, ③ matters assigned by the Strategy Council or its Chair, and ④ other matters raised by the Task force Committee Chair(National Cyber Security Management Code No. 7).

3. National Cyber Security Center

The National Intelligence Service launched a National Cyber Security Center in February of 2004 to oversee national cyber security measures, and in January 2005 based on the National Cyber Security Management Act (Executive Instructional Order 141) the Security Center has been in charge of establishing national cyber security policies, operational support for the Strategic Council and the Task force Team, collection, analysis and dissemination of national cyber security information, verification of the national information communication network, among others, to enable comprehensive and systematic countermeasures for cyber attacks.

First, to oversee the national cyber security policies, the Center established and operates programs for cyber security policy planning and coordination, established national cyber security related programs and guidelines, operates the National Cyber Security Strategy Council and Task force Committee, and cyber security information sharing programs among the private, government and military sectors.

Second, as a national cyber security assurance and preventative measure, the Center performs national information communications network security verifications, information security level evaluations, cyber security mock training sessions, information communications network security reviews and security-level evaluations.

Third, as part of its activities for comprehensive collection, analysis, and dissemination of national cyber risk information, the Center monitors cyber security status of major agencies, announces official warnings for risk levels such as normal-attention-warning-risk-high risk, disseminates security analyses information, and develops cyber security technology, 24 hours 365 days a year.

Fourth, as part of its emergency response, investigation and recovery efforts following attack incidents, the Center registers cyber attack incidents, investigates incidents, develops countermeasures, takes preventative action of

further escalation, provides recovery support, and establishes and operates a government-wide joint investigation a recovery support team.

In addition, the Center hosts a collaborative board for Korea's cyber security specialized institutions, has established collaborative relations with advanced nations(i.e. the United States, Great Britain, France, Germany, Canada, Japan, etc.), and holds invitational seminars and events with international experts. Meanwhile, the Center has joint operations with designated government officials and assigned researchers from the National Security Technology Research Center, Korea Information Protection Promotion Agency, etc. to ensure proper coordination of cyber security measures.

4. Information Communications Infrastructure Protection Committee

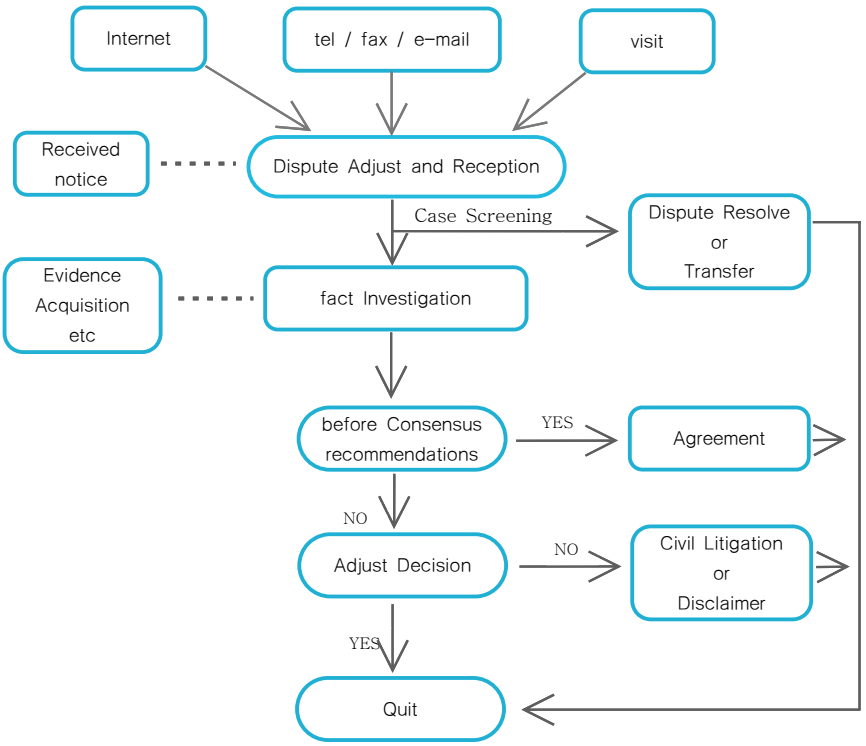
To discuss major information communications infrastructure protection issues, an Information Communications Infrastructure Protection Committee was established under the umbrella of the Prime Minister. The law sets forth that the Committee shall discuss: ① policy coordination for the protection of major information communications infrastructure, ② comprehensive coordination for protection plans of major information communications infrastructure, ③ issues related to implementation outcomes of protection plans for major information communication infrastructures, and ④ major information communication infrastructure protection systems improvements (the Information Communications Infrastructure Protection Act, Article 3 and 4).

