A Study on the Unification of Management Systems for National Critical Infrastructure and National Important Facilities

Changhyun Kim (Chungbuk National University, Cheongju, South Korea)

Abstract

Climate change, war, terrorism, and cyber threats can pose serious threats to National Critical Infrastructure and National Important Facilities, which perform essential national functions such as power, energy, finance, ro ads, aviation, and ports. The paralysis or destruction of these critical functions can have severe impacts on nati onal security and the economy.

In South Korea, the management systems for national critical infrastructure and important national facilities a re divided, resulting in overlapping targets and limiting the integrated response to various complex threats.

This study compares the management systems of national critical infrastructure and important national facilities to identify operational issues, and analyzes cases from the United States and Germany. Based on this analysis, and considering South Korea's disaster environment and security situation, the study proposes a plan to unify the management systems of national critical infrastructure and important national facilities.

As a result of the study, the following recommendations were made: First, promote unification through the revision of related laws and regulations. Second, establish a central integrated management organization. Third, redefine the classification of national critical infrastructure. Fourth, integrate planning, training, and evaluation processes. By implementing these measures, South Korea will be able to effectively respond to various future threats and create a safe and sustainable society.

Key words: National Critical Infrastructure, National Important Facilities, Crisis Management

I. Introduction

Modern society faces new challenges and crises due to extreme climate crises and rapidly evolving informati on and communication technologies. The recent increase in cyber threats, the threat of terrorism, and the frequ ent occurrence of natural disasters have heightened the risks to national critical infrastructure. Although policies and systems to protect national critical infrastructure from various threats have been developed, there is a lack of integrated systems for operating similar facilities. One of the biggest issues is the overlapping designation and management of national critical infrastructure and important national facilities. Even if the facilities are the same, the controlling authority and the responding department differ depending on the crisis situation, making it difficult to respond quickly and effectively to complex crises or incidents of unclear origin, thus reducing re silience.

According to a study by the Ministry of the Interior and Safety, the overlapping designation of national criti cal infrastructure and similar systems (important national facilities and national security facilities) and the contr ol of tasks by individual laws for the safety management of these infrastructures pose issues of decreased wor k efficiency and potential administrative cost wastage. The study argued that a system integrating relevant laws and institutions into the management of national critical infrastructure is necessary (Ministry of the Interior an d Safety, 2008:94). Additionally, national critical infrastructure is defined as the essential facilities, systems, and

functions that underpin the lives and property of citizens, the sovereignty of the state, and its economic, socia l, and cultural vitality (Lee Jae-eun, 2018:192). It was noted that South Korea has yet to complete the classific ation work for national critical infrastructure beyond facilities (Lee Young-geun, 2023:9).

The purpose of this study is to propose an efficient management plan by unifying the management systems of national critical infrastructure and important national facilities. This aims to efficiently respond to various and complex threats, and to integrate planning, training, and evaluation conducted by different regulatory agencies to prevent administrative inefficiency.

The research method involved literature review and analysis of related laws, papers, research reports, and media materials. The study analyzed the management systems of national critical infrastructure and important national facilities and proposed strategies for unifying these management systems.

II. Theoretical Discussions

1. Definition and Importance of National Critical Infrastructure

1.1 Definition of National Critical Infrastructure

National critical infrastructure can be defined as "core facilities, systems, and functions that are the basis of the lives and property of the people, the sovereignty of the state, and the economic, social, and cultural vitality" (Lee Jae-eun, 2004:80). The Framework Act on the Management of Disasters and Safety (hereinafter referred to as the Disaster Safety Act) defines the national core base as "facilities, information technology systems, and assets that can significantly affect the national economy, such as energy, information and communication, transportation, health care, and core functions of the government."

The types of National Critical Infrastructure are classified into 11 categories: energy, information and communication, transportation, finance, healthcare, nuclear power, environment, important government facilities, drinking water, cultural heritage, and utility-pipe conduit. National Critical Infrastructure is designated based on factors such as potential chain effects on other critical infrastructure, the need for joint response by two or more central administrative agencies, the scale and scope of damage to national security and the economy and society in the event of a disaster, and the likelihood of disaster occurrence or the ease of recovery. As of February 2024, 363 sites have been designated as National Critical Infrastructure.

Table 1. Criteria for Designating National Critical Infrastructure by Sector

Energy	Facilities for production, supply, and storage necessary for the supply of electricity, oil, and gas.
Information and Communication	Facilities where major communication equipment such as exchange systems are concentrated and national situation monitoring facilities for information and communication services. Key networks and major computer systems necessary for operating and managing national administration. Major computer systems required for the business operations of value-added telecommunications operators as specified in Article 7 of the "Framework Act on Telecommunications" and recognized by the Minister of Science and ICT as needing special management.

