Securing the National Security and Reinforcing the Cyber Crisis Management System in Asia

Jae Eun Lee
Chungbuk National University

The purpose of this study is to reinforce the cooperative cyber crisis management system for securing the national security against the cyber attack and cyber-terrorism in Asia. For accomplishing the research purpose, this paper begins with the conceptual frameworks of comprehensive security and cyber security crisis for suggesting the future directions to reinforce the cyber crisis management system. For improving the cyber security from various cyber crises, it is necessary that international cooperative system have to be established. In this paper, the organizational approach, communication and decision-making approach, planning approach, and mechanisms for operational coordination have been emphasized to suggest the future directions and the policy implications for building up the international cooperative systems of cyber security crisis management. The suggested future directions for cyber security crisis management in Asia are as follows: organizing for the coordination and cooperation, statutory authority, communication channels, function- and program-centered decision-making mechanism, preparing first responders, working with private owners of critical infrastructures.

Key Words: cyber-terrorism, cyber crisis management, comprehensive security, national security, cyber security

I. Introduction

Since September 11, the United States discovered a number of terrorist cells operating within its borders and in other countries. The security services of other nations including the United Kingdom, Germany, Spain, and others, also discovered active terrorist cells(Lewis, 2003: 35). Given the new threats from the terrorist cells in the global settings, the rationale for securing the national security should be changed. National security in the age of information can be constantly exposed to attacks from hostile forces and invite serious crisis and danger if dynamic concepts and perspectives of information warfare and security are net re-established to help prepare relevant strategies and implement tasks(Huh, Lee, and Chang, 2007: 217).

Computers and internet services may be fruitfully utilized in disaster-forecasting, saving lives and properties of millions of people. They can also be used in environmental monitoring, like pollution control, global warming, greenhouse effect and ozone level depletion. ICTs could be a very useful tool in alleviating poverty since they had useful applications in agriculture, industry, and the service sector, and they could revolutionize growth in various sectors to the benefit of people across national boundaries. But cyber-

terrorism is a dangerous real threat to the peaceful and universal usage of the internet. The worst acts of terrorism could be achieved through unauthorized possession and control of information contained in the computers of unsuspecting peaceful users. In the worst imaginable scenarios, trains could be made to collide, nuclear power stations could be made to melt down with horrendous effects on humanity by the click of mouse from a single computer from any corner of the world with an internet connection(Page, Alabi, and Lunn, 2003: 36).

Cyber attacks are increasingly becoming more sophisticated and pose greater threats. Understanding and assessing cyber attacks helps in making decisions to reduce their risk and prevent the damage of the cyber terrorism. A nation must decide what types of barriers or protection mechanisms and what types of legal or institutional mechanisms are necessary to defend against cyber attacks and where to place such barriers. Effective protection against attacks requires a knowledge and understanding of attack characteristics; such as attack activities, and state and performance impacts on computer and network assets(Ye, Newman, and Farley, 2005/2006: 135). In this context, Canada, New Zealand and a few other countries have reinforced existing security agencies or established new, dedicated ones to guard against this threat, and now, the United States is creating a strategy to combat cyber threats.

This study adopts cyber as a crucial concept or an analytic category. The notion of cyber, indeed, has been used frequently in diverse contexts, such as cyber-terror(Lewis, 2003), cyber-threats(Hamin, 2000), cyber crime(Esen, 2002), cyber security (Baybutt, 2004), and so on. In spite of the diverse usage of the cyber concept, we can explain the term cyber from the perspective of crisis management. In this paper, cyber terror or cyber attack is closely connected to the real world crisis. There is a close connection between cyber-terrorism crisis and real life hazard. Especially, thinking over the fact that critical infrastructures consist of the physical and cyber assets of public and private institutions, it is necessary to reinforce the cyber crisis management system for protecting the national security. Accordingly, this paper seeks to reinforce the cooperative cyber crisis management system for securing the national security against the cyber attack in Asia. It, first, begins with the conceptual frameworks of comprehensive security and cyber security crisis, followed by discussion of the approaches and future directions for reinforcing the cyber crisis management system.