5. The Private Information Conflict Mediation Commission

As a dispute mediation institution founded in December 2001, based on Article 33 of the Information Communications Network Use Promotion and Information Protection Act, an office was established within the Korea Information Protection Promotion Agency for the Conflict Mediation Committee. For efficient coordination of conflict mediation, the laws sets forth that a Coordination Section composed of 5 or less members of the Conflict Mediation Committee shall be established, one of whom shall be a licensed

attorney. Matters related to formation and operations of the Coordination Section is to be administered by the Ministry of Public Administration and Security (Information Communication Use Promotion and Information Protection Act, Article 33). The Mediation Committee not only protects citizens' rights but also enhances business efficiency contributing to building sound distributive order, through various recurrence prevention measures such as by mediating private information conflicts between users and businesses, providing damage prevention promotions and training, making suggestions for legal improvements, advising corrective actions to business transaction models and user agreements, processing of violation incidents, etc.(Private Information Conflict Mediation Committee).

<PICTURE 2> Committee Adjust Procedure



6. Industrial Technology Protection Committee

The Industrial Technology Protection Committee is the highest decision-making organization created based on the 'Industrial Technology Information Protection Act,'which launched on April 28. It is formed by a total of 23 members, including 17 government committee members from government agencies(i. e., related central government agency heads and intelligence investigative agency heads, etc.) and 6 commissioned members from the private sector. For deliberation of industrial technology information protection issues, the Industrial Technology Protection Committee was established under the auspices of the Prime Minister. The Committee head shall be the Prime Minister, and members shall consist of: ① a member who is a head of a related central government agency designated by the President, ② a member who is the head of a intelligence investigation agency responsible for industrial technology information protection, ③ a member with expert knowledge and experience in the industrial technology information protection field designated by the Protection Committee, etc. The Minister of Knowledge and Economy serves as its advisor. The law sets forth that the Minister of Knowledge and Economy shall establish procedural directives by which to protect industrial technology information, after consultation with related central government agency heads and the Protection Committee, and enable relevant institutions to utilization of these directives (Industrial Technology Protection Act, Article 7 and 8).

The Protection Committee operates under a diverse opinion gather process related to national core technology selection process with related government ministries by means of surveys and meetings with industries, researchers and academia, etc., and makes minimal appointments after considering national security, national economic impact, international and domestic market share of related products, research trends and technology expansion and compatibility within respective fields, etc. Based on concerns of negative effects that national core technology export restrictions may pose on corporate

global strategies and the corporation's participation in national research and development, prudent implementation plans are set in place. For national core technologies that received national research and development support, an export approval process is in place based on the evaluation of its national security and national economic impact. For technology developed independently by private sector entities which may have a serious impact on national security, ex post de facto measures such as export suspension, prohibition or return orders to original states will be taken(Ministry of Knowledge and Economy Press Release).

7. Software Industry Conflict Mediation Committee

It is difficult for the software industry to have a definitive contract objective in the initial phases of projects, and there are often wide opinion gaps between the client and business' interpretation of objectives. This makes accountability a grey area in times of conflict, causing escalation of discord between the client and business. Rather than conflict resolution by court proceedings, a software business conflict mediation system has been introduced to save time and money by promoting settlements between contesting parties. A Software Industry Conflict Mediation Commission has been established under the Ministry of Knowledge and Economy to provide mediation services related to software ventures. The Mediation Committee evaluates and mediates disputes at the request of either or both parties. However, their services exclude cases that require legal interpretation of contacts to which the government is a party, cases to which subcontractor transaction fairness regulations apply, and issues to which the user agreement restriction laws apply.