Transportation	Systems responsible for personnel and logistics transportation, as well as the transportation and transport facilities necessary for their actual operation and the facilities that control them.
Finance	Facilities or systems required for the operation of banks and investment trading and brokerage businesses.
Healthcare	Facilities that provide emergency medical services and those responsible for blood management services supporting these.
Nuclear Power	Facilities where main control devices essential for the stable operation of nuclear facilities are concentrated and facilities for the permanent disposal of radioactive waste.
Environment	Facilities in the waste management system for the collection, incineration, and landfill of municipal waste according to the "Waste Management Act."
Important Government Facilities	Major facilities where central administrative agencies are located.
Drinking Water	Facilities in the system for supplying drinking water from freshwater to purification.
Cultural Heritage	Cultural heritage recognized as nationally designated cultural properties under Article 2, Paragraph 3, Item 1 of the "Cultural Heritage Protection Act" and deemed by the Cultural Heritage Administration as requiring special management.
utility-pipe conduit	Utility-pipe conduits as defined in Article 2, Paragraph 9 of the "National Land Planning and Utilization Act," recognized by the Minister of the Interior and Safety or the Minister of Land, Infrastructure and Transport as requiring special management.

Source: Enforcement Decree of the Framework Act on Disaster and Safety Management, Appendix 2.

1.2 The Importance of National Critical Infrastructure

Natural disasters, social disasters, terrorism, local wars, and cyber-attacks can halt the functions of National Critical Infrastructure, causing severe impacts on national security and the economy, as well as endangering the lives and property of the citizens. For instance, the 2003 general strike by the cargo union led to a logistics crisis, significantly disrupting the national economy and the daily lives of the people.

In March 2004, the government classified the paralysis of National Critical Infrastructure as a disaster to pro tect public safety and essential government functions from social crises. Since January 2007, efforts have been made to implement a systematic management approach through the introduction of the National Critical Infrast ructure system. Over time, various terms such as national infrastructure and national critical infrastructure syste ms have been used. However, with the amendment of the Disaster Safety Act in 2019, the term was standardi zed to National Critical Infrastructure.

2. Definition and Importance of National Important Facilities

2.1 Definition of National Important Facilities

National Important Facilities are based on the Integrated Defense Act and are designated and managed from a military perspective. The core objective is to guard, secure, and protect these facilities from physical attacks by adversaries to prepare for integrated defense situations. According to the Integrated Defense Act, National I mportant Facilities are defined as public institutions, airports, ports, major industrial facilities, and others, whos e occupation or destruction by the enemy, or whose functional paralysis, would have a severe impact on natio nal security and the daily lives of the citizens.

According to Article 5 of the Ministry of National Defense Directive No. 2575 (2021.7.30.) "Directive on the

Designation and Protection of National Important Facilities," these facilities are classified into 12 types: agencies, industrial facilities, power facilities, broadcasting facilities, information and communication facilities, transportation facilities, airport facilities, port facilities, water supply facilities, scientific research facilities, correctional, settlement support, and foreigner protection facilities, and underground joint utility tunnels (Ha Chung-su, 2023: 2).

Table 2. Designation Targets of National Important Facilities

Government Facilities	Key national and public institution facilities (Cheong Wa Dae, National Assembly Building, Supreme Court, Government Complex, Constitutional Court, Ministry of National Defense, National Intelligence Service buildings, etc.)
Industrial Facilities	Key industrial facilities such as steel, shipbuilding, aircraft, refining, heavy chemical, defense industries, and large-scale gas and oil storage facilities.
Power Facilities	Key power facilities such as nuclear power plants, large-capacity power plants, and substations.
Broadcasting Facilities	Key broadcasting facilities including national and regional broadcasting stations, transmission and relay stations.
Information and Communication Facilities	Key information and communication facilities such as international satellite ground stations, submarine communication relay stations, national backbone networks, and telephone exchanges.
Transportation Facilities	Key transportation facilities including railway traffic control centers, subway integrated control rooms, bridges, and tunnels.
Airport Facilities	Major international and domestic airports.
Port Facilities	Ports capable of accommodating large ships.
Water Supply Facilities	Key water supply facilities such as large intake and purification facilities and multipurpose dams.
Scientific Research	Scientific research facilities with comprehensive systems, research facilities for nuclear fuel development, and other science research facilities critical to national security.
Correctional and Settlement Support Facilities	Correctional and settlement support facilities.
utility-pipe conduit	Major underground utility tunnels in metropolitan areas accommodating electricity, communication, water supply, and gas infrastructure.