II. Definition and Theoretical Discussions

1. Comprehensive Security

A burning issue on the agenda of nations in the twenty-first century is the new meaning of security and its place in world politics. A national security is no longer the traditional national defense(military security) but has economic, environmental, and human dimensions as well(separately known as economic security, environmental security, and human security). All three dimensions be subsumed under the rubric of comprehensive security, a new umbrella concept that grew out of the post-Cold War debate over the ramifications of security and over security studies as a field of inquiry.(Hsiung, 2004: 1). Exploring the relations between human security and the environment, the human security debate, in turn, has much to offer the discussion on sustainable development. Most notably, this includes an emphasis on the social dimension of sustainable development's "three pillars"(environment, economy, society), and an insistence that goals be set and progress be assessed at a disaggregate level commensurate with respect for the dignity and well being of individual humans, not just collectives(Raad, Khagram,and Clark, 2002: 1-2).

The term 'comprehensive security' was first used by the late Japanese prime minister Ohira[1], but the concept as such can be traced back to Japanese thinking on security during the fifties. Its meaning goes far beyond requirements of military defence against a particular 'enemy', and stresses the need to take into account other aspects vital to national stability; food, energy, environment, communication and social security(Radtke and Feddema, 2000). Military insecurity is not only a threat to bilateral relations, but to regional and global stability as well. Sudden changes in exchange rates, collapse of the stock market, outbreaks of infectious disease, and many more non-military crises have increasingly drawn the attention of governments and security planners. For decades, there has been a keen awareness of the linkages between military security and social, political, and economic stability(Radtke, 2003: 501).

While not denying the importance of military security, it explicitly encompasses a wide range of other aspects: the search for environmental security, for instance, which requires cooperation with other countries(including hypothetical 'enemies'). The concept 'comprehensive security' stresses the need for confidence building methods as requirement for its attainment and pertains to issues such as preventive diplomacy, energy security, second order cybernetics, greater transparency of international financial markets as means to enhance overall stability. It is a notion that goes beyond simplifications such as 'us' and 'them'. Since the word has been first coined in Japan, it has caught on in other Asian countries as well. It has become clear that the concept is particularly suited for a continent where large and powerful countries such as China, Korea, Japan and Indonesia are unlikely to enter into close cooperation along the model of the European Union(Radtke and Feddema, 2000).

With regard to the 'security', we see benefits in a broadening of the frame of discourse to a concept of "comprehensive security". This broader view expands and reformulates more conventional views of state, human and environmental security[2], which combine to a notion of comprehensive security. Comprehensive security is necessary for lasting human security and should be linked to the more humanistic forms of sustainable development(Raad, Khagram, and Clark, 2002: 2).

Comprehensive security is not just a fashionable buzzword for academics and armchair strategists. It has entered the conscious policy planning of government security managers in Washington, D.C., and other national capitals. In the Pentagon, comprehensive security demands vigilance on a panoply of concerns such as terrorism, environmental degradation, infectious diseases, drug trafficking, energy, and humanitarian relief.(Hsiung, 2004: 2). On October 25th 2001, homeland security chief Tom Ridge outlined the Bush administration's proposal for a comprehensive domestic security plan. He said "--- our police, fire, emergency response teams -- they are the front lines of defense. We never looked at them that way before Sept. 11." and that the homeland security plan would be built on that existing infrastructure, but noted that a fully effective strategy would go beyond government. He said, "It can't just the public sector. It has to be the private sector as well."(Washington, CNN. October 25, 2001 Posted

1) Hsiung(2004) has asserted differently that Olaf Palme, the late Swedish prime pinister who headed the Commission on Disarmament and Security Issues created in 1981, is sometimes credited with having been the first one to advance the notion comprehensive security. The exact import of the concept, however, has varied and expanded over time. The Commission developed the idea of mutual security, to be achieved through cooperation, as no country could win a nuclear war, and it argued against reliance on nuclear deterrence.

2) The term state security is used as one and the same as national security in this paper.

11:50 AM EDT).