The Mediation Committee mediates disputes related to: ① software business between the client and producer, ② accountability between joint contractors or between contractors and subcontractors for a software project, ③ accountability between the contactor and a third party for a software project, ④ guarantor accountability between software project contractor and a guarantor of the contact, and ⑤ accountability between involved parties to a

software project(Software Industry Promotion Act, Article 37).

Ⅲ. Problems and Improvements of Cyber Security Systems

Cyber space is a virtual space connected by a network of information technology devices, computers and the Internet, and has already settled itself as a common territory in citizen's daily lives. It transcends national borders, across the globe, and is closely intertwined with government and private sector participation. Based on such unique aspects, it is developing complex and highly advanced, and posed definite limits on either the government or the private sector to block cyber attacks that may occur without any limits on time and location. Moreover, cyber crises that are caused by cyber attacks may develop into a nationwide crisis even when targeted to a specific person, unlike physical order disruptions in reality. Risk for cyber catastrophes that may impose national and social damage, such as the 1.25 Internet Crisis that caused the paralysis of major nationwide information communication networks and lead to the leakage of national security and advanced technology from organized cyber attacked from overseas. However, as Korea does not have specific ways or procedures and policies set in place to manage a cyber crisis at the national level, a cyber crisis incident may pose a serious risks and great damage to national security and interests(Security News, 2008).

As previously mentioned, Korea's legal system for cyber crisis management are governed based on the National Cyber Security Management Act (Executive Order 222), the Information Technology Infrastructure Protection Act (No. 8852), Information Technology Network Use Promulgation and Information Protection Act (No. 8867), Industrial Technology Information Security and Protection Act (No. 8900), Software Industry Promotion Act (No. 8852), etc. Thus, there is an absence of a comprehensive and systematic policy for national cyber crisis, currently scattered around fields of national core technology protection, information communication networks, industrial technology information, private software industry information, etc. This

current states calls for the imminent action on establishing proper policies. In addition, national cyber security organizational structures are dispersed throughout sectors (the National Cyber Security Task force Committee, National Cyber Security Center, Information Communication Infrastructure Protection Commission, Private Information Conflict Mediation Commission, Industrial Technology Protection Committee, Software Industry Conflict Committee, etc. and requires action.

In the past, government-wide cyber attack response functions were disperse among the National Intelligence Service, the Ministry of National Defense and the Ministry of Information and Communication, and lacked in security programs, manpower and equipment with inadequate cyber attack crisis management response. To address this task at hand, on August 18, 2008, the National Cyber Security Management Act (Executive Instructional Order) came into effect. The Act set forth national cyber security related organization structural and operational issues and strengthened interagency collaboration for cyber security. To protect national information communication networks from cyber attacks that threaten national security, the National Cyber Security Strategy Council, the National Cyber Security Task force Team was established, in addition passing legislation so that the National Cyber Security Center could be established within the National Intelligence Services. However, the National Cyber Security Management Act was of a directive nature, it was conflictive of related Information Communication Infrastructure Protection Act (Code No. 8852), Information Communications Network Use Promotion and Information Protection Act (Code No. 8852), Industrial Technology Information Protection Act (Code No. 8900), the Software Industry Promotion Act (Code No. 8852), etc. Provisions of each of these Acts had varying subjects to protect from cyber crises, and had redundant organizational structures and functions under each Act.

Therefore, to resolve problem areas identified above, the National Cyber Security Management Act should be amended so that national cyber security management regulations may be properly effective. If the National Cyber Security Management Act has been established, this will enable effective and

proactive response to cyber security management within the framework of a comprehensive system of cyber security at a national level. The newly revised National Cyber Security Legislation will eliminate inefficient redundancies in cyber security functions that are scattered based on a number of laws.

Korea has developed into an advanced nation in information technology over the years through initiatives such as developing e-government, information technology industry promotion, etc. For sustained information technology development information security strengthening measures is needed. In this regard, we must be able to securely protect the networks, equipment, facilities, software and its systems related to information collection, processing, storage, retrieval, transmission, receipt, use, and others in the forms of communication infrastructures of wire, wireless, light beam, satellite as well as electronic formats. Information infrastructure protection regulations should be expanded to cover diverse structures from only the major information communication infrastructures, and more effort should be invested in stipulating basic areas in national information protection such information infrastructure protection measures, attack response systems, information protection training and promotions, etc. (Korea Policy Portal, 2008).

