Exploring Critical Infrastructure Protection Planning: Insight from International Experience

GUO Dongjun, WU Yanhua, ZHAO Hongxu, ZHU Xingping, CUI Tao, CHEN Zhilong

Abstract: In contemporary warfare, critical infrastructure often becomes a key economic target in attacks. Therefore, aligning territorial spatial planning with the protection of such infrastructure is essential. China's civil air defense system has two primary tasks: protecting urban population and safeguarding economic targets and critical infrastructure. While the former is addressed through the planning and development of civil air defense projects, the latter remains only partially achieved, although the Chinese government and some provinces have recognized its importance and advocated for its integration into national comprehensive planning and territorial spatial planning. This paper defines and analyzes the concepts of important targets, important economic targets, and critical infrastructure, providing an overview of the current state of critical infrastructure protection planning, with a focus on the evolution of its framework. Furthermore, it explores the vision, mission, goals, and core principles of the four versions of the United States' post-2006 National Infrastructure Protection Plan, examining the planning partnership structure and collaborative mechanisms for risk management and implementation. Drawing on international experiences, particularly those from the United States, the paper offers insights into partnership mechanisms, initiation timing, initial steps, and area for improvement in China's emerging critical infrastructure planning practices.

Keywords: critical infrastructure; protection plan; the United States; important economic target; insight

Chinese Library Classification No.: TU984; Document Code: A

DOI: 10.16361/j.upf.202501015; Article No.: 1000-3363(2025)01-0111-09

Author Biography: GUO Dongjun, Professor and Doctoral Supervisor, College of Defense Engineering, Army Engineering University of PLA. Email: guo_dongjun@163.com; WU Yanhua, Lecturer, College of Defense Engineering, Army Engineering University of PLA; corresponding author. Email: yanhua_wu@foxmail.com; ZHAO Hongxu, Master's Student, College of Defense Engineering, Army Engineering University of PLA; ZHU Xingping, Associate Professor, College of Defense Engineering, Army Engineering University of PLA; CUI Tao, Master's Student, College of Defense Engineering, Army Engineering University of PLA; CHEN Zhilong, Professor and Doctoral Supervisor, College of Defense Engineering, Army Engineering University of PLA, and National Master of Engineering Survey and Design.

Funding: General Program of the National Natural Science Foundation of China, “Criteria, Mechanisms, and Responses of Urban Underground Planning under the Carbon-Peaking and Carbon-Neutrality Goals” (Grant No. 52378083); General Program of the Natural Science Foundation of Jiangsu Province, “Facility and Spatial Micro-Renewal for Activating Freight Functions of Existing Metro Infrastructure: A Case Study of Nanjing Metro Line S1/Airport Line” (Project No. BK20231488).

Critical infrastructure protection directly affects the layout of urban systems and territorial spatial planning. The pre-World War II planning and construction of Soviet industrial-city bases in the Urals and China's Third Front Construction in the 1960s were both forms of protection planning[1]. The 1946 Draft Ten-Year Construction Plan for the Wartime Capital led to the planning and construction of numerous armament factories and defensive facilities in and around Chongqing, profoundly reshaping the city's spatial structure and character. These dispersal measures reinforced Chongqing's urban form

of “broad dispersal, localized concentration, and plum-blossom-like nodes”[2]. In recent local wars and the ongoing Russia-Ukraine conflict, critical infrastructure has invariably been a primary target for both sides, and the success of its protection has even become decisive to the outcome of war[1,3-4].

The protection of critical infrastructure, historically termed economic protection, can be traced to the aftermath of World War I and has evolved through three stages. The first was an early emergence before the end of World War II, represented by the Soviet Union, Germany, and Japan. The second, after World War II, was a major period of development in which economic protection shifted from defense against air raids to defense against missiles and nuclear weapons, with the Soviet Union, the United States, and the Nordic countries as leading examples. Following a brief readjustment in the 1990s after the Cold War, the field entered a new stage characterized by integration with counterterrorism, disaster prevention, and resilient-city development[5-6]. The United States and other countries have issued policies to strengthen critical infrastructure protection so that essential government operations and public services can continue during deliberate attacks, natural disasters, and other emergencies.

Overall, the focus of economic protection has shifted from aircraft attacks to missiles and nuclear weapons, while the protected objects have expanded from “economic targets”[7] to “critical infrastructure and key resources”[8]. Many countries have planned and implemented critical infrastructure protection according to their own conditions, and the United States is a pioneer and representative case. Since the first National Infrastructure Protection Plan (NIPP) was issued in 2006[9], it has undergone three subsequent updates - in 2007/2008, 2009, and 2013[10-12] - and has provided continuing guidance and support for U.S. critical infrastructure protection.

In China, requirements have been established through the Civil Air Defense Law of the People's Republic of China[13], the National Defense Law of the People's Republic of China[14], the National Defense Mobilization Law of the People's Republic of China[15], and the Regulations on the Security and Protection of Critical Information Infrastructure[16], which specify that national economic mobilization and protection should be incorporated into overall national development plans and programs. At the provincial and municipal levels, regulations such as the Inner Mongolia Autonomous Region Regulations on the Protection and Management of Important Economic Targets[17] require the civil air defense authority (or development and reform authority) and sectoral departments to prepare a master plan for protecting important economic targets and to incorporate it into economic and social development planning and territorial spatial planning. Implementation, however, remains limited because of the absence of relevant planning standards and other constraints[18-19]. Drawing on previous national, provincial, and municipal projects, this paper focuses on the U.S. NIPP in order to support the preparation of critical infrastructure protection plans at national and local levels[20] and to contribute to China's resilient-city development and national security strategy[21-22].

1 Critical Infrastructure and Related Concepts

Any theory must be founded on clarified ideas and precisely defined concepts. A shared understanding of terminology is necessary for coherent research and for a deeper grasp of underlying laws and logical relationships[23]. Critical infrastructure and related objects have been described by multiple terms. In the United States, these have included “industrial base”[24], “economic target”[7], “key assets,” and “key resources”[25]. In China, they are generally referred to as “important economic targets.” This section clarifies the connotations and scope of “important economic targets” and “critical infrastructure,” as well as their relationship with military and political targets.

Countries face different threats and priorities in protecting important economic targets and therefore define and classify them differently[3]. Their connotations and boundaries have also evolved with changes in military conditions and economic structures. Before the 1990s, domestic and international understandings were broadly similar: the term “economic target” was normally used, with protection focusing on targets related to national defense and economic security.