Until the end of the Cold War, national security always focused on the military defense of the state. In contrast to comprehensive security, the traditional concept of national security embraces two distinct characyeristics(Hsiung, 2004: 3). First, security is commensurate with national survival in a system of world politics that is inherently contentious and anarchical; and the State is the central unit of analysis. Second, understanding force postures and capabilities is a key tenet of traditional security. Comprehensive security, by contrast, demonstrates two distinct shifts away from the state as the central unit of analysis, representing two opposite but ultimately interelated foci(Hsiung, 2004: 4). The first shift is toward focusing on the external community at large, as it has been shown that the rampaging forces of the environment and the ravaging effects of globalization go far beyond the ability of the state to contain them by its own resources. Epidemics like AIDS and the recent SARS attacks in East and Southeast Asia in early 2003 are but a potent reminder of this new reality. Another such reminder os the series of financial crises hitting Europe(early 1990s), Latin America(1994-1995), and Pacific Asia(1997-1999), leaving no nation unaffected in their trail. The other trend is a shift inward from the state toward the individual citizen in terms of human security. The concept of human security has been expanded to include economic, health, and environ-mental concerns, as well as the physical security of the individual.

The various components of comprehensive security are intertwined. Global warming may have worldwide economic implications, and epidemics may ravage the physical and economic security of the individual(and society at large).While seemingly heading in opposite directions, both the globalization shift and the opposite shift toward the individual are ultimately interrelated because the individual is the ultimate beneficiary of both environmental and economic security. In either case, the state loses its previous salience as the central focus and unit of analysis.

2. The Concept of National Crisis

Crisis is a lay term in search of a scholarly meaning. Some scholars treat it synonymously with stress, panic, catastrophe, disaster, violence, or potential violence. Others, adhering to the medical connotation, regard it as a 'turning point' between a fortunate and an unfortunate change in the state of an organism(International Encyclopedia of the Social Sciences, 1974: 510). Crises involve events and processes that carry severe threat, uncertainty, an unknown outcome, and urgency. Crises come in a variety of forms, such as terrorism, natural disasters, nuclear plant accidents, riots, business crises, and organizational crises facing life-or-death situations in a time of rapid environmental change(Farazmand, 2001: 3). Pauchant and Mitroff(1992) defined crisis as a disruption that physically affects a system as a whole and threatens its basic assumptions, its subjective sense of self, its existential core. A more realistic definition might be: A situation faced by an individual, group or organization which they are unable to cope with by the use of normal routine procedures and in which stress is created by sudden change(Booth, 1993: 86). This definition may serve for what might be seen as organizational crises.

We are now seeking the definition of the national crisis, which covers most of the types of crisis that threatens the people in a country. From the perspective of the national crisis, we first consider the definition of the nation. Webster's Third New International Dictionary(1977: 1505) defines a concept of nation as a community of people composed of one or more nationalities and possessing a more or less defined territory and government. In Korea, we have accept this kind of definition of nation to some extent. This

paper defines the concept of nation from the point of view of the components of nation. From such point a nation is a community composed of people, territory, sovereignty, and critical infrastructures. In this context, national crisis may be a situation which threatens the security of people, territory, sovereignty, and critical infrastructures that form a nation.

It is possible for us to classify the types of national crisis on the grounds of national components; conventional security crisis, disaster crisis, living safety crisis, and critical infrastructure security crisis.

Figure 1. The Classification of National Crisis

Types		Contents
Conventional security crisis		war, armed strife, coup d'etat, subversive activities, etc.
Disaster crisis	Natural disaster	flood, typhoon, earthquake, drought, cold-weather damage, storm, torrential rain, etc.
	Man-made disaster	conflagration, collapse, submergence, plane crash, gas explosion, etc.
Critical infrastructure security crisis		breakdown of banking, transportation, electric power, IT, energy, nuclear, dam, public health, public order, etc. system
Living safety crisis		food, drug, traffic, disadvantaged consumer, economic security, living environmental pollution, occupational etc. crisis

3. Critical Infrastructure and Cyber Threats

Modern society relies on the effective functioning of critical infrastructure networks to provide public services, enhance quality of life, sustain private profits and spur economic growth. This growing dependence is accompanied by an increased sense of vulnerability to new and future threats such as terrorism and climate change(OECD, 2003; Perrow, 2006; Boin and McConnell, 2007: 50).

According to the White House(2003: viii), the importance of critical infrastructures is as follow: Critical infrastructure sectors provide the foundation for national security, governance, economic vitality, and way of life. Furthermore, their continued reliability, robustness, and resiliency create a sense of confidence and form an important part of the national identity and purpose. Critical infrastructures frame our daily lives and enable us to enjoy one of the highest overall standards of living in the world. The facilities, systems, and functions that comprise critical infrastructures are highly sophisticated and complex. They include human assets and physical and cyber systems that work together in processes that are highly interdependent.