As was seen from the 1.25 Internet Crisis (On January 25, 2008, the Internet was entirely paralyzed, causing a crisis and approximately 220 billion won in damages), the cyber attacks are rapidly emerging as a nationwide and social threat and is a direct risk factor to national security. Each national worldwide are fiercely engaging cyber information warfare to exploit the opponent nation's secrets or national functions (June 2004 government agency system hacking incident originating from China; May 2004 attempts to paralyze Estonia's information communications networks originating from Russia). As cyber attacks may have a serious national and social impact on a nation or society, it has already been identified as a new national security risk factor to which a response system by private and public sectors has faced its limits. Korea does not have policies, specific methods and processes with which to systematically mange nationwide cyber crises, and could cause a great threat and serious damage to national security and national interest in the

break out of a cyber crisis. Therefore, legislation must be passed to enable pre-cyber attacks detection and prevention of crisis break outs, and to consolidate all national resources for a comprehensive national response system in which both the private and public sectors participate(Security News, 2008).

Second, efficiently ensure nationwide cyber security, a national cyber security standard and models should be proposed, and meanwhile a national cyber security management structure and system should be established to implement national cyber security policies at each government-agency and social-component levels. By developing a consistency in information protection laws, policies and programs through integrating and revising legislation and implementation systems, we will be able to more effectively respond to various threats to information protection. Therefore, the government should expand and strengthen the functions of its current 'National Cyber Security Center' to perform its integrated national cyber crisis management role in the areas of national cyber security management policy planning and coordination. Foremost, it must serve as the comprehensive collection, analysis, and processing of national cyber crisis related information, oversee each government and public agency, and establish a collaborative system with the private sector.

For voluntary information protection level evaluations public agencies' Information Protection Management System authentications should be expanded; new regulations on administrative information protection system selections and use should be passed to simplify procurement of information protection products at administrative offices and propel their use; and establish regulations that promote sharing of attack information; and by setting attack information sharing regulations among information systems operators and information sharing/analysis centers, etc., so that we may effectively protect our national and social facilities from cyber attacks(Korea Policy Portal, 2008).

Also, a nationwide and comprehensive response system in which both government and the private sectors participate should be established to cyber

attack detections before the fact and to block cyber crisis risks at an earlier stage, and in case of a breakout a nationwide effort shall be mobilized for quick response(Security News, 2008).

Finally, the National Cyber Security Center should serve the following functions. It's major roles should include: 1) major policy planning, oversight and coordination related to national cyber security management; 2) planning and coordinating national cyber security management systems, warnings, drills, practice, and evaluations, etc.; 3) coordination and council on national cyber security management institutional efforts; 4) integrated response execution and coordination in the occurrence of a national cyber crisis; 5) establishment and implementation of national cyber crisis preventative policies; 6) determination of emergency response measures to be implemented by individual institutions in time of a national cyber attack incident; and 7) development of damage recovery and stabilization measures following a national cyber crisis.

Ⅳ. Conclusion

Korea's cyber security systems are governed based on the National Cyber Security Management Act (Executive Order 222), the Information Technology Infrastructure Protection Act (No. 8852), Information Technology Network Use Promulgation and Information Protection Act (No. 8867), Industrial Technology Information Security and Protection Act (No. 8900), Software Industry Promotion Act (No. 8852). Therefore, Korea lacks a systematic national cyber security policy. In addition. cyber security organizations, including the National Cyber Security Center, Information Communication Infrastructure Protection Commission, Private Information Conflict Mediation Commission, Industrial Technology Protection Commission, Software Business Conflict Mediation Commission, etc., are also dispersed over various sectors, and needs to be reorganized. Therefore, this research suggests the following solutions.

First, the National Cyber Security Management Act should be passed to have its effectiveness as the national cyber security management regulation. With the Act's establishment, a more efficient and proactive response to cyber security management will be made possible within a nationwide cyber security framework, and define its relationship with other related laws. The newly passed National Cyber Security Management Act will eliminate inefficiencies that are caused by functional redundancies dispersed across individual sectors in current legislation.