As the protective role of infrastructure has been more fully understood, foreign systems have progressively incorporated social targets related to public health and safety, national morale, and even environmental facilities. The U.S. system now covers sixteen sectors, including energy, critical manufacturing, the defense industrial base, and transportation systems[12]. Because the term “economic target” no longer adequately covers hospitals, landmark buildings, and other facilities related to public health, safety, and morale, the broader term “critical infrastructure” is now commonly used. It encompasses resources and facilities associated with national defense, economic security, public health and safety, national morale, and the environment, as shown in Fig.1. Military targets and some political targets are excluded from this category of civilian facilities.

Essential targets consist collectively of critical infrastructure, political targets, and military targets. These categories are closely connected and partly overlap. Critical infrastructure clearly includes important economic targets and social targets and overlaps with certain government facilities treated as political targets. For example, lower-level government facilities serving communities may be considered civilian critical infrastructure, while top-level command organs should be classified as political targets. Their relationships are illustrated in Fig.2. In this paper, critical infrastructure refers to civilian targets essential to national defense, economic security, public health and safety, national morale, and the ecological environment; military targets and top-level command organs are excluded.

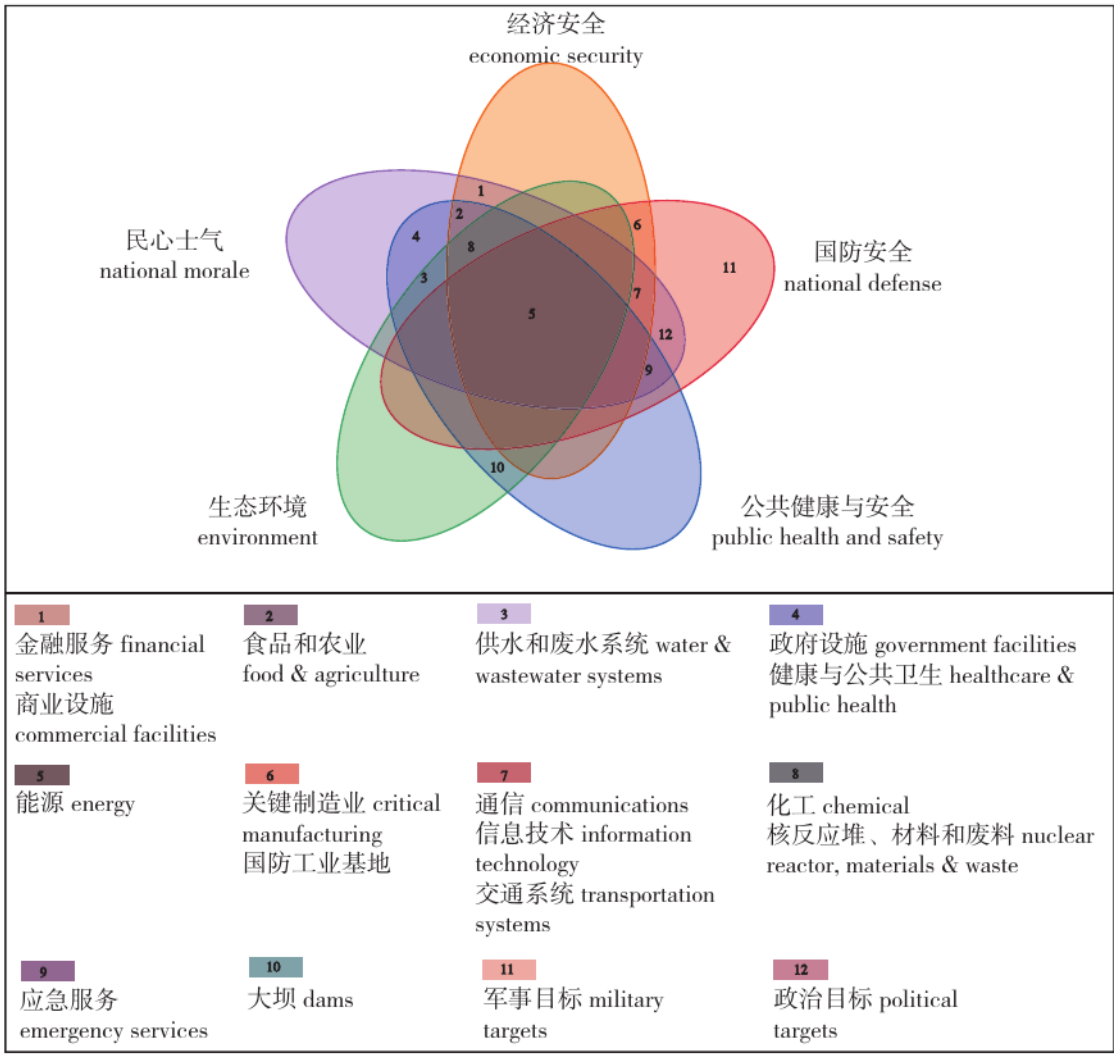

Fig.1 Classification of protective functions for critical infrastructure and military and political targets[3,12,26]

