Comprehensive Security and Crisis & Emergency Management for Protecting Critical Infrastructure*

Jae Eun Lee
Department of Public Administration
Chungbuk National University, Cheongju, 361-763, Korea

ABSTRACT

Recently, interest has heightened over 'critical infrastructures' and their reliability in the face of potential terrorist attack. Assault on any of the critical infrastructures as transportation, power, water, telecommunications, and financial services, entails great consequences for their users as well as the other interdependent critical infrastructures. How to protect our vital critical infrastructures is the key question in this paper. The purpose of this article is to suggest the implications for crisis and emergency management to protect the critical infrastructures in our society. For achieving the purpose, we examined the concept of comprehensive security, national crisis, and critical infrastructure and, using the holistic approach, we examined the comprehensive emergency management for suggesting the implications for establishing the critical infrastructure protection system; building up the high reliability organization, organizing and partnering, assessing the risk, preparing first responders, working with private owners of critical infrastructures, working with communities, improving the administrative capacity.

Keywords: *Comprehensive Security, Critical Infrastructure, Crisis and Emergency Management*

1. INTRODUCTION

Among the most critical roles that government serves are emergency preparedness and management[1]. The essential role of government is to protect its citizens from harm. This role has led to a series of policies and government actions that were designed to anticipate risk, prepare citizens to manage risk, and assist them in recovering from damaging events. The events of 9/11 significantly altered both the public perception of risk and government's role in reducing or managing this risk. Even more devastating than the colossal damage inflicted on the civilian targets of the World Trade Center was the perception that the existing government policies to protect citizens from such an attack were inadequate or dysfunctional[2].

After this, a definition of security is no longer the conventional national security(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 concept 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[3]. Exploring the relations between human security and the environment, the human security debate, in turn, has much to offer the discussion on sustainable development. 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[4].

Recently, interest has heightened over 'critical infrastructures' and their reliability in the face of potential terrorist attack. Assault on any of the critical infrastructures as transportation, power, water, telecommunications, and financial services, entails great consequences for their users as well as the other interdependent critical infrastructures[5].

How to protect our vital critical infrastructures is the key question in this paper. The purpose of this article is to suggest the implications and alternatives for crisis and emergency management to protect the critical infrastructures in our society. For accomplishing the purpose, in this essay, the concept of comprehensive security and critical infrastructure is dealt with by literature review. And we use the holistic approach and comprehensive emergency management for suggesting the implications.

2. THEORETICAL DISCUSSION

2.1 Changing to Comprehensive Security

Until the end of the Cold War, national security always

* *Corresponding author. E-mail : jeunlee@chungbuk.ac.kr*
Manuscript received Aug. 10, 2009 ; accepted Sep. 02, 2009

This work was supported by the research grant of the

focused on the military defense of the state[6]. The debate on expanded notions of security, which began in the late 1970s and early 1980s, entered mainstream intellectual and policy debates in the early 1990s. This was in the aftermath of the end of the Cold War and superpower confrontation, which challenged the primacy of military dogma in debates on the security of people and states. Perceptions of factors influencing state and people's security changed. Poverty, internal conflict, over-population, environmental change and competition over resources were seen increasingly as more "threatening" to the well-being of people and integrity of states. The resulting debate to expand security focused on three main dimensions[4]: expanding the threats to state security from the traditional military/political to the social, economic and environmental; expanding what is to be secured to include people as well as states; and expanding the definitions of security itself to incorporate physical safety, as well as basic needs and beyond that human dignity and capabilities.[1)]

Comprehensive security demonstrates two distinct shifts away from the state as the central unit of analysis, representing two opposite but ultimately interrelated foci[3]. 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 as 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 environmental concerns, as well as the physical security of the individual.

Till now, we have seen a striking change in the ways in which citizens perceive and respond to sudden, urgent, destructive events and, more importantly, in citizen expectations of the government's capacity to anticipate and respond to such events. September 11, 2001 initiated a critical review of government performance, both before and after the disaster[2].

