Techno-Economic Security: Research Priorities, Evolution Mechanism, and Evaluation Framework Postprint

Authors: Cheng Yanlin, Dai Tao, Ding Yuye, Zhao Danyang

Date: 2023-05-08T00:00:00+00:00

Abstract

Against the backdrop of a new round of technological revolution and industrial transformation, issues related to techno-economic security have become a common focus of attention for major countries and regions. From the perspective of discipline construction, this article conducts fundamental theoretical research around key questions such as "why," "what," and "how to evaluate," analyzing the importance and urgency of focusing on techno-economic security, proposing key techno-economic security issues that should be prioritized at different levels including technology, enterprise, industry, nation, and region, constructing a framework for the occurrence and evolution mechanisms of techno-economic security composed of four components: environmental inducement, factor transmission, multiple feedback, and spatiotemporal evolution, and on this basis, forming a TMAPS (Technology-Market-Agent-Policy-Security) model and indicator framework for techno-economic security assessment. This research work helps to further clarify the connotation and boundaries of techno-economic security, and provides theoretical and methodological support for strengthening techno-economic security assessment and ensuring the level of techno-economic security.

Full Text

Special Issue: Theory and Practice of Techno-economic Security

As the world undergoes profound changes unseen in a century, a new round of scientific and technological revolution and industrial transformation is accelerating, intensifying international competition in science, technology, and the economy. Major countries worldwide are attaching great importance to technological sovereignty and strategic dominance, strengthening their techno-economic security. China's 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives Through 2035 explicitly calls for "strengthening techno-economic security assessment," creating an urgent need to enhance research on assessment theories and methods, the interaction mechanisms between technological and economic security, and strategies for safeguarding techno-economic security. To this end, the *Bulletin of the Chinese Academy of Sciences* has organized this special issue on "Theory and Practice of Techno-economic Security," inviting relevant experts and scholars to address key issues including theoretical methods, evaluation frameworks, and practical experiences, with the aim of providing methodological insights for strengthening techno-economic security assessment and decision-making references for national policy formulation. This special issue was guided by Professor Li Xiaoxuan, Director of the Center for Management Innovation and Evaluation at the Institutes of Science and Development, Chinese Academy of Sciences.

Techno-economic Security: Key Issues, Evolution Mechanism and Evaluation Framework

Against the backdrop of the new round of scientific and technological revolution and industrial transformation, issues related to techno-economic security have become a common focus for major countries and regions. From a disciplinary development perspective, this paper conducts foundational theoretical research around key questions of "why," "what," and "how to evaluate," analyzing the importance and urgency of focusing on techno-economic security. It proposes key techno-economic security issues that should be prioritized at different levels—technology, enterprise, industry, and nation/region—constructs a framework for the occurrence and evolution of techno-economic security comprising four components: environmental induction, factor transmission, multiple feedback, and spatio-temporal evolution. Based on this framework, it develops the TMAPS (Technology-Market-Actors-Policy-Security) model and indicator framework for techno-economic security evaluation. This research helps further clarify the connotation and boundaries of techno-economic security and provides theoretical and methodological support for strengthening techno-economic security assessment and safeguarding techno-economic security levels.

Keywords: techno-economic security, national security, evolution mechanism, evaluation framework, TMAPS (Technology-Market-Actors-Policy-Security) model

---

Problem Statement

The world today is experiencing profound changes unseen in a century, with intensifying great power competition. Emerging technologies such as big data, artificial intelligence, and quantum information are accelerating their integration and penetration into economic and social domains, continuously reshaping the global economic landscape and governance system. All nations are seeking "technological breakthroughs," placing science and technology at the core of enhancing economic competitiveness, comprehensive national power, and safeguarding national security. Maintaining techno-economic security is an inevitable requirement for developed countries to sustain their leading positions and implement technological protection, as well as an urgent need for developing countries to seize development opportunities and respond to risks and challenges.