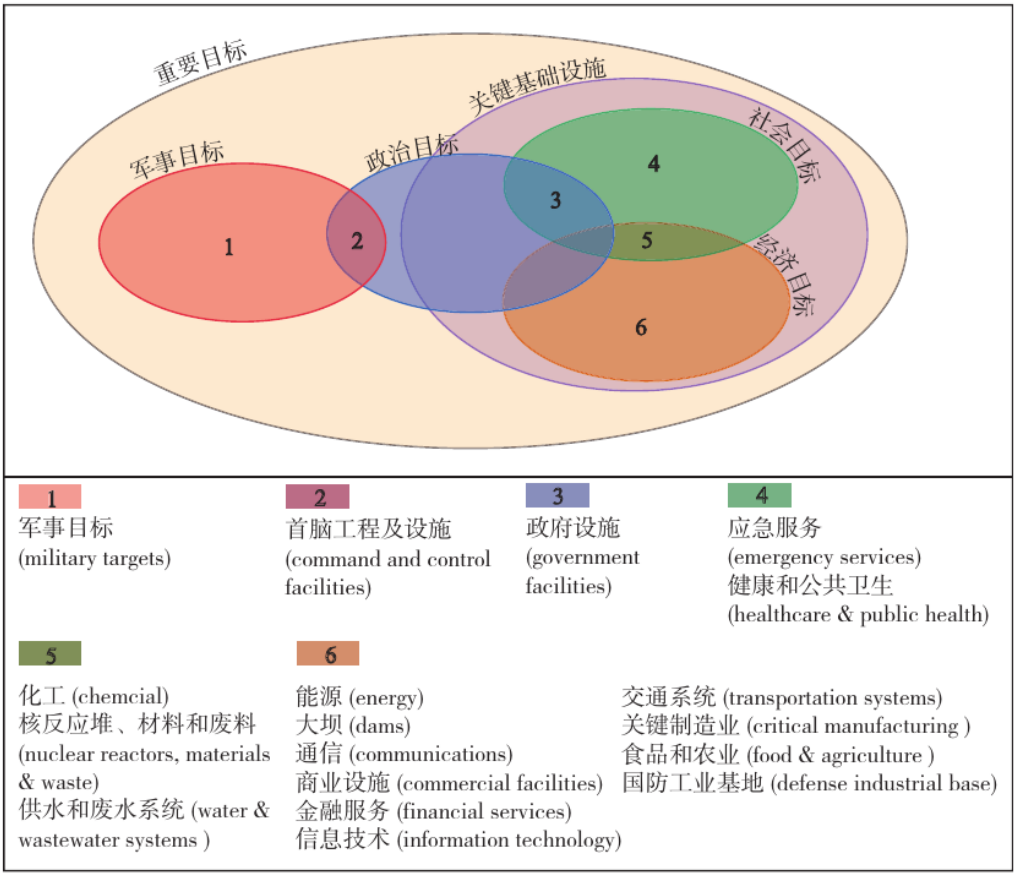

Fig.2 The relationship between critical infrastructure and political targets, military targets, and essential targets[3,12,26]

2 Overview of Critical Infrastructure Protection Planning in China and the United States

2.1 Critical Infrastructure Protection Planning and Development in China

Protecting economic targets and protecting the population are the two basic tasks of China's civil air defense system[27]. Beginning in the 1950s, regulations concerning civil air defense measures for factories were introduced. In the 1960s and 1970s, China established and implemented the Third Front planning strategy of locating facilities “near mountains, dispersed, and concealed.” Large numbers of important industrial enterprises were relocated from border and coastal areas to the interior, while cities constructed dual-use personnel shelters and underground production workshops. These measures substantially enhanced national and urban protective capacity and provided effective deterrence against war[28].

From the 1980s into the twenty-first century, the development of precision-guided weapons made fixed economic targets increasingly vulnerable, further highlighting the importance of protection. National authorities and civil air defense departments repeatedly issued documents requiring stronger protection of important economic targets. Military and civilian research institutions explored integrated protection systems combining traditional measures - such as rational spatial distribution, underground construction, emergency repair, and rapid restoration - with information-age techniques represented by interference and decoying, in order to strengthen wartime air-defense capacity[28].

At the planning and construction level, critical infrastructure protection has become a primary task of civil air defense[27]. National laws and regulations explicitly require the preparation of economic-

target protection plans, and some provinces and cities have begun exploratory practice. Nevertheless, the scope of critical infrastructure protection is exceptionally broad[29-30]. National pilot programs remain at an exploratory stage, and targeted regulations, effective organizational and management mechanisms, and planning standards are still insufficient[31]. Consequently, actual implementation is limited, and cases incorporated into urban-system layouts and territorial spatial plans are even rarer.

2.2 Infrastructure Protection Planning in the United States

In June 2006, pursuant to Homeland Security Presidential Directive 7[32], the first U.S. National Infrastructure Protection Plan defined the division of responsibilities among security partners involved in critical infrastructure protection, established a broadly comprehensive management framework, and designed a relatively complete model for organizational cooperation and information sharing. It emphasized consensus through extensive coordination and communication and integrated protection efforts to improve planning consistency, continuity, and collaboration. As an important policy safeguarding national security and economic stability, the NIPP underwent updates in 2007/2008, 2009, and 2013 and has become a major theoretical and practical guide for U.S. critical infrastructure protection. Its evolution can be divided into a planning-preparation stage, a planning and adjustment stage, and an implementation and supporting-policy refinement stage; key milestones are shown in Fig.3.

The 2007/2008 update was issued at the end of 2007 and took effect in 2008. Its principal purpose was to respond more effectively to increasingly complex and changing cybersecurity threats while strengthening collaboration and information sharing across departments and sectors. Although essentially a supplementary “patch,” the update incorporated lessons from prior practice and stakeholder input and proposed timely improvements that informed the reissued 2009 NIPP.

Compared with the preceding version, the 2009 NIPP changed relatively little. It further clarified responsibilities, emphasized public-private partnerships, promoted technological upgrading, and focused on the long-term, effective execution of the plan.

In 2013, the U.S. Department of Homeland Security drew on practical experience and, for the first time, explicitly articulated the vision, mission, goals, and principles of critical infrastructure protection. The plan placed greater emphasis on risk management, public-private cooperation, information sharing, and resource allocation. It also clearly specified implementation steps for protective action, providing important guidance for the continuing security of U.S. critical infrastructure.

The United States has continued research on a new round of plan revision to address changing threats, security needs, and challenges. From 2021 to 2024, the Cybersecurity and Infrastructure Security Agency issued several versions of the Infrastructure Resilience Planning Framework[41-43] to help state, local, and territorial governments identify critical infrastructure, assess risks, and formulate resilience solutions.