Source: "Table 1. Targets of National Important Facilities" (Ha Chung-su, 2023:3)

When designating a facility as a National Important Facility, the Minister of National Defense, in consultation with the heads of relevant administrative agencies and the Director of the National Intelligence Service, is responsible for the designation. According to the "Directive on the Designation and Protection of National Important Facilities," facilities are classified into grades A, B, and C based on the importance and value of their functions and roles. Grade A National Important Facilities require integrated defense operations over a wide area if occupied or destroyed by the enemy and have a decisive impact on the lives of the citizens. These include the Presidential Office, the National Assembly Building, the Supreme Court, government buildings, nuclear power plants, public radio and TV production facilities, and international airports. Grade B National Important Facilities require integrated defense operations in certain areas if occupied or destroyed by the enemy and can have a significant impact on the lives of the citizens. These include the offices of the Supreme Prosecutors' Office and the National Police Agency, international satellite ground stations, and major domestic airports. Grade C N

ational Important Facilities require short-term integrated defense operations if occupied or destroyed by the ene my and can have a considerable impact on the lives of the citizens. These include the buildings of central ad ministrative agencies and major national and public institutions (Ahn Yong-woon, 2023:53).

2.2 The Importance of National Important Facilities

National Important Facilities have high military and strategic value, making them potential targets for enemy attacks. Facilities such as ports and broadcasting stations, if destroyed or paralyzed, can significantly impact military operations. In peacetime, these facilities promote national industrial development and enhance national power, while in wartime, they support warfighting capabilities. Damage to these facilities would result in substantial national losses. Therefore, National Important Facilities are strictly protected by military forces, police forces, professional security personnel, and self-defense personnel (Ha Chung-su, 2023:2).

Managers of National Important Facilities are responsible for their security, safety, and protection. They establish self-defense plans to prepare for integrated defense situations and can request assistance from the heads of municipal or provincial police agencies or local military commanders if necessary.

3. Foreign National Critical Infrastructure Systems

3.1 The United States

The concept of National Critical Infrastructure in the United States emerged during the Cold War era with the Soviet Union in the 1950s. At that time, the term National Critical Infrastructure was used to refer to facilities that needed protection in the event of war, including nuclear testing facilities, nuclear power plants, ports, airports, and railroads. However, after the 9/11 terrorist attacks, the scope of National Critical Infrastructure was expanded. With the issuance of Presidential Decision Directive-63, specific sectors of National Critical Infrastructure were designated, and a related governance system was established (Kim Yun-hee, 2023:1).

In the United States, the realm of National Critical Infrastructure encompasses security, governance, economic vitality, and the foundation of daily life, signifying very sophisticated and complex facilities, systems, and functions. National Critical Infrastructure includes highly interdependent human assets, physical systems, and cyber systems that operate together (The White House, 2003:□).

The United States designates 16 sectors as National Critical Infrastructure, which include energy, dams, water and wastewater systems, transportation, information and communications, healthcare and public health, and financial services.

Table 3. Classification of U.S. National Critical Infrastructure (16 Types)

Chemical	Commercial Facilities	Communications	Critical Manufacturing
Dams	Defense Industrial Base	Emergency Services	Energy
Financial Services	Food and Agriculture	Government Facilities	Healthcare and Public Health
Information Technology	Nuclear Reactors,	Transportation Systems	Water and Wastewater

	Materials, and Waste		Systems

Source: U.S. NIPP 2013 (p.9)

The United States' National Critical Infrastructure protection system is operated under the leadership of the Cybersecurity and Infrastructure Security Agency (CISA). CISA, as part of the Department of Homeland Security (DHS), implements various strategies and programs to enhance the protection and cybersecurity of the nation's critical infrastructure.

The U.S. strategy is based on the National Infrastructure Protection Plan (NIPP). This plan adopts a risk management framework to assess risks, identify necessary protective measures, and suggest methods to enhance the resilience of National Critical Infrastructure.

CISA collaborates with the private sector and other government agencies to ensure the continuity and resilience of services essential to national security and economic stability. The focus is on protecting National Critical Infrastructure from a variety of threat elements, including traditional security threats, natural and social disasters, and cyber crises.

The United States' National Critical Infrastructure protection system spans a wide network and diverse industrial sectors, establishing flexible and comprehensive protection and response plans tailored to the characteristics and needs of each sector. This strategy plays a crucial role in enhancing the nation's overall security and resilience.

3.2 Germany

Germany's National Strategy for Critical Infrastructure Protection (CIP) provides systematic and integrated protection guidelines. Germany's CIP considers various threats, including technical failures, natural disasters, terrorism, and cyber threats, and has evolved to integrate these into the national risk management strategy. This strategy emphasizes the interdependence of various infrastructure sectors and the need for coordinated responses, as failures in one sector can trigger cascading effects.