In protecting critical infrastructure, the responsibility for setting goals rests primarily with the government, but the implementation of steps to reduce the vulnerability of privately owned and corporate assets depends primarily on private-sector knowledge and action. Although private firms uniquely understand their operations and the hazards they entail, it is clear that they currently do not have adequate commercial incentive to fund vulnerability reduction (Auers, et. al., 2005: 77). In the U.S., one of the top 10 priorities of Department of Homeland Security is protection critical national infrastructures including power, communications, transportation, and water. Each of the infrastructures is highly dependent on telecommunications and each of the infrastructures is subject to disruptions, examples of which are shown in the list below(Conrad, LeClaire, O'Reilly, and Uzunalioglu, 2006: 57-58).

Figure 2. Examples of Critical Infrastructure Disruptions

Critical Infrastructure	Disruptions
Telecommunications	Congestion or disruption of key communications nodes by fire, wind, water, or sabotage
Power	Blackouts caused by insufficient generation to meet demand, transmission bottlenecks, or equipment outages
Emergency services	Demand greater than response capacity, as during a disaster
Water	Contamination with toxic substances
Agriculture and food	Contamination of food supply
Chemical industry	Explosions, release of toxic gas clouds
Defense industrial base	Supply line interruptions
Banking and finance	Disruption of Electronic payments systems that cause bank liquidity problems
Public health	Infectious diseases, anthrax
Government	Disruptions in operations

An infrastructure is "critical" when the services it provides are vital to national security(Auerswald, et. al., 2005: 78). By the White House(2003: xii), we can identify major protection initiatives for the following critical infrastructure sectors: Agriculture and Food, Water, Public Health, Emergency Services, Defense Industrial Base, Telecommunications, Energy, Transportation, Banking and Finance, Chemicals and Hazardous Materials, Postal and Shipping. Threats to these critical infrastructures fall into two categories: physical threats to tangible property("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures("cyber threats"). Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation(Executive Order 13010-Critical Infrastructure Protection July 15, 1996).

4. Cyber Security Crisis Management and Its Challenges

Global information and communication networks are now an integral part of the way in which modern governments, businesses, education and economics operate. However, the increasing dependence upon the new information and communication technologies by many organizations is not without its price; they have become more exposed and vulnerable to an expanding array of computer security risks or harm and inevitably to various kinds of computer misuse(Hamin, 2000: 105).

President Clinton's Commission on Critical Infrastructure Protection(1998: ix) described the vulnerability of critical infrastructures in the following terms(Boin, et. al., 2003: 100):

"Our national defense, economic prosperity, and quality of life have long depended on the essential services that underpin our society. These critical infrastructures - energy, banking and finance, transportation, vital human service, and telecommunications - must be viewed in the Information Age. The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex network of interdependence. The interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk."

The nation's critical infrastructures consist of the physical and cyber assets of public and private institutions in several sectors: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is the nervous system of these infrastructures - the control system of the country. Cyberspace comprises hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make the critical infrastructures work(The White House, 2003: 1).

It is possible for us to see four patterns in contemporary crisis management practices that may be particularly prohibitive in protecting critical networks from disruption(Boin, et. al., 2003: 101-102).

First, the very characteristics of infrastructural networks discussed above create challenges for crisis management preparedness. The Millennium operation has shown how difficult it is to distinguish between critical and non-critical networks. The interdependence between networks suggests the futility of such a distinction. The Millennium operation also displayed a fascination with hardware(technology, production

lines, pipes etc.). Crisis managers tend to focus on potential violations of the hardware(fire, explosions, sabotage etc.) and very little attention to the 'human software', which is captured in the organizations running these hardwired networks. They are preoccupied with prevention and tend to forget that resilience is the key to adequate responses.

Secondly, crisis management is still predominantly a local affair. For instance, the trend in designing emergency management structures is to build them from the bottom up: local authorities begin to deal with a disaster, regional and national authorities offer assistance. Only when a disaster outpaces local capacity will regional or national authorities take over. This way of organizing rests on the idea that a disaster is almost by definition local in nature. These are worrying observations, as crisis challenges are shifting to the systemic level. Local disturbances have immediate consequences for the system in which they occur, but also in connected systems.