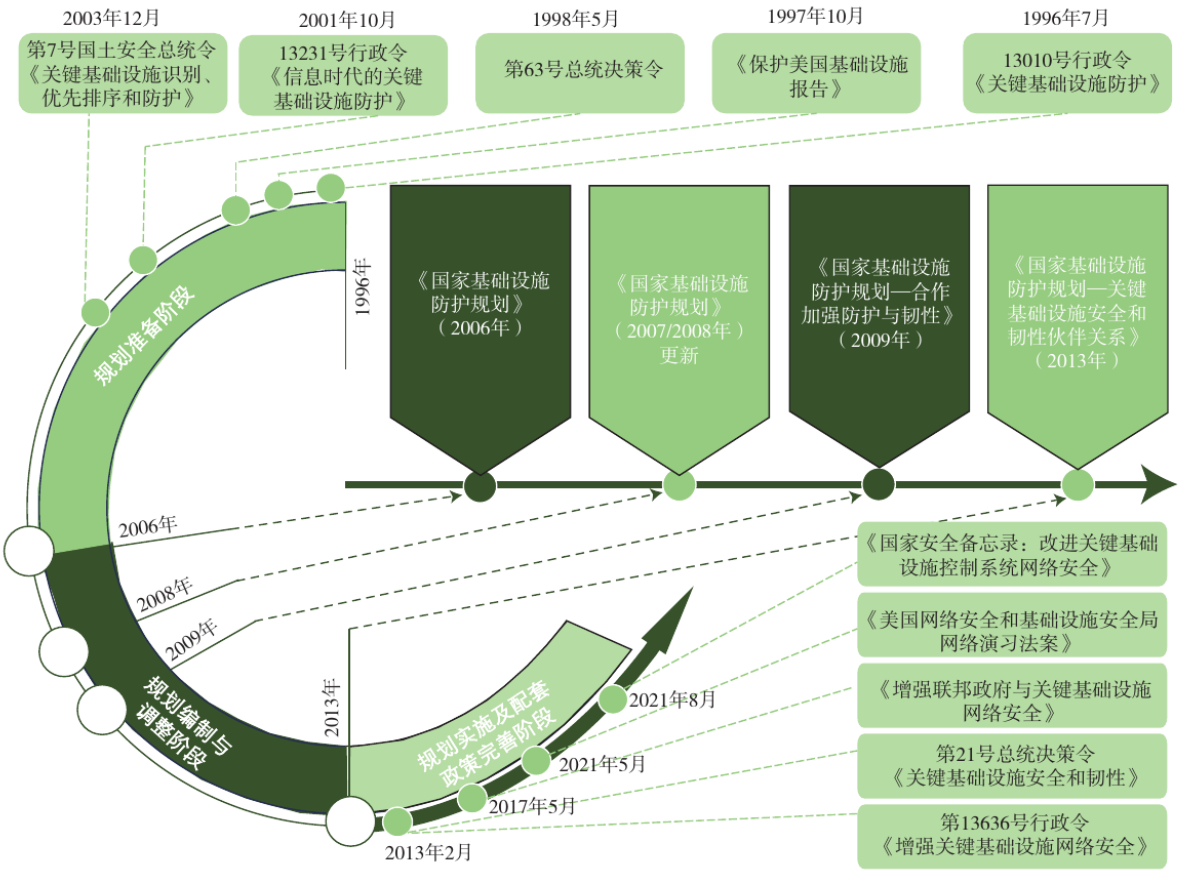

Fig.3 Key milestones in the "national infrastructure protection plan" of the United States[8-12,32-40]

3 Main Contents of U.S. Infrastructure Protection Planning

3.1 Evolution of the Master Framework

Across four versions, the NIPP has undergone dynamic refinement and updating. The original version contained seven chapters covering the introduction; authorities, roles, and responsibilities; protection planning strategy and risk management; organization and partnership for protecting critical infrastructure and key resources; integration of critical infrastructure and key-resource protection into the homeland security mission; ensuring the long-term effectiveness and efficiency of the program; and resourcing critical infrastructure and key-resource protection. By the fourth version, the plan had been condensed from seven chapters to six, with major changes in content: introduction; vision, mission, and goals; the critical infrastructure environment; core principles; partnership-based risk management; and a call to action (Fig.4).

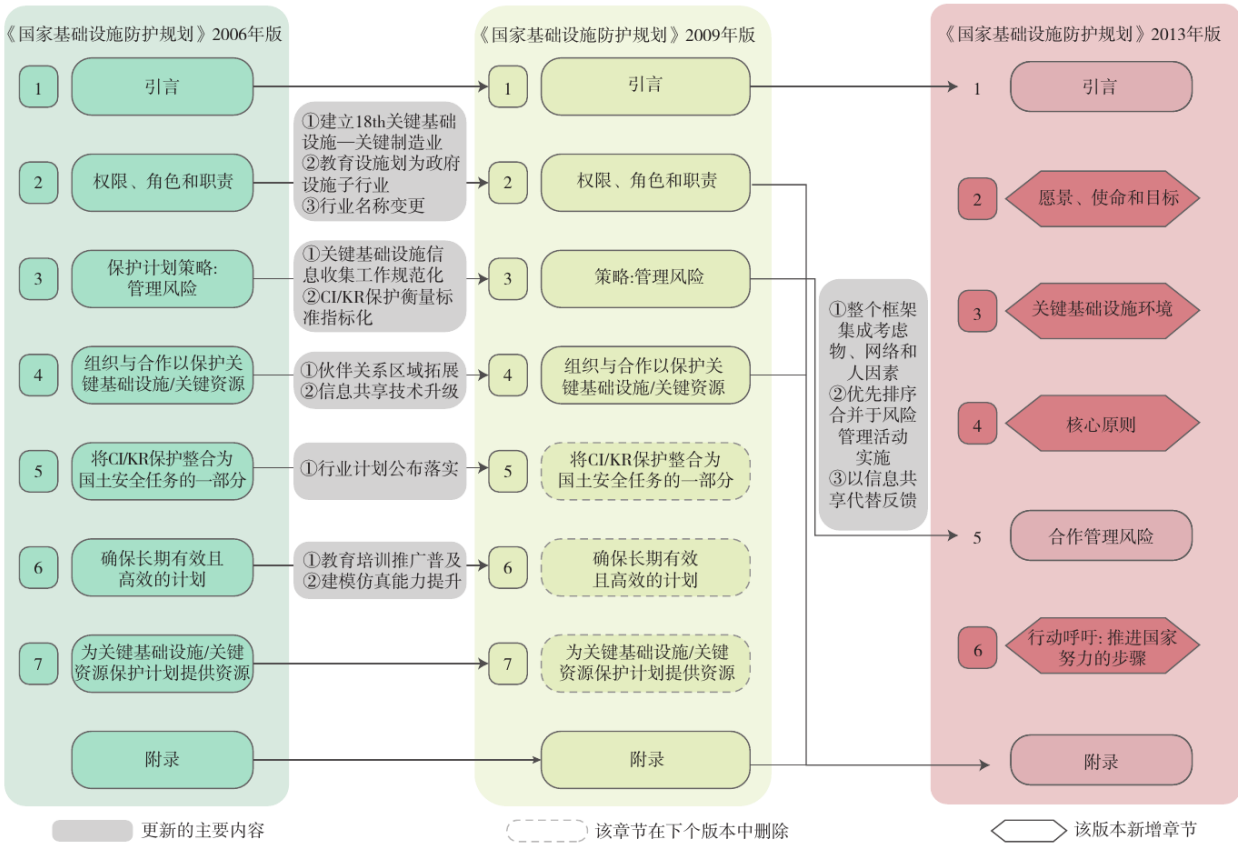

Fig.4 Evolution of the master framework for "national infrastructure protection plan" of the United States[9-12]

3.2 Vision, Mission, Goals, and Core Principles

The NIPP's vision, mission, goals, and core principles were first clearly stated in the 2013 edition. Its vision is a Nation in which physical and cyber critical infrastructure remains secure and resilient by reducing vulnerabilities, minimizing consequences, identifying and disrupting threats, and improving response and recovery. Its mission is to strengthen the security and resilience of national critical infrastructure through coordinated and integrated efforts by the critical infrastructure community.