Table 4. Threats, risks, vulnerabilities and risk culture

Natural events	Technical failure/ human error	Terrorism, crime, war
Extreme weather events inter alia, storms, heavy precipitation, drops in temperature, floods, heat waves, droughts	System failure inter alia, insufficient or excessive complexity of planning, defective hardware and/or software bugs	Terrorism
Forest and heathland fires	Negligence	Sabotage
Seismic events	Accidents and emergencies	Other forms of crime
Epidemics and pandemics in man, animals and plants	Failures in organization inter alia, shortcomings in risk and crisis management, inadequate coordination and co-operation	Civil wars and wars
Cosmic events inter alia, energy storms, meteorites and comets		

Source: Germany National Strategy for Critical Infrastructure Protection 2009(p.9)

Germany's National Critical Infrastructure is classified into a total of nine sectors based on technical, structural, and

functional characteristics, divided into 'technical basic infrastructure' and 'social-economic service infrastructure.'

Technical basic infrastructure includes essential services for the basic functioning and operation of society, such as power supply, information and communications, transportation, and water supply. Social-economic service infrastructure encompasses services such as public health, finance, and government operations, which also play a crucial role in the stability and functioning of society.

This classification aids in the effective formulation and implementation of risk management and crisis response plans. By developing protection plans tailored to each type, it ensures a swift and appropriate response when specific threats or incidents occur.

Table 5. Threats, risks, vulnerabilities and risk culture

Technical basic infrastructure	Socio-economic services infrastructure
●Power supply ●Information and communications technology●Transport(ation) ●(Drinking-) water supply and sewage disposal	●Public health; food ●Emergency and rescue services; disaster control and management ●Parliament; government; public administration; law enforcement agencies ●Finance; insurance business ●Media; and cultural objects (cultural heritage items)

Source: Germany National Strategy for Critical Infrastructure Protection 2009(p.7)

3.3 Comparison with Foreign National Critical Infrastructure Systems

The United States' National Infrastructure Protection Plan (NIPP) and Germany's National Strategy for Critical Infrastructure Protection (CIP) are strategies for the integrated protection of National Critical Infrastructure from various threats, including traditional security threats, natural disasters, and cyber crises. However, in South Korea, protection is managed in a dispersed manner according to each type of threat.

In the United States, the concept of National Critical Infrastructure started in the 1950s during the Cold War era with the Soviet Union as facilities that needed protection in the event of war, and the scope was expanded after the 9/11 terrorist attacks. Similarly, in South Korea, the concept of National Important Facilities emerged in the 1960s to protect against North Korean infiltration and provocations. However, there is a need to integrate these with National Critical Infrastructure for better protection.

In Germany, National Critical Infrastructure is classified into technical basic infrastructure facilities and social-economic service infrastructure functions and services. Korea can also consider classifying infrastructure into facilities and functions/services to help integrate National Critical Infrastructure and National Important Facilities.

III. Current Management System and Problem Analysis

1. Current Management System of National Critical Infrastructure and National Important Facilities

1.1 Management System of National Critical Infrastructure

The Ministry of the Interior and Safety is responsible for National Critical Infrastructure and manages it in accordance

with the Disaster Safety Act. The Ministry oversees the operation of the National Critical Infrastructure system, distinguishing between supervising agencies and managing agencies.

Table 6. National Critical Infrastructure Operational System Diagram

Ministry of the Interior and Safety (MOIS)	Lead Agency	Management Agency
<Overall System Operation> - Propose new designations for National Critical Infrastructure to the Safety Policy Coordination Committee - Notify guidelines for the establishment of National Critical Infrastructure Protection Plans - Develop and notify plans for inspections of management status, disaster management evaluations, etc. (Conduct inspections, verifications, and evaluations)	<Overall Operation by Designated Sector> - Coordinate new designations for National Critical Infrastructure - Manage protection plans (continuity of functions) for managing agencies (designated facilities) by sector - Conduct and evaluate inspections of management status by managing agencies (perform self-inspections and evaluations)	<Operation and Management by Designated Facility> - Establish and implement protection plans for each facility 1. Safety inspections and detailed safety diagnoses 2. Self-defense measures 3. Information and communication protection 4. Crisis management manuals 5. Situation management 6. Education and training 7. Management of protective resources

The supervising agencies are central administrative bodies responsible for sector-specific tasks, while managing agencies are entities that oversee designated facilities (e.g., Korea Hydro & Nuclear Power, telecommunications operators). Various ministries and agencies share roles across different sectors.

The designation of National Critical Infrastructure is decided by the Central Committee of the Safety Policy Coordination Committee. The chairperson of the Safety Policy Coordination Committee is the Minister of the Interior and Safety, and the committee members include vice ministers or vice-ministerial level officials from central administrative agencies determined by presidential decree, as well as experts in disaster and safety management appointed or commissioned by the chairperson.

National Critical Infrastructure establishes a Protection Plan and conducts the Safe Korea Training for Disaster Response (once a year) to enhance disaster response capabilities.