The term 'comprehensive security' was first used by the late Japanese prime minister Ohira, 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[7]. 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.

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[7].

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, 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[4].

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.

Four key elements distinguish human from state security[4].

The first is clearly a shift in the focus on what or who is to be secured - from political-administrative units that are territorially bounded to individual human beings no matter where they may be at any point in time.

The second is an expansion of what security means, from a focus solely on the survival of states to both the survival and dignity of human beings.

The third essential contrast between state and human security involves the claim that the survival and dignity of human beings requires "freedom from fear" that is associated with the survival of states.

Fourth and last, the threats to human security (understood as the survival and dignity of human beings through freedom from fear and freedom from want) are far more numerous, diverse in type, and complex than the threats to state security.

Chungbuk National University in 2008.

1) In contrast to comprehensive security, the traditional concept of national security embraces two distinct characteristics[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.

2.2 Significance of the Critical Infrastructures

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[8].

September 11, 2001 and its following anthrax attacks demonstrates the increasing vulnerability of civilian societies to hostile actors and to the harmful usurpation of interdependent services designed to facilitate global exchange in transportation, communications, commercial activity, and other regional services. This vulnerability is related to the increasing use of technology that makes possible the rapid exchange of goods, services, people, information, and knowledge at an ever-decreasing cost to a wider group of the world's population[9].

The critical infrastructures consist of the physical and cyber assets of public and private institutions in several sectors: agriculture/food, drinking water/treatment, public health/healthcare, energy, banking and finance, defense industrial base, telecommunications, transportation systems, postal and shipping, national monuments/icons, information technology, chemical, emergency services, dams, governmental facilities, nuclear reactors/materials/waste, and commercial facilities[10]. The importance of critical infrastructures is as follow[11]: 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[12].[3)]

Table 1. 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

Source: [13][6].

2.3 Types of the 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[14]. 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[15]. Pauchant and Mitroff 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[16]. 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[17]. 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[18]. 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.

3) In the U.S.A., one of the top 10 priorities of DHS(Department of Homeland Security) is to protect the critical 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.

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

Table 2. 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 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

Source: [6].

3. HOLISTIC APPROACH TO CRISIS AND EMERGENCY MANAGEMENT

3.1 Holistic Approach

Risk is defined as the uncertainty of outcome, whether positive opportunity or negative threat, of actions and events[19]. And risk often connotes uncertain diverse sources of initiating events, uncertain likelihood of occurrences, and uncertain adverse consequences. Therefore, identifying all sources of risks to a system, assessing the likelihood of their occurrences, and projecting all their possible consequences requires a continuous, concentrated effort. Such a process demands a systemic and holistic approach that is principle-based, quantitative to the extent possible, repeatable, and based on sound and documented assumptions. In particular, the risk of terrorism to critical cyber and physical infrastructures and to the organizational-social infrastructures that enable and sustain democratic societies cannot be addressed on an ad hoc basis. Physical infrastructure is a general term for man-made engineered systems that include telecommunications, electric power, gas and oil, transportation, water treatment plants, water distribution networks, dams, and levees. The threats to national critical infrastructures are real, and their vulnerability to manmade hazards, especially terrorism, must become high on the agendas of government and the professional community[20].

3.2 Comprehensive Crisis & Emergency Management

According to Waugh, crisis and emergency management means the processes of preparing for, preventing, or lessening the effects of, responding to, and recovering from natural and human disasters[21]. Emergency management can be defined as the process of developing and implementing policies that are concerned with the four phases of management: mitigation; preparedness; response; and recovery[22]. And risk management is defined as the systematic application of management policies, procedures and practices to the tasks of identifying, analyzing, assessing, treating and monitoring risk[23][24]. The risk has to be assessed in respect of the combination of the likelihood of something happening, and the impact which arises if it does actually happen. So, risk management includes identifying and assessing risks(the inherent risks) and then responding to them.