To achieve this vision and mission, the NIPP establishes five action goals: provide information for risk management; protect critical infrastructure against threats through cost-effective security investment; strengthen resilience through rapid recovery capacity; support decisions through information sharing across the critical infrastructure community; and improve response capability through exercises and drills.

The NIPP also establishes seven core principles: identify and manage risks comprehensively; understand risks arising from cross-sector dependencies and interdependencies; share information across the infrastructure community; recognize the characteristics and strengths of different infrastructures; build consensus among partners on identifying gaps and improving security and resilience; strengthen international cooperation; and incorporate security and resilience into infrastructure design. These principles embody the values and assumptions to be considered when developing critical infrastructure security and resilience plans at national, regional, state, local, tribal, territorial, owner, and operator levels.

Guided by the NIPP's vision, mission, and goals, infrastructure stakeholders collaborate to identify detailed priorities while considering resource availability, achievements to date, current technological gaps, and emerging risks. These priorities promote coordinated action nationwide and are complemented by sectoral, regional, state, local, and tribal priorities. Based on goals, priorities, and

implementation progress, they also support a shared understanding of the current state of critical infrastructure security and resilience.

3.3 Planning and Implementation Mechanisms

The organizational framework for critical infrastructure protection was initially established by Presidential Decision Directive 63, which designated the relevant department for each infrastructure sector as the lead coordinating body, while the federal government assumed implementation responsibility. In 2006, the NIPP reclassified the sectors. As understanding deepened, sectors were renamed, adjusted, and merged, and the concept of "key resources" was discontinued in favor of the unified term "critical infrastructure." The system ultimately comprised sixteen sectors, with a federal department or agency designated as the principal coordinator - the Sector-Specific Agency (SSA) - for each sector, as shown in Tab.1.

Tab.1 Classification of critical infrastructure and associated supervisory agencies of the United States[12]

<table>
<tr><td rowspan="2">关键基础设施
行业分类</td><td rowspan="2">政府分管部门</td><td colspan="5">关键基础设施伙伴关系咨询委员会</td></tr>
<tr><td colspan="2">行业协调委员会</td><td colspan="2">政府协调委员会</td><td>区域联
协调委</td></tr>
<tr><td>化工</td><td rowspan="8">国土安全部</td><td>√</td><td rowspan="15">关键基础设施跨行业委员会</td><td>√</td><td rowspan="15">联邦高级领导委员会</td><td rowspan="15">州、地方、部落和地区政府协调委员会</td><td rowspan="15">区域联
协调委</td></tr>
<tr><td>商业设施</td><td>√</td><td>√</td></tr>
<tr><td>通信</td><td>√</td><td>√</td></tr>
<tr><td>关键制造业</td><td>√</td><td>√</td></tr>
<tr><td>大坝</td><td>√</td><td>√</td></tr>
<tr><td>应急服务</td><td>√</td><td>√</td></tr>
<tr><td>信息技术</td><td>√</td><td>√</td></tr>
<tr><td>核反应堆、材料和废料</td><td>√</td><td>√</td></tr>
<tr><td>政府设施</td><td>国土安全部、总务管理局</td><td>未设置行业协调委员会</td><td>√</td></tr>
<tr><td>交通系统</td><td>国土安全部、交通部</td><td>按运输模式或分行业细分</td><td>√</td></tr>
<tr><td>食品和农业</td><td>农业部、卫生和公众服务部</td><td>√</td><td>√</td></tr>
<tr><td>国防工业基地</td><td>国防部</td><td>√</td><td>√</td></tr>
<tr><td>能源</td><td>能源部</td><td>√</td><td>√</td></tr>
<tr><td>健康和公共卫生</td><td>卫生和公众服务部</td><td>√</td><td>√</td></tr>
<tr><td>金融服务</td><td>财政部</td><td>适用独立的协调实体</td><td>√</td></tr>
<tr><td>供水和废水系统</td><td>环境保护署</td><td>√</td><td>√</td></tr>
</table>

注：√表示该基础设施行业设置了行业协调委员会或者政府协调委员会

3.4 Partnership-Based Risk Management

Risk management is one of the most important components of the NIPP. Through four versions, the updated framework has clarified three elements of critical infrastructure - physical assets, cyberspace, and people - and established five steps: set goals and objectives; identify critical infrastructure; assess and analyze risk; implement risk-management activities; and measure

effectiveness (Fig.5). The framework also emphasizes information sharing throughout the process. Information exchange runs through every step, enabling feedback and continuous improvement in critical infrastructure security and resilience.

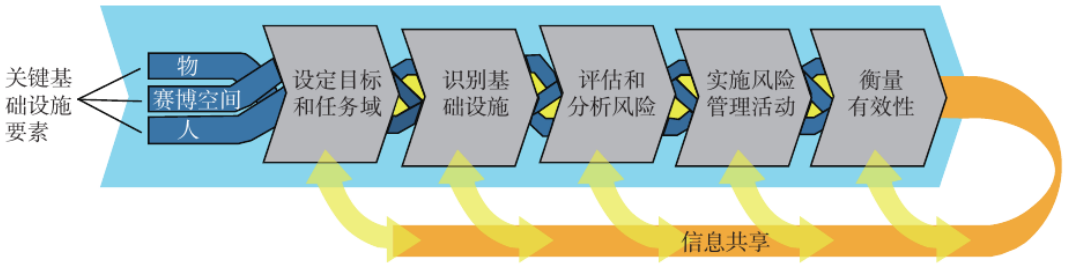

Fig.5 Framework of critical infrastructure risk management of the United States[12]

The plan identifies thirty-one core capabilities supporting five mission areas (Tab.2). The development of many of these capabilities contributes to critical infrastructure security and resilience, and communities, owners, and operators can apply them to identified activities for managing risk. Incorporating critical infrastructure risk when setting capability targets strengthens implementation measures.