Each year, the Ministry of the Interior and Safety conducts inspections and evaluations. Based on the results, it rewards excellent agencies and provides consulting for those with insufficient evaluation results to improve their management capabilities.

1.2 Management System of National Important Facilities

The managing agency for National Important Facilities is the Ministry of National Defense (Joint Chiefs of Staff), which protects them from a military perspective. National Important Facilities are designated and managed according to the "Directive on the Designation and Protection of National Important Facilities," and are designated by the Minister of National Defense in consultation with the heads of relevant administrative agencies and the Director of the National Intelligence Service.

National Important Facilities establish self-defense plans and crisis management manuals in preparation for integrated defense situations, and they develop Chungmu plans for wartime preparation. Training is conducted in conjunction with

the military through exercises such as Ulchi exercises and Hwarang exercises. Guidance and supervision of security activities during peacetime are carried out by the heads of relevant administrative agencies and the Director of the National Intelligence Service.

Table 7. Comparison of National Critical Infrastructure and National Important Facilities

Classification	Supervisory Department	Legal Basis	Plan Development	Training	Supervision
National Critical Infrastructure	Ministry of the Interior and Safety (MOIS)	Basic Law on Disaster and Safety Management, Article 3-12	National Critical Infrastructure Protection Plan, Crisis Management Manual	Safe Korea Training for Disaster Response	Ministry of the Interior and Safety, Central Administrative Agencies, National Intelligence Service (upon request)
National Important Facilities	Ministry of National Defense (Joint Chiefs of Staff)	Integrated Defense Act, Article 2	Self-Defense Plan, Chungmu Plan, Crisis Management Manual	Ulchi Exercises, Hwarang Exercises	Central Administrative Agencies, National Intelligence Service

2. Problems in the Management Systems of National Critical Infrastructure and National Important Facilities

2.1 Inadequate Revision of Laws in Response to Changing Crisis Environments

In 2002, the Integrated Defense Act was amended to include provisions related to National Important Faciliti es. The Integrated Defense Act evolved from Presidential Decree No. 18, 'Anti-Spy Measures,' established in December 1967, and Presidential Decree No. 28, 'Integrated Defense Guidelines,' revised in January 1970, lead ing to the enactment of the Integrated Defense Act in 1997. The current integrated defense system was primar ily designed to respond to North Korea's military threats in the 1960s, focusing on the military domain.

National Critical Infrastructure began systematic management in January 2007 with the amendment of the Dis aster and Safety Management Act, which introduced designation and management regulations. According to the detailed provisions of the law at the time, National Critical Infrastructure was to be designated based on 'the scale and scope of damage to national security and the economy and society in the event of a disaster.'

Since the early 2000s, the state has recognized the importance of critical infrastructure and the fatal impact it s destruction or functional impairment could have on national security and the economy. Just as the United St ates improved its National Critical Infrastructure system following the 9/11 terrorist attacks in 2001, Korea sho uld have established a protection system for critical infrastructure. However, National Critical Infrastructure and National Important Facilities are still operated as separate systems, not integrated. This indicates inadequate re vision of laws to appropriately respond to the changing crisis environment.

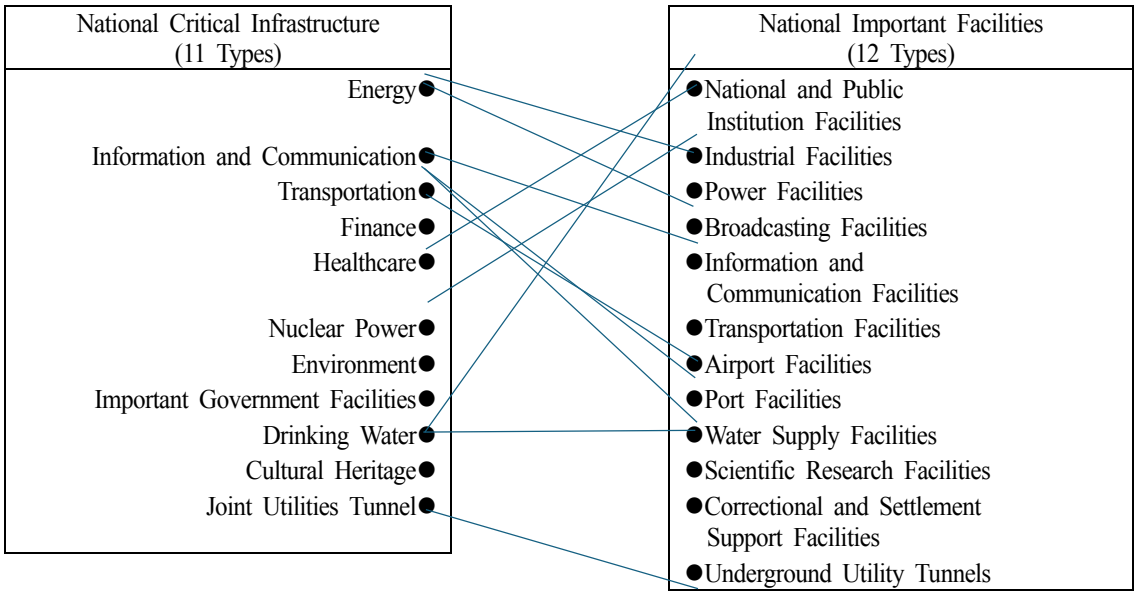
According to the Government Organization Act, the Ministry of the Interior and Safety oversees the establishm ent, coordination, and adjustment of policies related to safety and disaster, emergency preparedness, civil defens e, and disaster prevention. The Ministry of National Defense handles military administration and orders related to national defense and other military affairs, while the Joint Chiefs of Staff is tasked with the execution of in tegrated defense operations involving civilians, government, and the military. Since the protection of National I mportant Facilities has a strong emergency preparedness nature, it should be considered a task for the Ministry