The comprehensive crisis and emergency management model, developed under the auspices of the National Governors Association, provided the basic framework for FEMA's IEMS(Integrated Emergency Management System) model and became the basis for most state and local emergency management systems. The comprehensive emergency management model has four phases: mitigation, preparedness, response, and recovery[21][25].

3.2.1 Mitigation: Mitigation activities are directed, when possible, towards eliminating the causes of disasters or significantly reducing the chance that a disaster will occur. Mitigation and prevention sets the stage for all subsequent steps by identifying the location and type of populations at risk, the kinds, amounts and sources of chemicals that produce risks, and mitigation measures to reduce risk. Mitigation programs include land use regulation, building codes, structural barriers(such as dams and levees), and insurance programs to lessen the economic impact of disaster.

3.2.2 Preparedness: Preparedness activities are those which are undertaken to protect human lives and property in conjunction with threats that cannot be manipulated via mitigation measures, or from which only partial protection may be achieved. We may think of preparedness measures as falling into two general categories: actions related to providing an alert that impact is eminent, and actions designed to enhance the effectiveness of emergency operations. Preparedness depends on the ability to identify an emergency, its magnitude, severity, and precursors; communicate the situation to potential victims and response agencies through notification and warning systems; and design contingency funds and management agencies to administer them in the event of an emergency. Preparedness is the pre-disaster activity of readying for expected threats, including such actions as planning for contingencies, positioning of resources, developing cooperative agreements with other jurisdictions and response agencies, clarifying jurisdictional responsibilities, and training response personnel.

3.2.3 Response: Emergency response activities are conducted during and just after the period of impact and focus upon assisting the affected public, as well as minimizing damage from secondary or repeated impact. Some of response activities include securing the impact area, search and rescue, provision of emergency medical care, sheltering evacuees and other victims, and firefighting. Response is as effective as the

mitigation and preparedness stages are. Response includes acting to reduce the likelihood of secondary damage, such as putting plastic over damaged roofs to limit damage to furniture and appliances within buildings, and preparing for recovery.

3.2.4 Recovery: Recovery activities begin shortly after disaster impact and may extend for long periods of time. The objective of recovery measures is to restore the physical part of the community, as well as the quality of life to at least the same levels as before the disaster, and possibly to introduce improvements. Traditionally, recovery has been thought of in terms of short range (relief and rehabilitation) measures versus longer range (reconstruction) measures. Recovery derives its strength from the feedback mechanisms to detect deficiencies in the regulatory programs that led to an emergency in the first place. Recovery is the post-disaster phase, largely dealing with the restoration of lifelines. Recovery includes the provision of temporary housing, food and clothing, psychological services, job services, restoration of electrical power, and small business loans. The recovery phase stops short of full reconstruction of the community.

The comprehensive emergency management model currently used in dealing with natural and technological disasters was originally conceptualized as having four phases as above. Comprehensive emergency management refers to the problem of developing a capacity for handling all phases of activity - mitigation, preparedness, response, and recovery - in all types of disasters by coordinating the efforts and resources of many different organizations or agencies(Perry, 1985: 2).

4. NEEDED CAPABILITIES FOR PROTECTING CRITICAL INFRASTRUCTURES

An infrastructure is "critical" when the services it provides are vital to national security[12]. 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[5](Executive Order 13010-Critical Infrastructure Protection July 15, 1996).

For protecting the critical infrastructures, four broad kinds of capabilities would be useful to meet the threat of attacks: prevention and mitigation; operational warning; response; and counter-action[26].

4.1 Prevention and Mitigation

Prevention and mitigation activities reduce the likelyhood of sussessful attacks or mitigate the damage that can be inflicted. Physical hardening, dispersal, and diversification of facilities are important components of prevention, as these help reduce vulnerabilities, particularly to unsophisticated attacks. Redundant and backup systems are key elements of mitigation, since both can decrease the operational down-time resulting from successful attacks. Prevention and mitigation are complemented by the full spectrum of counter-action capabilities. The government can play a number of useful roles in supplementing or encouraging the private sector's prevention and mitigation activities: threat analysis and awareness; research and development; Norms for prevention and mitigation; access control policies for related technologies.