Tab.2 Level 5 protection response: 31 core capabilities of the United States[44]

预防	防护	减轻	响应	恢复
规划				
公共信息及警告				
运作协调				
取证和归因	访问控制和验证	社会韧性	关键运输	经济复苏
情报和信息共享	网络安全	长期脆弱性减少	环境响应/健康与安全	卫生和社会服务
阻断和中断	情报和信息共享	风险和灾害韧性评估	死亡管理服务	住房供给
筛查和检查	阻断和中断	威胁和危害识别	基础设施系统	自然和文化资源
	物理防护措施		大众护理服务	基础设施系统
	防护计划和活动的风险管理		大规模搜救行动	
	筛查和检查		现场安全和保护	
	供应链完整性和安全性		业务通信	
			公共卫生、医疗保健和紧急医疗服务	
			公共和私人服务与资源情况评估	

3.5 Planning Implementation Actions

The NIPP groups implementation into twelve actions under three categories, with the aim of enhancing national critical infrastructure security and resilience and mobilizing coordinated action by all stakeholders.

First, it emphasizes partnership-based efforts: jointly establish priorities; identify collective actions through joint planning; empower local and regional partnerships to build national capacity; and use incentives to improve security and resilience.

Second, it calls for innovative risk management: strengthen situational awareness to support risk-based decisions; analyze infrastructure dependencies, interdependencies, and cascading effects; identify, assess, and respond to cascading infrastructure failures during and after incidents; promote the recovery of infrastructure, communities, and regions after emergencies; coordinate technical assistance, training, and education; and advance research and development solutions to further improve critical infrastructure security and resilience.

Third, it emphasizes implementation results: assess progress toward goals and learn and adapt through training and real-world events.

4 Implications for Critical Infrastructure Protection Planning in China

4.1 Organizational Innovation: Institutionalizing Planning Research and Clarifying Working Mechanisms

As noted above, national and some provincial and municipal policies specify that civil air defense authorities (or development and reform authorities) and sectoral departments should prepare master plans for the protection and construction of important economic targets and critical infrastructure. Compared with other specialized territorial spatial plans, however, few such plans have been implemented because critical infrastructure protection spans many fields and involves exceptionally complex mechanisms[30]. The U.S. experience shows that, in addition to clearly assigning leadership to the Department of Homeland Security, national planning requires the participation of more than ten departments, including transportation, energy, agriculture, commerce, environmental protection, and finance. Sector councils, government coordinating councils, regional consortia, and other organizational and working mechanisms are also needed.

China should draw on this experience while adapting it to national conditions. Civil air defense or development and reform authorities should take the lead, together with transportation, energy, industry and information technology, finance, and other relevant departments, to coordinate cross-departmental resources and ensure that planning research is institutionalized, normalized, integrated, and continuous. Bodies such as a Critical Infrastructure Government Coordinating Council and Sector Coordinating Councils should be established. Plans should define unified leadership and organization, funding allocation, project design, supervision and inspection, policy implementation, and other functions and mechanisms so that protection resources across sectors can be shared and used efficiently. Responsibilities should be further clarified in accordance with the principles that civil air defense and sectoral authorities “guide, supervise, and coordinate critical infrastructure protection,” while infrastructure entities “prepare protection programs, plans, and work schedules”[45-46].

4.2 Planning Leadership: Initiating and Continuously Improving Critical Infrastructure Protection Plans

Critical infrastructure protection belongs to territorial defense and is also an important component of national defense construction. It is therefore indispensable to territorial spatial planning and urban planning. China has already established explicit requirements concerning urban infrastructure protection, civil air defense works, and the coordinated provision of underground space[47-48]. Some territorial spatial master plans and civil air defense special plans contain provisions for the protection of “important targets,” but these are fragmented. Drawing on international experience, China should uphold “planning as the framework,” adopt a strategic perspective, and promptly initiate critical infrastructure protection planning with the participation of national, provincial, municipal, sectoral, interdepartmental, community, and enterprise actors. Planning should integrate resources, establish

goals, design projects, determine priorities, allocate responsibilities, and steadily improve the capacity of critical infrastructure to cope with uncertain risks.

Critical infrastructure is extensive, spans numerous sectors, and is exceptionally complex to manage[18]. Countries are still exploring the field, and no mature framework or version can simply be copied. The U.S. NIPP underwent four versions within its first seven years and remains subject to continuing adjustment. China likewise cannot complete the task at once. It should first initiate planning and solve the problem of whether such plans exist, then continue to improve and update them while maintaining policy continuity.

During planning and implementation, protection of specific categories or individual facilities should follow the principle of classified protection. Critical infrastructure entities, governments, and sectoral management departments should clearly define their respective responsibilities and obligations. Government and sectoral departments should organize education and training, establish technical expert pools, and formulate protection codes and standards. Infrastructure entities should prepare and implement their own protection plans, organize necessary exercises, and establish recovery mechanisms and backup systems for critical functions.

4.3 First Step: Clarifying Planning Classification, Grading, and Related Codes and Standards

Classification and grading, as part of conceptual clarification, constitute the first step in critical infrastructure protection planning. Since the beginning of the twenty-first century, the United States has expanded the scope of protection beyond infrastructure supporting warfare and economic operation to include public rescue and healthcare systems affecting public health and safety, facilities affecting national morale, and infrastructure related to the ecological environment. The four NIPP versions show continuous optimization of infrastructure categories and names (Tab.3). China currently lacks national classification and grading standards. Provincial and municipal classifications focus mainly on national defense and economic security and have not yet fully considered infrastructure related to public health and safety, national morale, or the ecological environment. International experience suggests that concepts of classification and grading should continue to evolve and that the development of standards should be treated as a priority in planning preparation.

Tab.3 The optimization process of categorizing critical infrastructure in the United States[9-12]

关键基础设施分类	NIPP版本		
	2006年版本	2009年版本	2013年版本
食品和农业	√	√	√
国防工业基地	√	√	√
能源	√	√	√
健康与公共卫生	√	√	√
国家纪念碑和标志	√	√	× 合并到“政府设施”
银行和金融	√	√	√ 更名为“金融服务”
饮用水和水处理系统	√	√ 更名为“供水”	√ 更名为“供水和污水处理服务”
化工	√	√	√
商业设施	√	√	√
大坝	√	√	√
应急服务	√	√	√
商业核反应堆、材料和废物	√	√ 更名为“核反应堆、材料和废物”	√
信息技术	√	√	√
电信	√	√ 更名为“通信”	√
邮政和船运	√	√	× 合并到“交通系统”
交通系统	√	√	√
政府设施	√	√	√
关键制造业	×	√	√

注：①√表示在该版本中存在，×表示不存在；②NIPP的2007/2008年版本作为补充更新，变化较小，表中对该版本未体现

Grading is one of the most difficult aspects of critical infrastructure protection planning. Provinces and cities usually grade facilities according to local conditions and the “importance” of the facility itself. A steel enterprise in southern China, for example, may appear unquestionably critical when judged by local output value and importance, but its national significance is debatable because it may be substitutable when compared with steel-producing provinces in northern China. Critical infrastructure functions as a system reflecting overall social performance. A common and serious error, identified in the NIPP and related U.S. studies, is inadequate understanding of dependencies among different facility categories. Lifeline functions such as communications, energy, transportation, and water are central to such dependencies and interdependencies. Failure of one function may cause cascading disruption, severe consequences, and impairment of preparedness plans and capabilities. During an urban emergency, for example, the water-supply system depends on stable electricity; power repairs depend on road access; and road accessibility is constrained by command-and-communications systems and emergency repair services. China currently gives insufficient attention to dependencies in

grading. Scientific classification and grading methods and standards based on dependency criteria are urgently needed.