A third characteristic of contemporary crisis management patterns is the long-time reliance on rational planning procedures. Crisis management has long been approached in terms of finding or generating certainties for emerging uncertainty. If a crisis meant that the basic references did no longer suffice to deal with a situation, crisis management aimed to bring in new solutions. During a crisis, crisis managers routinely rely on the advice of experts. But in systemic disruptions of critical infrastructures, basic references of experts are frequently shattered. When BSE(Mad Cow Disease) emerged in the UK, the experts of the European Union could not even agree on the nature of the problem(Grönvall, 2001).

Fourth, crisis management preparation is in too many organizations still only a paper reality. Elaborate plans nicely describe procedures, exercises, scenarios, organizational structures, competences and responsibilities. But they have never been tested and the question is whether they will hold up in the actual event of network disruption.

III. Approaches to the Cooperative Cyber Crisis Management System

There might be many approaches for establishing the cooperative cyber crisis management system in Asia. This study uses the Jennings' approach to suggest the alternatives for cooperating and coordinating in Asia. The approaches to coordinate and cooperate among the Asian countries are as follows: (1)organizational approaches; (2)communication and decision-making approaches; (3)planning approaches; and (4)mechanisms for operational coordination and cooperation (Jennings, 1994: 54-56; Lee, 2007: 65).

1. Organizational Approaches

Although reorganization to enhance coordination and cooperation among the countries was not mentioned specifically, it is an avenue that could be followed. Historically, this has been a significant issue among those concerned about coordination and cooperation, and it continues to be of interest as a good evidence of playing an important role for cooperating and coordinating the crisis and emergency management issues. It is possible for the nearby countries to make an organization for effective crisis and emergency management.

As a matter of fact, cooperative activities are growing in Asia, including Japan, China, and Korea. For example, the central personnel agency in related countries does have a regular meeting every year for promoting cooperative activities. Likewise, it could be possible for the central cyber security crisis management agencies in Asian countries to organize a regular meeting in order to enhance coordination and cooperation in the field of cyber security crisis management.

2. Communication and Decision-Making Approaches

For countries to coordinate and cooperate in the cyber security crisis management functions, each country must interact effectively to bring together the elements of the cyber security crisis management system. This requires that they find ways to communicate effectively and develop shared goals. At a minimum, they must find out how their goals interrelate. Communication and decision-making approaches to coordination and cooperation include a variety of structures, procedures and policies for insuring that effective communication develops, and shared goals are identified and pursued.

Whenever a cyber security crisis occurs, particularly a large-scale cyber crisis affecting a broad range of countries, several countries need to communicate with each other and find a common solution for all concerned stakeholders. Under such circumstances, information sharing and establishing a collaborative decision-making body could be an example of communication and decision-making approaches.

3. Planning Approaches

Planning is one of the central components for effective communication and decision-making of an international system. It is central to efforts to develop shared goals. Planning approaches to a global cooperative system for cyber security crisis management involve the use of planning processes, techniques, and plans to expedite cooperation among the countries at the international level.

Various crises including both physical and cyber crisis may arise in countries in Asia. In order to prevent and prepare for effective crisis management, all concerned countries need to plan various cooperative activities and channels in terms of how to effectively respond, what to do, when to do it, etc. Therefore, if countries in Asia agree to cooperate with each other for effective cyber security crisis management, they need to develop a broader-scale strategic plan rather than an individual country-specific plan.

4. Mechanisms for Operational Coordination and Cooperation

All of the countries must do more than just plan and communicate if cooperation and coordination is to take place. They must also develop mechanisms for operational coordination and cooperation. Mechanisms for operational cooperation and coordination typically formalize relationships among programs or organizational units or create particular operational patterns.

IV. Future Directions for Cyber Security Crisis Management in Asia

The importance of cyber security has gained recognition from governments of all the related countries around world. In states of crisis, all participating cyber security agencies need to work together and communicate with each other. However, disorganized and inexperienced response can delay the recovery processes(Kamolvej, 2007: 46). From the Jennings's perspective, it is possible to propose the new alternatives for the regional and global cooperative systems to secure the cyber security.