4.2 Operational Warning

The fact that cyber attacks and their consequences can develop rapidly has the effect of shrinking drastically the time available for effective reaction. The capability to provide warning of impending attacks - or indicators of attacks under way - would contribute significantly to the nation's ability to muster resources for responding, and to engage effectively the nation's national security, law enforcement, and counterterrorism assets. Such a capability requires a well-structured incident reporting system and a sophisticated understanding of potential warning indicators that would permit attacks to be distinguished from common problems. There are several important roles the government could play in establshing an effective operational warning mechnism: data collection and integration; analysis and correlation; dissemination.

4.3 Response

Response includes capabilities needed to resolve an infrastructure crisis and manage its consequences. Response activities thus range from initial efforts to halt further destruction of the infrastructure and protect public safety, to subsequent efforts to provide disaster relief and eventually facilitate recovery of communities and infrastructure. Any response must draw on private sector assets, which provide the vast majority of response capabilities. Three government roles are needed to address the challenges of responding to purposeful attacks: government leadership; response preparedness; response operations.

4.4 Counter-action

Counter-action includes capabilities to preempt or intercept would-be attackers; possibly counterattack physically or using offensive information warfare tools; or track down, apprehend, and prosecute attackers in the wake of an attack. In sum, counter-action includes all of the measures at the nation's disposal to deal directly with the individuals, groups, or states that perpetrate attacks. While law enforcement and counterterrorism are generally considered government functions and most such capabilities are within the government, private security provides most of the day-to-day protection for their business. Private security, however, has much to contribute, but it is limited in scope, leaving lots of the law

5) The government can play a number of useful roles in supplementing or encouraging the private sector's prevention and mitigation activities: threat analysis and awareness; research and development; norms for prevention and mitigation; access control policies for related technologies[26].

enforcement and counterterrorism work to be done by the government. Three main government capabilities are needed in this area: government leadership; law enforcement; counterterrorism operations.

5. IMPLICATIONS FOR PROTECTING CRITICAL INFRASTRUCTURES

5.1 Building up the High Reliability Organization

The rise of modern and dangerous technologies has been accompanied by warnings of destructive effects[27]. Both the optimistic(nothing really bad will happen) and pessimistic(there is nothing we can do when it happens) perspectives leave crisis managers unprepared. As a result, crisis and emergency managers are left with only extreme alternatives. In the event of a system breakdown, network managers can either shut down the network(limiting the diffusion effect, but with heavy consequences for many people) or continue to operate with the possibility that the network capability will be redirected against the users of the network. Crisis and emergency management will have to be based on the premise of resilience: learning to organize for the unknown. Organizations will have to rely on the expertise of their operators who know the networks and understand the cascading dynamics of breakdowns. Crisis and emergency managers may learn from so-called high reliability organizations in which resilience has been embedded into the finest veins of the organization, thus limiting both the potential impact and chance of network breakdowns.

5.2 Organizing and Partnering

Implementing a comprehensive national critical infrastructure and key asset protection strategy requires clear and unifying organization, clarity of purpose, common understanding of roles and responsibilities, accountability, and a set of well-understood coordinating processes. A solid organizational scheme sets the stage for effective engagement and interaction between the public and private sectors. Without it, accomplishing the task of coordinating and integrating domestic protection policy, planning, resource management, performance measurement, and enabling initiatives across the governments and the private sector would be impossible[11].