Foresight is an essential characteristic of planning, and related codes and standards should fully consider how emerging technologies and their application may affect planning. Technological iteration will drive continuing change. Under conditions of informationized and intelligent warfare, cities face operational modes that seek to paralyze an entire system by striking key nodes, making stable critical infrastructure operation even more important and stimulating new protective technologies, planning models, and systems. Three groups of technologies deserve particular attention. The first consists of traditional protective techniques represented by underground construction. Examples include the underground protection design of the Oslo Airport Traffic Control Center[49] and Israel's underground civil-defense blood bank completed in 2022[50-51]. The second consists of information-age protection methods such as interference, decoying, and induced detonation. As early as the 1990s, Academician Qian Qihu argued that responses to high-technology informationized weapons should integrate the resistance of underground structures with information-based protection and other measures[23]. The third consists of category-specific technologies: freshwater supply and fuel-delivery networks require rapid pipeline-leak detection and repair, while chemical plants and other facilities with secondary-hazard potential require protection addressing domino effects. Advances in these three fields will substantially influence planning codes and standards.

5 Conclusion

China's system for preparing urban critical infrastructure protection plans remains exploratory. Although individual provinces and cities have begun practice, the system is not yet mature. The U.S. NIPP offers useful lessons. Compared with the United States, China faces an even more severe security environment. Three immediate tasks are proposed. ① Organizational innovation: civil air defense authorities should take the lead, cooperate with transportation, energy, finance, and other departments, and establish government and sector coordinating councils to clarify functions and working mechanisms. ② Planning leadership: “planning as the framework” should be upheld; planning should begin promptly to resolve the question of whether plans exist, then be continuously improved while maintaining policy continuity. ③ First steps: classification, grading, and related codes and standards should be developed as priorities. Particular attention should be paid to traditional techniques represented by underground construction, information-age methods such as interference, decoying, and induced detonation, and category-specific protective technologies, especially the dependencies among different kinds of infrastructure.

International experience should nevertheless be adopted selectively because national conditions differ. Countries such as the United States have first-mover strengths, while China has the advantage of learning from later development. Although external experience can be instructive, China must build its critical infrastructure protection planning system in accordance with its own institutions and conditions. The U.S. NIPP emphasizes strategic planning and combines strategic design with action plans, whereas strategic planning in China occupies an important position outside the statutory planning system[52-53]. How to adapt such experience to China requires further study. Because confidentiality and time constraints limited access to relevant information, the arguments presented here are preliminary and intended to stimulate discussion. Considerable work remains to develop a critical infrastructure protection planning system suited to China.

References

[1] MA Enshan, KOU Qingao. A Study of Economic Protection Abroad [M]. Beijing: National Defense University Press, 2001. (in Chinese)

[2] Wartime Capital Construction Planning Commission. Draft Ten-Year Construction Plan for the Wartime Capital [Z]. Chongqing: Chongqing Planning Exhibition Gallery and Chongqing Library, compiled in 1946 and reprinted in 2005. (in Chinese)

[3] GUO Dongjun, ZHAO Xudong, FENG Bing, et al. Progress in the classification and grading of important economic targets abroad and its implications [J]. Protective Engineering, 2016, 38(4): 69-78. (in Chinese)

[4] Saisi Think Tank. Analysis of Facility Deployment, Strikes, and Damage in the Russia-Ukraine Conflict [R]. Hebei: Hebei Yipu Saisi Information Technology Co., Ltd., 2023. (in Chinese)

[5] RAN Jing, JIANG Xiaohui, HE Lei, et al. Types, spatial systems, and planning and construction priorities of urban dual-use public infrastructure for routine and emergency conditions [J]. Urban Planning Forum, 2024(5): 98-105. (in Chinese)

[6] HE Lei, DAI Shenzhi, SONG Yan. U.S. experience in preparing and evaluating comprehensive urban disaster-prevention plans and its implications for China [J]. Urban Planning Forum, 2011(5): 87-94. (in Chinese)

[7] LAMBETH B S, LEWIS K N. Economic targeting in modern warfare [R]. Santa Monica, California 90406: The Rand Corporation, 1982.

[8] Administration of Clinton W J. The Clinton administration's policy on critical infrastructure protection: presidential decision directive No. 63 [R]. Washington, D.C.: The White House, 1998.

[9] The Department of Homeland Security. National infrastructure protection plan [R]. Washington, D.C.: The Department of Homeland Security, 2006.

[10] The Department of Homeland Security. National infrastructure protection plan - 2007/2008 update [R]. Washington, D.C.: The Department of Homeland Security, 2008.

[11] The Department of Homeland Security. National infrastructure protection plan - partnering to enhance protection and resiliency [R]. Washington, D.C.: The Department of Homeland Security, 2009.

[12] The Department of Homeland Security. National infrastructure protection plan - partnering for critical infrastructure security and resilience [R]. Washington, D.C.: The Department of Homeland Security, 2013.