of the Interior and Safety rather than the Ministry of National Defense (Joint Chiefs of Staff). However, the l egal framework has not been revised to reflect the changing security environment.

2.2 Inefficiencies and Problems Due to Dual Management

Among the 11 types of National Critical Infrastructure, 8 types overlap with the types of National Important Facilities, excluding healthcare, environment, and cultural heritage. Among the 12 types of National Important Facilities, 9 types overlap with the types of National Critical Infrastructure, excluding broadcasting facilities, scientific research, and correctional/settlement support facilities. It is difficult to accurately determine the extent of overlap as the targets of National Important Facilities are designated as confidential. However, by comparing the types, it can be inferred that there is significant overlap, with approximately 360 National Critical Infrastructure sites and about 500 National Important Facilities.

Fig. 1. Comparison of Overlapping Types between National Critical Infrastructure and National Important Facilities



Such overlapping designations lead to increased administrative burdens and inefficient use of personnel and budget, as the same facility falls under the management of multiple agencies. Although protection plans are established for each type of threat, these plans are not integrated or coordinated, and training and evaluations are conducted in a dualized manner.

The dual management system results in significant issues, including a lack of information sharing and cooperation. When information is not smoothly shared, each agency can only make decisions based on limited information, which can reduce the effectiveness of protection and response strategies. In complex crisis situations such as cyber threats or terrorism, the lack of information flow can lead to even greater risks.

2.3 Inadequate Preparedness for Diverse and Complex Threats

Due to the climate crisis and rapidly changing information and communication technologies, National Critical Infrastructure and National Important Facilities are exposed to various risks and threats such as natural disasters, cyber-attacks, and terrorism.

First, traditional security threats. South Korea faces military threats from North Korea. North Korea's nuclear missiles, unmanned aerial vehicles (drones), and special forces pose direct threats to National Critical Infrastructure and National Important Facilities. Among these, North Korea's drones can stealthily approach and target facilities like Incheon International Airport or government buildings, potentially causing destruction and paralysis. The discovery of North Korean drones that flew into South Korean territory in 2014 and 2017 proves the reality of these threats. North Korea's special forces can also create physical damage to National Critical Infrastructure and National Important Facilities through terrorist activities, causing psychological and social instability among the population.

As seen in the Russia-Ukraine war in February 2022, military strategies targeting energy and industrial facilities to paralyze the opponent's functions are being employed. One of the characteristics of this war is Russia's execution of combined military and cyber-attacks. Such tactics could be similarly applied by North Korea, which has significant military exchanges with Russia, in an attack on South Korea.

Second, the risk of natural disasters. Recently, the world has been experiencing severe natural disasters such as floods, heatwaves, and wildfires. Modern disasters are changing from single disaster phenomena to complex disasters where multiple disasters are interlinked. Destruction of National Critical Infrastructure due to natural disasters directly leads to service interruptions, causing social disasters that hinder the provision of services to the public (Ministry of the Interior and Safety, 2008:1).

Extreme temperature changes, with high temperatures in summer and severe cold in winter, significantly increase energy demand, placing a heavy load on the power supply system and potentially causing blackouts or energy supply interruptions. In the summer of 2018, South Korea experienced a record heatwave, which led to a nationwide surge in energy demand. This caused temporary blackouts due to overloads in the power supply network, revealing the vulnerability of National Critical Infrastructure. The 2003 blackout in New York and power outages caused by hurricanes starkly demonstrate the vulnerability of modern society's high dependence on electricity.