5.3 Assessing the Risk

Successful problem structuring is a crucial first step in developing successful solutions. Vulnerability assessment, which examines the interaction of hazards, communities, agencies and the environment(physical, social, political and economic) taps a wide range of information sources[24]. Risk assessments for a country, a geographic region, a community, or a specific building or lifeline system in the community require an integration of hazard assessments with the vulnerability of the exposed elements of the built environment to obtain reliable answers to the following hypothetical questions. What can happen? What are the odds for each possible outcome? What are the likely consequences and losses for each possible outcome? The answers to the three broad questions above provide policymakers with a sound technical basis to call for changes in public policies and professional practices. However, these changes involve social, administrative, economic, political, and legal considerations as well and require the adoption and implementation of physical and social adjustments that will provide the community with more effective preparedness, mitigation, emergency response, and recovery measures. The ultimate objective is long-term measures that manage or reduce the perceived risk to the community to an acceptable level with the highest possible benefit/cost[28].

5.4 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. They should be instilled with a set of core values, ethics and priorities that will guide them in their decisions and actions[8].

5.5 Working with Private Owners of Critical Infrastructures

In most western countries, a substantial part of the critical infrastructure landscape is directly or indirectly in private hands. This means that the repair of critical infrastructure breakdowns is, in many cases, a job for the operator or owner[8]. Although some 85% of the critical infrastructure in the United States is privately owned, the reality is that market forces alone are, as a rule, insufficient to induce needed investments in protection[12]. Governments typically bear responsibility for the consequences of these breakdowns. The boundary between the two is not always clear, however. Private actors should get more incentives to invest in changing management structures, practices and cultures in order to anticipate, mitigate and plan for breakdowns and their societal consequences. Governmental actors should get to know these private actors who will become their counterparts during a crisis. Public and private actors should invest in an institutional venue for public-private collaboration that is driven neither by top-down government nor market forces[8]. close cooperation among all levels of government and the private sector both nationally and internationally is essential to developing a shared vernacular and vision for the future[11].

5.6 Working with Communities

Modern society has come to depend on so-called critical infrastructures, the networks that facilitate traffic, financial transactions, communication and the delivery of water, electricity, gas and food. We depend on more networks than we probably realize. Waste disposal and sewer systems may not be classified as critical, but a two-week strike of garbage men will plunge a big city into chaos. Daily life and regular operations have become so dependent on all these infrastructures that even a slight disruption has significant consequences[29]. Contingency planning and business continuity plans should be conducted in full consultation with local communities[30]. To this end, partnerships should be developed (government,

business, citizens, media) that facilitate an 'organic' community response to catastrophe[8].

5.7 Improving the Administrative Capacity

Historically, the responsibility of government to protect citizens and property from harm has served as the rationale for developing federal legislation to protect lives and property in emergencies, disasters, and extreme events. For improving the governmental capacity, first, it is necessary to develop a systematic program to increase adaptiveness and capacity for learning within and among governmental agencies, as well as between government agencies and nonprofit and private organizations. Second, we need to map the complexity and interdependence of governmental functions to guide the organizational design required for increased communication, coordination, and information sharing among public agencies that have specific responsibilities for public security. Third, there is a necessity to map the interdependence of support functions among public, private, and nonprofit organizations in the continuing task of maintaining the balance between individual freedoms and public security. Finally, it is necessary to invest in the information infrastructure that will support increased information sharing, communication, and coordination of action among public, private, and nonprofit agencies[2].

6. CONCLUSIONS

Modern society is confronted with the inherent vulnerability and risk of its society. And our society relies on the effective functioning of critical infrastructure networks to provide public services, improve quality of life, preserve private profits and spur economic growth[8]. Thus, in this paper, what we should do to protect the critical infrastructures is the key question and consequently the purpose of this article is to suggest the appropriate crisis and emergency management system for protecting the vulnerable critical infrastructures in our society. We examined the concept of comprehensive security, national crisis, and critical infrastructure and, using the holistic approach, we examined the comprehensive emergency management for suggesting the implications for establishing the critical infrastructure protection system.