[13] Civil Air Defense Law of the People's Republic of China [S]. 1996-10-29. (in Chinese)

[14] National Defense Law of the People's Republic of China [S]. 1997-03-14. (in Chinese)

[15] National Defense Mobilization Law of the People's Republic of China [S]. 2010-02-26. (in Chinese)

[16] Regulations on the Security and Protection of Critical Information Infrastructure [S]. 2021-08-17. (in Chinese)

[17] Inner Mongolia Autonomous Region Regulations on the Protection and Management of Important Economic Targets [S]. Inner Mongolia Daily (Chinese edition), 2022-09-07(006). (in Chinese)

[18] DAI Shenzhi, LIU Tingting, GAO Xiaoyu, et al. Planning strategies for critical municipal infrastructure in China's large cities during transition: a case study of Taiyuan [J]. Urban Planning Forum, 2019(S1): 212-219. (in Chinese)

[19] DAI Shenzhi, LIU Tingting. Transformation strategies for municipal infrastructure planning in a new round of metropolitan master plans [J]. Urban Planning Forum, 2018(1): 58-65. (in Chinese)

[20] XIE Lei, ZHOU Yangjun. Guidelines for integrated municipal infrastructure planning based on protective-distance analysis [J]. Urban Planning Forum, 2012(S1): 245-250. (in Chinese)

[21] CPC Central Committee. Recommendations on Formulating the Fourteenth Five-Year Plan for National Economic and Social Development and the Long-Range Objectives through 2035 [EB/OL]. [2020-10-29]. https://www.gov.cn/zhengce/2020-11/03/content_5556991.htm. (in Chinese)

[22] Political Bureau of the CPC Central Committee. Meeting reviews the National Security Strategy (2021-2025) [EB/OL]. [2021-11-18]. https://www.gov.cn/xinwen/2021-11/18/content_5651753.htm. (in Chinese)

[23] ZHU Daming, LI Xiaojun, WANG Zhenyu, et al. “Integrated protection” and “protection of operational systems” [J]. Protective Engineering, 2013, 35(3): 5-9. (in Chinese)

[24] Defense Production Act [S]. 1950-09-08.

[25] BOVEN T L. The DOD key asset protection program [R]. U.S. Army War College, Carlisle Barracks, PA 17013-5050: FEMA, 1989.

[26] Law of the People's Republic of China on the Protection of Military Installations [S]. 1990-10-28. (in Chinese)

[27] GUO Yanpeng, QIN Youquan, ZHENG Ying, et al. Protection of important economic targets in informationized warfare [J]. Science & Technology Review, 2020, 38(20): 106-112. (in Chinese)

[28] QIAN Qihu. Selected Papers of Academician Qian Qihu [M]. Beijing: Science Press, 2007. (in Chinese)

[29] ZHANG Shangwu, PAN Xin. Strategic considerations for planning and constructing major cross-regional infrastructure in the new era [J]. Urban Planning Forum, 2021(2): 38-44. (in Chinese)

[30] DAI Shenzhi, LIU Tingting, GAO Xiaoyu, et al. Planning system and implementation mechanism for territorial disaster prevention and mitigation [J]. Urban Planning Forum, 2023(1): 48-53. (in Chinese)

[31] XIA Yu, REN Weiyang. Technical standards for smart infrastructure planning in Xiong'an New Area [J]. Urban Planning Forum, 2022(5): 107-111. (in Chinese)

[32] Administration of Bush G W. Homeland security presidential directive/HSPD-7 - critical infrastructure identification, prioritization, and protection [R]. Washington, D.C.: The White House, 2003.

[33] Administration of Clinton W J. Executive Order 13010 - critical infrastructure protection [R]. Washington, D.C.: Federal Register, 1996.

[34] Administration of Obama B H. Presidential Policy Directive/PPD-21 - critical infrastructure security and resilience [R]. Washington, D.C.: The White House, 2013.

[35] Administration of Bush G W. Executive Order 13231 - critical infrastructure protection in the information age [R]. Washington, D.C.: Federal Register, 2001.

[36] The Department of Homeland Security. The report for the Department of Homeland Security [R]. Washington, D.C.: The Department of Homeland Security, 2002.

[37] OBAMA B H. Executive Order 13636 - improving critical infrastructure cybersecurity [R]. Washington, D.C.: Federal Register, 2013.

[38] TRUMP D J. Executive Order 13800 - strengthening the cybersecurity of federal networks and critical infrastructure [R]. Washington, D.C.: Federal Register, 2017.

[39] Cybersecurity and Infrastructure Security Agency Cyber Exercise Act [R]. 2021-01-01.

[40] Executive Office of the President of the United States. National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems [R]. Washington, D.C.: The White House, 2021.

[41] Cybersecurity and Infrastructure Security Agency. Infrastructure Resilience Planning Framework Version 1.0 [R]. Washington, D.C.: U.S. Government Publishing Office, 2021.

[42] Cybersecurity and Infrastructure Security Agency. Infrastructure Resilience Planning Framework Version 1.1 [R]. Washington, D.C.: U.S. Government Publishing Office, 2023.

[43] Cybersecurity and Infrastructure Security Agency. Infrastructure Resilience Planning Framework Version 1.2 [R]. Washington, D.C.: U.S. Government Publishing Office, 2024.

[44] Department of Homeland Security. National Preparedness Goal [R]. Washington, D.C.: Department of Homeland Security, 2011.

[45] Opinions of the Shandong Provincial Civil Air Defense Office on Strengthening the Protection and Management of Important Economic Targets [J]. Gazette of the People's Government of Shandong Province, 2021(3): 41-43. (in Chinese)

[46] Beijing Municipal Civil Air Defense Regulations [S]. 2002-03-29. (in Chinese)

[47] YAO Wenqi. Methods for underground-space planning in urban central areas: a case study of Bao'an Central District, Shenzhen [J]. Urban Planning Forum, 2010(S1): 36-43. (in Chinese)

[48] TANG Yuqing, ZHOU Bingyu. Planning control of underground space in central districts of China's large cities: a case study of Huangdao Central Business District, Qingdao [J]. Urban Planning Forum, 2006(5): 89-94. (in Chinese)

[49] LITTLE R G, PATTAK P B, SCHROEDER W A. Use of underground facilities to protect critical infrastructures: summary of a workshop [R/OL]. Washington, D.C.: National Academy of Sciences, 1998. http://www.nap.edu/catalog/6285.html.

[50] JEFFAY N. Israel opens world's most protected blood bank, rocket-proof and underground [EB/OL]. [2022-05-02]. https://www.timesofisrael.com/israel-opens-worlds-most-protected-blood-bank-rocket-proof-and-underground/.

[51] NEHAMA-ABADI R, ADOM M D. A vision of dedication, determination to save lives [EB/OL]. [2022-09-25]. https://www.jpost.com/special-content/magen-david-adom-a-vision-of-dedication-determination-to-save-lives-718089.

[52] ZHENG Guo. Changes in local-government behavior and the evolution of urban strategic planning [J]. City Planning Review, 2017, 41(4): 16-21. (in Chinese)

[53] XU Ze, ZHANG Yunfeng, XU Ying. A ten-year review and outlook of strategic planning: a case study of the Ningbo 2030 Urban Development Strategy [J]. City Planning Review, 2012, 36(8): 73-79. (in Chinese)

Revised: December 2024