From an international perspective, competition in comprehensive national strength, primarily manifested as economic and technological competition, has become increasingly prominent, making techno-economic security a key focus for major nations. In its successive national security strategies, the United States has emphasized safeguarding national and economic security by consolidating technological advantages, explicitly identifying competition in critical and emerging technology areas such as advanced computing, advanced manufacturing and materials, and artificial intelligence as an important pillar of its national security. To achieve strategic autonomy, promote technological sovereignty, and reduce external technological dependence, the European Union introduced the "EU Security Union Strategy (2020–2025)" in 2020, prioritizing cybersecurity, critical infrastructure, and technology security. In 2022, Japan enacted the Economic Security Promotion Act, addressing supply chain security, infrastructure security, advanced technology cooperation, and non-disclosure of specific patents to reduce excessive external dependence and ensure stable supply of strategic materials such as semiconductors and pharmaceuticals. In 2021, Australia launched its "Critical Technologies Action Plan" to safeguard economic interests, national security, and social prosperity, identifying 63 critical technologies across seven domains including quantum, energy, and remote sensing for prioritized attention and protective measures. Evidently, reducing technological dependence on foreign sources and consolidating technological advantages have become common policy priorities for major countries and regions to safeguard economic and national security—the very essence of techno-economic security.

From China's development needs, safeguarding techno-economic security by addressing weaknesses and strengthening strengths is an urgent requirement for achieving high-level technological self-reliance and high-quality economic development. The 20th National Congress of the Communist Party of China identified the next five years as a critical period for building a modern socialist country in all respects, with "achieving new breakthroughs in high-quality economic development, significantly enhancing self-reliance and self-improvement in science and technology, and making major progress in building a new development pattern and a modernized economy" as primary objectives. Currently, the new round of scientific and technological revolution and industrial transformation is reshaping the global innovation and economic landscape, with the United States, European Union, Japan, and China accelerating deployment in key areas such as artificial intelligence, quantum information, and clean energy to seize opportunities. China still faces challenges including dependence on foreign sources for key core technologies, insufficient competitiveness in future technologies, and unstable industrial and supply chains, resulting in a severe techno-economic security situation. To gain advantages in intense international competition, ensure high-quality economic development, and achieve high-level technological self-reliance, China must address its weaknesses while strengthening its strengths, keeping techno-economic security risks within acceptable ranges to ensure high-quality development through high-level security.

From the perspective of the national security system, techno-economic security represents the intersection of technological security and economic security, constituting core content for safeguarding national security in the innovation-driven development stage. Under the guidance of a holistic approach to national security, China's national security system has been gradually enriched and improved, forming a comprehensive system encompassing political security, economic security, technological security, and other domains. The national security system exhibits hierarchical and structural characteristics, comprising basic first-level elements as well as numerous secondary elements not yet fully articulated. Techno-economic security derives from national security as a subset and secondary element at the intersection of technological and economic security. Technological security primarily focuses on the safety of the science and technology system and its safeguarding role in other national security domains, while economic security centers on strategic resource supply, industrial survival and development, financial system operation, and fiscal balance. Techno-economic security, however, is grounded in the techno-economic system, focusing on technology acquisition, output, supply, transfer, transformation, development, and application, as well as market performance, with the goal of ensuring the security of economic benefits from technology and controlling the economic constraints imposed by technological factors within acceptable levels. In the innovation-driven development stage, techno-economic security extends technological security to ensure that science and technology safeguard economic development and economic security, while serving as the core of economic security and the key to safeguarding other aspects of economic security.

From a research perspective, techno-economic security studies remain in the exploratory and initial stages, requiring continuous in-depth research on basic theories, formation mechanisms, and situation assessment. Existing studies have explored concepts of techno-economic security, its influencing factors and mechanisms, and assessment content and methods. However, overall, techno-economic security research is still nascent, manifesting in three aspects: First, in disciplinary construction, "National Security Studies" was established as a first-level discipline in 2020, with its theoretical system and research methods currently under development. How to conduct techno-economic security research within the national security framework requires further exploration. Second, in basic theory, while the impact of technology on economic growth has attracted widespread scholarly attention, research on the mechanisms through which technology affects economic security remains scarce, and consensus on the research boundaries of techno-economic security has yet to form. Third, in assessment methods and practice, relatively comprehensive evaluation systems for different levels of actors and different types of risks have not yet been established, necessitating continuous improvement and development of techno-economic security assessment methodologies.