Second, to ensure efficient nationwide cyber security management, national cyber security standards and models should be proposed; while at the same time a national cyber security management organizational structure should be established to implement national cyber security policies at each government-agencies and social-components. The National Cyber Security Center must serve as the comprehensive collection, analysis and processing point for national cyber crisis related information, oversee each government agency, and build collaborative relations with the private sector. Also, national and comprehensive response system in which both the private and public sectors participate should be set up, for advance detection and prevention of cyber crisis risks and for a consolidated and timely response using national resources in times of crisis.

References

Arthur J. Bilek · Peter P. Lejins · Clifford W. Van Meter (1997), *Private Security*, Anderson Publishing co.

Beck, U. (1998), *Risk Society: Towards a New Modernity*(translated by Mark Ritter). London: Sage Publications.

Benjamin Netanyahu (1986), *Defining Terrorism: How The West Can Win?,* New York: Farrar.

Cigler, Beverly A. (1988), "Emergency Management and Public Administration." in Michael T. Charles & John Choon K. Kim (eds.). *Crisis Management : A Casebook*. Springfield, Ⅲ: Charles C. Thomas Publisher. 5-19.

Clary, Bruce B. (1985), "The Evolution and Structure of Natural Hazard Policies", *Public Administration Review.* 45: 20-24.

David F Forte (1986), *Terror and Terrorism : There is Difference*. Ohio Northern University Law Revieu.

Dong Kyun Park · Ik Ju Shin (2007), "Case Analysis on Counter-Terrorism for International Events and Political Implications", *Study on Security.* 13 : 161-179.

Edward A. Lynch (1987), "International Terrorism: The Search for a Policy". *Terrorism.* 9: 1-5.

Haugh, R. (2003), Cyber Terror. *Hospitals & health networks.* 77(6): 15-20.

Holman, K. (2008), Cyber Terror Threat Looms: Financial industry infrastructure still at risk, group says. *Investment Dealers Digest.* 74(5): 20-28.

Korea Information Security Agency. The Private Information Conflict Mediation Commission: http://www.kopico.or.kr/

Korea political measures portal(2008. 9. 1). "Information Communications Infrastructure Protection"

Korea internet security center : http://www.krcert.or.kr

Korea information security agency : http://www.kisa.or.kr

Ministry of Knowledge and Economy Press Release(2008. 8. 21) "Industrial Technology Protection general planning decision"

National Intelligence Service (2001), *Characteristics of New Terrorism and the Move of Overseas Counter-Terror Reinforcement.*

National Security Research Institute : http://www.nsri.re.kr

National cyber security center : http://www.nsri.re.kr

National intelligence service : http://www.ncsc.go.kr

Prosecutors′ office: http://icic.sppo.go.kr

Robert L. O′ Block & Joseph F. Donnermeyer & Stephen E. Doeren (1991), *Security and Crime Prevention*(Boston: Butterworth-Heinemann), 322.

Robert R. Robinson, Issues in Security Management (1999), *Thinking Critically About Security*, Butterworth-Heinemann, 14.

Security News (2008), "21C the National Cyber Security Management Act (Executive Instructional Order 222) verification"

Seok Heon Jang (2006), Study on Counter-Terrorism Solutions for major National Facilities, *The Korean Society of Private Security.* 8: 89.

Siegel, G. B. (1985), "Human Resource Development for Emergency Management", *Public Administration Review.* 45 : 113-116.

National Cyber Security Management Code.

Software Industry Promotion Act, Article 37.

The Information Communications Infrastructure Protection Act, Article 3 and 4.

ABSTRACT

Analysis and Improvement Strategies for Korea's Cyber Security Systems Regulations and Policies

Park, Dong-Kyun · Cho, Sung-Je · Soung, Jea-Hyen

21세기 첨단기술을 활용하고 있는 테러집단들이 앞으로 활용할 가능성이 높은 방법 중의 하나가 바로 사이버테러이다. 현실에서는 상상만으로 가능한 일이 사이버 공간에서는 실제로 가능한 경우가 많다. 손쉬운 예로 병원에 입원 중인 요인들의 전산기록 중 혈액형 한 글자만을 임의로 변경하여도 주요 인물에게 타격을 주어 상대편의 체제전복에 영향을 줄 수 있다. 이와 같이 테러분자들이 사이버테러를 선호하는 이유는 다른 물리적인 테러수단 보다 적은 비용으로 큰 효과를 거둘 수 있기 때문이다. 폭탄설치나 인질납치 보다 사이버 테러리스트들은 인터넷으로 언제 어디서나 공격 대상에 침투할 수 있다.