As you know in the title of this paper, the national security concept after September 9.11 has been changed from conventional to comprehensive security. Under this newly formed umbrella, the importance of the critical infrastructure as a foundation for national security has been increasingly emphasized. So, the suggested implications or plans based on the theoretical discussion in this review are as follows: enhancing capabilities meeting the threat of attacks; organizing and partnering; assessing the risk; preparing first responders; working with private owners of critical infrastructures; working with communities; improving the administrative capacity, etc.

REFERENCES

[1] Glendening, Parris, N. 2002. Governing after September 11th: A New Normalcy. *Public Administration Review*. 62(Special Issue): 21-23.

[2] Comfort, Louise K. 2002. Rethinking Security: Organizational Fragility in Extreme Events. *Public Administration Review*. 62(Special Issue): 98-107.

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

[4] 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.

[5] Schulman, Paul, Emery Roe, Michel van Eeten and Mark de Bruijne. 2004. High Reliability and Management of Critical Infrastructures. *Journal of Contingencies and Crisis Management*. 12(1): 14-28.

[6] Lee, Jae Eun. 2008. Securing the National Security and Reinforcing the Cyber Crisis Management System in Asia. *Korean Review of Crisis and Emergency Management*. 4(1): 105-116.

[7] 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.

[8] 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.

[9] Comfort, Louise K. 2005. Risk, Security, and Disaster Management. *Annual Review of Political Science*. 8(1): 335-356.

[10] Department of Homeland Security. 2004. Overview of the Department of Homeland Security(internal data).

[11] The White House. 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, D.C.: The White House.

[12] 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.

[13] 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.

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

[15] Farazmand, Ali. 2001. Introduction: Crisis and Emergency Management. Ali Farazmand(ed.). *Handbook of Crisis and Emergency Management*. New York?Basel: Marcel Dekker, Inc.

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

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

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

[19] HM Treasury. 2004. *The Orange Book: Management of*

Risk - Principles and Concepts. London: HM Treasury.
[20] Haimes, Yacov Y. 2002. Risk of Terrorism to Cyber-Physical and Organizational-Societal Infrastructures. *Public Works Management & Policy*. 6(4): 231-240.
[21] Waugh, William L., Jr. 1998. Emergency Management. Jay M. Shafritz(editor in chief). *International Encyclopedia of Public Policy and Administration, Vol. 2*. Boulder, CO: Westview Press.
[22] Kim, Pan Suk and Jae Eun Lee. 2001. Emergency Management in Korea: Mourning over Tragic Deaths. Ali Farazmand(ed.). *Handbook of Crisis and Emergency Management*. Marcel Dekker, Inc.
[23] Standards Australia/Standards New Zealand. 1995. *Australian/New Zealand Standard - Risk Management*. Standards Australia, Sydney.
[24] Salter, John. 1997. Risk Management in a Disaster Management Context. *Journal of Contingencies and Crisis Management*. 5(1): 60-65.
[25] Zimmerman, Rae. 1985. The Relationship of Emergency Management to Governmental Policies on Man-Made Technological Disasters. *Public Administration Review*. 45(Special Issue): 29-39.
[26] IDA, 1997. *National Strategies and Structures for Infrastructure Protection: Report to the President's*
[27] *Commission on Critical Infrastructure Protection*. Institute for Defense Analyses.
[28] Perrow, C. 1984. *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books.
[29] Hays, Walter W. 1998. Reduction of Earthquake Risk in the United States: Bridging the Gap Between Research and Practice. *IEEE Transactions on Engineering Management*. 45(2): 176-180.
[30] 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.
[31] Coles, E. and Buckle, P. 2004. Developing Community Resilience as a Foundation for Effective Disaster Recovery. *Australian Journal of Emergency Management*. 19(4): 6-15.

Jae Eun Lee
He received the B.S., M.S., and Ph.D. in the department of public administration from Yonsei University, Seoul, Korea in 1991, 1993, 2000 respectively. Since 2000, he has been a professor in the department of public administration, Chungbuk National University. He has been interested in the crisis and emergency management, organization theory, and policy implementation.