Third, increasing cyber crises and vulnerabilities. The development of information and communication technology in the 21st century has brought hyperconnectivity and hyperintelligence to power and traffic control systems, enhancing efficiency but also increasing security vulnerabilities and exposing them to hacking threats. Cyber-attacks, through acts such as theft, distortion, or damage of electronic information, and the destruction or malfunction of major communication networks via electronic means, can significantly impact national security and cause social and economic chaos.

Additionally, internal technical defects, operational errors, and data leaks by insiders can cause more damage than external hacking. National Critical Infrastructure requires very high levels of technology and security, employing sophisticated and complex technologies. The application of advanced technologies and heightened security measures can increase vulnerabilities and lead to large-scale accidents.

Beyond logical intrusions and information theft, hybrid attacks that involve electromagnetic interference and physical damage can escalate to the worst-case scenario, potentially incapacitating National Critical Infrastructure and threatening

the very existence of the nation (Hong Soon-min, 2022:7). Therefore, it is necessary to establish comprehensive protection strategies for National Critical Infrastructure and National Important Facilities by integrating the management of various vulnerabilities, risks, and threats, ensuring information sharing and preparing response measures.

IV. Strategy for Unifying the Management Systems of National Critical Infrastructure and National Important Facilities

1. Promote Unification through Legal Revisions

The aim is to revise the laws and systems governing national critical infrastructure and important national fa cilities to integrate and unify their management systems. In the short term, this involves amending the Integrat ed Defense Act. Specifically, Article 21 of the Integrated Defense Act (Security, Protection, and Guard of Imp ortant National Facilities) should be revised to change the term "important national facilities" to "national critic al infrastructure," thereby absorbing and integrating important national facilities into national critical infrastructu re. The consolidated national critical infrastructure's management system, including security, protection, and gua rding, should be unified under the Ministry of the Interior and Safety. Given that the security, protection, and guarding of national critical infrastructure have a strong contingency planning nature, it is appropriate to transf er these responsibilities from the Ministry of National Defense to the Ministry of the Interior and Safety in ac cordance with the Government Organization Act.

Amending the Integrated Defense Act to integrate national critical infrastructure and important national facilit ies aims to protect against physical threats. However, for integrated protection against electronic warfare acts s uch as cyber attacks, a more comprehensive and systematic approach is necessary. The dispersed management system makes inter-agency cooperation and coordination difficult and hinders swift and consistent responses to complex crisis situations.

To address this, the long-term goal is to establish a clearer and more integrated "National Critical Infrastructure Protection Act." This law would harmonize the various existing laws and provide a legal foundation for systematic protection and management. By clarifying legal definitions and eliminating redundant regulations, this act would enhance the efficiency of management.

2. Establishment of a Central Integrated Management Organization

For the effective protection of National Critical Infrastructure, it is necessary to form an integrated organizati on capable of coordinating and controlling responses to all threats, including traditional security threats, disaster safety, and cyber crises. To achieve this, a central integrated management organization that can serve as a co ntrol tower should be established under the Prime Minister's Office or the Ministry of the Interior and Safety. This organization should coordinate cooperation between various ministries and agencies, establish consistent po licies, and provide integrated responses. It must be prepared to respond swiftly and consistently in emergencie s.

The Cybersecurity and Infrastructure Security Agency (CISA) in the United States plays a significant role in protecting National Critical Infrastructure from various threats, such as terrorism, natural and social disasters, a nd cyber crises, by collaborating with the private sector and other government agencies. CISA ensures the nati on's safety through comprehensive responses to threats across various fields. Similarly, South Korea needs a ce ntral integrated management organization capable of performing a similar role to CISA.

3. Reestablishment of the Classification of National Critical Infrastructure

National Critical Infrastructure includes facilities, systems, and functions that have a significant impact on na tional security, the economy, and citizens' lives. In contrast, National Important Facilities are primarily designat ed based on facilities. This dual designation method can lead to overlaps and inefficiencies. Therefore, it is ne cessary to integrate National Important Facilities into National Critical Infrastructure and reestablish their classif ication. This is essential for building a more systematic and consistent protection and management system.

The United States has classified National Critical Infrastructure into 16 types, while Germany has categorized it into 9 types. By comparing the types of National Critical Infrastructure in other countries and considering th e types of National Important Facilities, we propose expanding the current 11 types of National Critical Infrast ructure to 14 types.

Table 8. Classification Plan for National Critical Infrastructure (14 Types)

Energy	Information and Commu nication	Transportation	Finance
Healthcare	Nuclear Power	Broadcasting Facilities	Environment
National and Public Insti tution Facilities	Drinking Water	Industrial Facilities	Food Supply
Joint Utilities Tunnel	Cultural Heritage	-	-

4. Integration of Planning, Training, and Evaluation

Modern crisis situations often involve a complex interplay of various threat elements such as terrorism, disas ters, and major accidents. In such complex crisis situations, threats can emerge ambiguously without clear bou ndaries, making it difficult to effectively respond with the existing separate training and evaluation systems for disaster and security. Currently, training and evaluation are conducted according to different laws and regulator y agencies, leading to administrative inefficiencies and a lack of integrated and consistent response capabilities. Therefore, the training and evaluation systems should be integrated while unifying National Critical Infrastructu re and National Important Facilities.