1. Organizing for the Coordination and Cooperation

Global networks supporting critical economic and security operations must be secure and reliable. Securing global cyberspace will require international cooperation to raise awareness, increase information sharing, promote security standards, and investigate and prosecute those who engage in cybercrime(The White House, 2003: 51). Cyber security crisis manage-

ment requires coordination of a wide range of organizations and activities, both public and private. Everyone acknowledges the critical need for such coordination in a crisis, but in fact not many people want to be coordinated, nor is it clear just what the term means in practice. Ensuring the abilities for the effective cyber security crisis management among the multi-nations is needed to be coordinated among the related nations. One important source of core competences is coordination ability, an organization's ability to coordinate its functional and organizational resources to create maximum value (Jones, 2004: 229). For establishing the cooperative system in Asia, it is necessary to set up a responsible organization to coordinate and cooperate for efficient cyber security crisis management functioning.

2. Statutory Authority

Statutory authority is not easily transformed into legitimate political authority, and cyber security crisis management agencies are very seldom given anything but statutory authority to coordinate in the event of a cyber crisis(Schroeder, Wamsley, and Ward, 2001: 360). Crisis managers and responders are trained to obey the statutory provisions. Another mission is to make the statutory rules, for example the "international cooperative treaty" among the Asian countries, so that they can function effectively and coordinate with their counterparts in neighboring countries.

3. Communication Channels

All communication is culturally shaped and defined(Philipsen, 1992). Communication and culture constantly interact and exert mutual influence in international cooperation efforts. In cyber security crisis management situations requiring intercultural interaction, differences in values, verbal and nonverbal styles, and notions of status can seriously impair communication competency(Köhn and Ngai, 2001: 740).

4. Function- and Program-Centered Decision-Making Mechanism

To engage in international management is to perform management activities across national borders(Certo, 1990: 180). One should keep in mind that central cyber security crisis management authorities feel unable enable to react adequately due to a high degree of uncertainty, lack of experience and the existing legal vacuum(Cazada, 1991: 12). Successful crisis management requires: (1)sensing the urgency of the matter; (2)thinking creatively and strategically to solving the crisis; (3)taking bold actions and acting courageously and sincerely; (4)breaking away from the self-protective organizational culture by taking risks and actions that may produce optimum solutions in which there would be no significant losers; and (5)maintaining a continuous presence in the rapidly changing situation with unfolding dramatic events (Farazmand, 2001: 4). Crisis decision-making is mostly seen asa function in the response phase of crisis management. The body of knowledge concerning decision-making characteristics includes tentative propositions on organizational, informational and psychological patterns to be observed during crisis situations(Rosenthal and Pijnenburg, 1991: 3). Not from an institutional perspective, butfrom the functional and program-centered perspectives, it is necessary to decide to solve the problems with coordination and cooperation virtually in the crisis situations.

5. Preparing First Responders

If an effective response to a catastrophic breakdown of critical infrastructures depends on the performance of the so-called first responders, these people must be identified and trained to act independently and effectively in dire circumstances. Potential responders should be trained to assess when plans need to be

activated and adhered to and when plans are rendered useless(Boin and McConnell, 2007: 55).

6. Working with Private Owners of Critical Infrastructures

Successfully developing capabilities for analysis, indications and warnings requires a voluntary public-private information sharing effort. The voluntary sharing of information about such incidents or attacks is vital to cybersecurity(The White House, 2003: 25). Public and private actors should invest in an institutional venue for public and private collaboration that is driven neither by 'top down' government nor market forces(Boin and McConnell, 2007: 55).

V. Conclusions

Many cyber security experts and governments officials fear that the internet, e-mail, or the nation's network infrastructure could be used as the next vehicle for a terrorist attack. Cyber attacks of different forms threaten a nation's network systems and critical infrastructures. Such attacks are increasingly becoming more sophisticated and pose greater threats. This paper seeks to reinforce the cooperative cyber crisis management system for securing the national security against the cyber attack in Asia. It, first, begins with the conceptual frameworks of comprehensive security and cyber security crisis, followed by discussion of the approaches and future directions for reinforcing the cyber crisis management system.