1999년 4월 26일 발생했던 CIH 대란은 여러모로 시사하는 바가 크다. 대만의 대학생이 뚜렷한 목적 없이 만들었던 몇 줄짜리 바이러스 프로그램이 인터넷을 통해 기하급수적으로 퍼져 국내에서만 30만대의 PC를 손상시켰고, 수리비와 데이터 복구에 소요된 비용만 20억원 이상이 소요된 것으로 확인되었다. 전세계적으로 피해액은 무려 2억 5000만 달러로 추정된다. 이와 같은 사이버테러의 위험성에도 불구하고, 국내 사이트의 상당수가 보안조치에 허술한 것으로 알려져 있다. 심지어는 수백만명 이상의 회원이 가입한 사이트를 운영하고 있는 회사마저도 보안조치에는 소홀한 경우가 많다. 사이버테러에 대한 전국가적인 대비가 필요한 때이다. 이러한 맥락에서 본 연구에서는 우리나라 사이버 안전체계의 실태를 법률과 제도적인 시각에서 분석하고, 아울러 개선전략을 제시하였다.

본 연구에서 제시한 연구결과를 압축하여 제시하면 다음과 같다. 첫째, 현재 우리 나라에서는 사이버위기를 국가차원에서 체계적으로 관리할 수 있는 제도와 구체적 방법·절차가 정립되어 있지 않아 테러 등 각종 위기상황 발생시 국가안보와 국익에 중대한 위험과 막대한 손해를 끼칠 우려가 높다. 따라서 사이버공격을 사전에 탐지하여 위기발생 가능성을 조기에 차단하며 위기발생시 국가의 역량을 결집하여 정부와 민간이 참여한 종합적인 국가대응체계를 구축하기 위해서는 법률 제정이 필요하다.

둘째, 국가차원의 사이버 안전의 효율적인 수행을 위해서는 국가사회 전반의 국가 사이버 안전의 기준과 새로운 모범을 제시하는 한편, 각 부처 및 국가사회의 구성요소들에 대해 국가 사이버 안전관리 정책을 집행할 수 있는 국가 사이버 안전관리 조직체계를 구축하는 것이 요구된다. 법률 및 추진체계 등을 통합·정비하여 정보보호 법률·제도·운영의 일관성을 확보함으로써 각종 정보보호 위협에 보다 효과적으로 대응할 수 있을 것이다. 즉 정부는 국가 사이버

안전관리에 관한 주요 정책의 심의 및 기획・조정, 통합된 국가 사이버 위기관리의 기능을 수행하기 위하여 현행 '국가사이버안전센터'의 기능을 확대 강화하는 것이 필요하다. 특히, 국가 사이버 위기와 관련된 정보의 종합적 수집, 분석, 처리의 종합적 기능을 수행하고 각 정부 및 공공 기관을 통할하며 민간부문과의 협조체계를 구축하는 것이 요구된다.

자율적 정보보호 수준제고를 위해 행정기관·공공기관의 정보보호관리체계(ISMS) 인증 제도를 확대하고 행정기관의 정보보호제품 도입 간소화 및 사용 촉진을 위해 행정정보보호용 시스템 선정 및 이용 규정을 신설 주요정보기반으로 지정된 정보기반 운영자, 정보공유·분석센터 등의 침해정보 공유 활성화 규정을 신설 및 정비함으로써 사이버침해로부터 국가·사회 주요 시설을 효과적으로 보호할 수 있을 것이다.

끝으로 정부와 민간부분이 공동으로 참여하는 국가차원의 종합적인 대응체계를 구축하여 사이버공격을 사전에 탐지하여 사이버위기 발생 가능성을 조기에 차단하며 위기 발생 시 국가의 역량을 결집하여 신속히 대응할 수 있도록 해야 한다.

주제어 : 사이버 테러, 사이버 안전체계, 산업기술보호, 정보통신기반보호, 사이버 안전센터