The current individual Disaster Safety Korea Training and Ulchi Exercises should be integrated into a multi-purpose training model tentatively named the "National Crisis Management Comprehensive Training." This red esigned training model should focus on mastering crisis response tasks in both peacetime and wartime (Jeong

Chan-kwon, 2022:21).

Regular and integrated training and evaluation should promote cooperation between various ministries and ag encies, fostering comprehensive crisis response capabilities. This integrated approach will play a crucial role in protecting the nation's critical assets and enhancing response capabilities in crisis situations.

V. Conclusion

To effectively respond to the complex and ambiguous crisis situations faced by modern society, it is necessa ry to unify the management systems of National Critical Infrastructure and National Important Facilities. This s tudy aims to propose comprehensive and efficient measures to address disaster and security situations through such integration.

Firstly, it is essential to unify the management systems of National Critical Infrastructure and National Impor tant Facilities through legal revisions. In the short term, the Integrated Defense Act should be amended to abs orb National Important Facilities into National Critical Infrastructure, centralizing management under the Minist ry of the Interior and Safety. In the long term, the enactment of the "National Critical Infrastructure Protection Act" is needed to establish a clearer and more integrated legal foundation. These legal revisions will enhance management efficiency by clarifying definitions and eliminating redundant regulations.

Secondly, the establishment of a central integrated management organization is necessary. A central organizati on capable of coordinating and controlling responses to all threats, including traditional security threats, disaster safety, and cyber crises, should be established under the Prime Minister's Office or the Ministry of the Interior and Safety. This organization should coordinate cooperation between ministries and agencies, establish consisten t policies, and provide integrated responses.

Thirdly, the classification of National Critical Infrastructure needs to be reestablished. National Critical Infrast ructure includes facilities, systems, and functions that significantly impact national security, the economy, and c itizens' lives. In contrast, National Important Facilities are primarily designated based on facilities. This dual de signation method can lead to overlaps and inefficiencies. Therefore, it is necessary to integrate National Import ant Facilities into National Critical Infrastructure and reestablish their classification. By comparing foreign class ifications and referencing the types of National Important Facilities, it is proposed to expand the current 11 ty pes of National Critical Infrastructure to 14 types.

Fourthly, the integration of planning, training, and evaluation is crucial. Modern crisis situations often involv e a complex interplay of various threat elements such as terrorism, disasters, and major accidents. In such com plex crisis situations, threats can emerge ambiguously without clear boundaries, making it difficult to effectivel y respond with the existing separate training and evaluation systems for disaster and security. Currently, trainin g and evaluation are conducted according to different laws and regulatory agencies, leading to administrative i nefficiencies and a lack of integrated and consistent response capabilities. Therefore, the training and evaluation systems should be integrated while unifying National Critical Infrastructure and National Important Facilities.

The integration of National Critical Infrastructure and National Important Facilities is not merely an institutional change but an essential strategy for protecting national security and the lives of citizens. The measures proposed in this study will play a vital role in establishing a strong and consistent protection system, enabling South Korea to effectively respond to various future threats and create a safe and sustainable society.

One limitation of this study is the difficulty in accurately determining the extent of overlap between National Critical Infrastructure and National Important Facilities due to the confidentiality of the latter's targets. Additionally, further in-depth research is needed to legislate the protection of National Critical Infrastructure and establish a comprehensive protection system.

References

Ministry of the Interior and Safety. 2008. Study for the Efficient Protection of National Infrastructure System.

Lee, Jae-eun. 2018. Crisis Management Studies, 2nd ed. Seoul: Daeyoung Munhwasa.

Young Kune Lee and one other. 2023. A Legal Review of the Process of Introducing National Core Infrastructure Legislation in the Disaster and Safety Law.

Ahn Yong-woon. 2023. Study on the Establishment of a New Protection System for National Important Facilities (Focusing on the Triple Dome Protection System against Drone Threats).

Hong Soon-min and two others. 2022. Analysis of Trends in Intelligent Cyber Attacks on Power Systems.

Kim Yun-hee. 2023. Implications of the U.S. National Critical Infrastructure Protection System.

Jeong Chan-kwon. 2022. A Study on the Design Direction of the National Security and Disaster Crisis Management System.

Disaster and Safety Management Basic Act, Article 3.

Integrated Defense Act, Articles 2 and 21.