The foreign experiences in crisis and emergency management could give others a good lesson so that it is necessary to learn from other nations and global best practices. In order to improve the cyber security from various cyber crises, it is necessary that international cooperative system have to be established. In this paper, the organizational approach, communication and decision-making approach, planning approach, and mechanisms for operational coordination have been emphasized to suggest the future directions and the policy implications for building up the international cooperative systems of cyber security crisis management. The suggested directions for international cooperative systems among the related countries are as follows; organizing for the coordination and cooperation, statutory authority, communication channels, function- and program-centered decision-making mechanisms, preparing first responders, and working with private owners of critical infrastructures, etc.

At present, each country has its own primary organization in charge of cyber security crisis management, but there is a lack of international cooperation and exchange among neighboring countries. In each region, several countries need to organize cooperative regional cyber security crisis management system. Similarly, it is necessary to develop effective global cyber security governance.

<References>

▷ Auerswald, Philip, Lewis M. Branscomb, Todd M. La Porte, and Erwann Michel-Kerjan. 2005. The Challenge of Protecting Critical Infrastructure. *Issues in Science and Technology*. Fall: 77-83.

▷ Baybutt, Paul. 2004. Cyber Security: Are Your Computer Control Systems Safe from Attack?. *Hydrocarbon Processing*. March 2004: 49-53.

▷ Boin, Arjen and Allan McConnell. 2007. Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. *Journal of Contingencies and Crisis Management*. 15(1): 50-59.

▷ Boin, Arjen, Patrick Lagadec, Erwann Michel-Kerjan, and Werner Overdijk. 2003. Critical Infrastructures under Threat: Learning from the Anthrax Scare. *Journal of Contingencies and Crisis Management*. 11(3): 99-104.

▷ Booth, Simon A. 1993. *Crisis Management Strategy: Competition and Change in Modern Enterprises*. London and New York, Routledge.

▷ Braithwaite, Timothy. 2001. Executives Need to Know: The

Arguments to Include in a Benefits Justification for Increased Cyber Security Spending. *Information Systems Security*. September·October 2001. 35-48.

▷ Certo, Samuel C. and J. Paul Peter. 1990. *Strategic Management: A Focus on Process*. Singapore: McGraw-Hill Inc.

▷ Conrad, Stephen H., Rene J. LeClaire, Gerard P. O'Reilly, and Huseyin Uzunalioglu. 2006. Critical National Infrastructure Reliability Modeling and Analysis. *Bell Labs Technical Journal*. 11(3): 57-71.

▷ Czada, Roland. 1991. "Politics and Administration during a 'Nuclear-Political' Crisis: The Chernobyl Disaster and Radioactive Fallout in Germany." in Uriel Rosenthal and Bert Pijnenburg(eds.). *Crisis Management and Decision-making: Simulation Oriented Scenarios*. London: Kluwer Academic Publishers. 9-35.

▷ Esen, Rita. 2002. Cyber Crime: A Growing Problem. *The Journal of Criminal Law*. 66(3): 269-283.

▷ Farazmand, Ali. 2001. Introduction: Crisis and Emergency Management. Ali Farazmand(ed.). *Handbook of Crisis and Emergency Management*. New York·Basel: Marcel Dekker, Inc.

▷ Gillespie, Alisdair A. 2006. Cyber-bullying and Harassment of Teenagers: The Legal Response. *Journal of Social Welfare & Family Law*. 28(2): 123-136.

▷ Granville, Johanna. 2003. Tracking Computer Hacking: The Dangers of Cyber Terrorism. *Global Society*. 17(1): 89-97.

▷ Grönvall, J. 2001. Mad Cow Disease: The Role of Experts and European Crisis Management. in Uriel Rosenthal, R. A. Boin, L. Comfort(eds.). *Managing Crises: Threats, Dilemmas and Opportunities*. Springfield: Charles C Thomas.

▷ Hachigian, Nina. 2001. China's Cyber-Strategy. *Foreign Affairs*. 80(2): 118-133.

▷ Haimes, Yacov Y. 2002. Risk of Terrorism to Cyber-Physical and Organizational-Societal Infrastructures. *Public Works Management and Policy*. 6(4): 231-240.

▷ Hamin, Zaiton. 2000. Inside Cyber-threats: Problems and Perspectives. *International Review of Law Computers & Technology*. 14(1): 105-113.

▷ Hsiung, James C. 2004. *Comprehensive Security: Challenge for Pacific Asia*. Indianapolis: University of Indianapolis Press.

▷ Huh, Tae-hoi, Sangho Lee, and Woo-Young Chang. 2007. Contemporary Information Warfare and National Strategy: Korea's Military Cyber Security Issues and Tasks. *International Area Review*. 10(1): 215-238.

▷ *International Encyclopedia of the Social Sciences*. 1974. New York: The Macmillan Company and The Free Press.

▷ Jennings, Edward T. 1994. Building Bridges in the Intergovernmental Arena: Coordinating Employment and Training Programs in American States. *Public Administration Review*. 54(1): 52-60.

▷ Jones, Gareth R. 2004. *Organizational Theory, Design, and Change: Text and Cases*(4th ed.). New Jersey: Pearson Education, Inc.

▷ Koehn, Peter and Phyllis Bo-Yuen Ngai. 2001. Managing Refugee-Assistance Crises in the Twenty-First Century: The Intercultural Communication Factor. Ali Farazmand. (ed.). *Handbook of Crisis and Emergency Management*. New York·Basel: Marcel Dekker, Inc. 737-765.

▷ Lee, Jae Eun. 2007. "Efficient Disaster Management and the Establishment of the Cooperative System among the Civil Society, Government, and the Military: Using the Jennings' Model." *Korean Review of Crisis and Emergency Management*. 3(1): 62-74.

▷ Lewis, James. 2003. Cyber Terror: Missing in Action. *Knowledge, Technology, & Policy*. 16(2): 34-41.

▷ Page, Richard, Mojeed Alabi, and Gary Lunn. 2003. Report of the Workshop: The Digital Divide and the Threat of Cyber terrorism. *The Parliamentarian*. 84(1): 33-37.

▷ Pappalardo, Joe. 2005. Digital Defenses. *National Defense*. 89(Jan. 2005): 27-29.

▷ Pauchant, T. and I. Mitroff. 1992. *Transforming the Crisis Organisation*. San Franscisco: Jossey-Bass.

▷ Raad, Firas, Sanjeev Khagram, and William Clark. 2002. From Human Security and the Environment to Comprehensive Security and Sustainable Development. *Working Draft: for Review by the the Global Commission on Human Security in Johannesburg*. Aug 2002.

▷ Radtke, Kurt W. and Raymond Feddema. eds. 2000. *Comprehensive Security in Asia: Views from Asia and the West on a Changing Security Environment*. Boston: Brill Academic Publishers.

▷ Rosenthal, Uriel and Bert Pijnenburg. 1991. "Simulation-oriented Scenarios: An Alternative Approach to Crisis Decision-making and Emergency Management." in Uriel Rosenthal and Bert Pijnenburg(eds.). *Crisis Management and Decision-making: Simulation Oriented Scenarios*. London: Kluwer Academic Publishers. 1-7.

▷ The White House. 2003. *The National Strategy to Secure Cyberspace*. Washington, D.C.: The White House.

▷ The White House. 2003. T*he National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, D.C.: The White House.

▷ *Webster's Third New International Dictionary*. 1977. Chicago, IL: G. & C. Merriam Co.

▷ Ye, Nong, Clark Newman, and Tony Farley. 2005/2006. A System-Fault-Risk Framework for Cyber Attack Classification. *Information Knowledge Systems Management*. 5: 135-151.

▷ Ye, Nong, Joseph Giordano, and John Feldman. 2001. A Process Control Approach to Cyber Attack Detection. *Communications of the ACM*. 44(8): 76-82.

李在恩: 연세대학교에서 행정학 박사학위를 취득하고(논문: 한국의 위기관리정책에 관한 연구: 집행구조의 다조직적 관계 분석을 중심으로, 2000), 현재 충북대학교 행정학과 부교수로 재직 중이다. 주요 관심분야는 위기관리, 조직이론, 정보체계론 등이며, 재난관리론(공저, 2006) 등의 저서와 주요 논문으로는 "수요자 관점에서 접근한 재난관리서비스의 개선 방안(공저, 2008)", "국가위기관리의 새로운 영역 설정과 추진 전략: 국민생활안전 위기 영역의 분류와 운영 방안 모색(공저, 2007)", "재난관리에서의 민·관·군 협력체계 구축 방안: Jennings 접근법을 중심으로(2007)" 등의 연구논문이 있다 (jeunlee@chungbuk.ac.kr).