Key Research Issues in Techno-economic Security

Techno-economic security is a complex, multi-level, multi-actor, and multi-dimensional system encompassing four levels from micro to macro: technology, enterprise, industry, and nation/region. Different levels exhibit varying influencing factors and degrees of impact, with distinct key issues and content requiring attention .

At the **technology level**, the focus is on micro-level techno-economic security issues, including risks in technology acquisition, transfer, and usage. First, in technology acquisition, which occurs through external and internal channels, it is necessary to comprehensively consider the security of external acquisition channels and the substitutability of internal supply. Technologies with high external dependence, single sources, and no domestic alternatives pose high techno-economic security risks. For example, extreme ultraviolet (EUV) lithography machines are currently monopolized by the Dutch company ASML; once access is lost, high-end chip production becomes impossible. Second, in technology transfer and application, while external technology transfer generates benefits, it may also enhance competitors' capabilities, creating a "security dilemma." Moreover, only technologies that gain market recognition can generate corresponding economic benefits; inappropriate technology route choices may result in a situation of "having technology without a market." For instance, despite its advanced technology, the Airbus A380 was discontinued due to high operating costs and insufficient market demand. Third, in technology usage, technology safety accidents and technology misuse also create economic security issues. For example, Samsung's Galaxy Note7 phones experienced explosions due to battery defects, leading not only to poor product sales but also threats to life and health. The misuse of deep synthesis technologies such as AI face-swapping and voice synthesis is also creating increasing economic and social risks.

At the **enterprise level**, the focus is on supply chain security and the enterprise's own competitiveness and sustainable development capabilities. First, ensuring supply chain security is paramount. In today's highly complex technological environment, no single enterprise can produce products entirely on its own and must cooperate with other enterprises in the supply chain. However, the exit of any node enterprise in the supply chain can cause overall transaction costs to rise and fluctuate, bringing various uncertainties and risks. Therefore, focusing on supply chain security is the primary task for enterprises to safeguard their techno-economic security. Second, enhancing the competitiveness of key technologies and products is essential. Enterprises must ensure technological competitiveness by focusing on technology advancement, stability, and cost-effectiveness, while also improving market competitiveness by focusing on market share, user acceptance, and production/sales volumes. Once competitiveness in technology and products becomes insufficient, it directly impacts production and business operations. Third, expanding survival and development space involves enterprises enhancing their technological and market capabilities through overseas investment, mergers and acquisitions, and continuous R&D investment to maintain sustainable competitiveness. During this process, risks such as investment security reviews, intellectual property security, and loss of key core technical talent also threaten enterprise development.

At the **industry level**, the focus is on industrial chain security and its influencing factors, including import-export trade, talent pools, and international governance discourse. First, industrial chain security is critical. An industry comprises upstream, midstream, and downstream segments. For example, the integrated circuit industry chain includes not only design, manufacturing, and packaging but also upstream materials and equipment. Due to its long and complex chain, the absence of any segment can create a "broken chain" risk. Therefore, techno-economic security at the industry level must emphasize both the controllability of key technologies and industrial generic technologies and the overall security and stability of the industrial chain. Second, import-export trade security matters. External technology controls or other factors that block imports or restrict exports of key technologies and products affect production and operations of enterprises within the industry, thereby impacting the entire industry. Third, talent security is vital. Talent represents the primary resource. Industries need basic research talent to provide source technological support, R&D and engineering talent to enhance key core technology levels and competitiveness, and technology management and business talent to better transform technology into productivity. Issues in recruiting, retaining, and managing high-level talent directly affect the survival and development of the entire industry. Fourth, discourse power in international governance determines an industry's international competitiveness and influence. A country's dominance or participation in international standards and organizations in specific industries directly affects the industry's international competitiveness and discourse power, influencing related technological development and application.

At the **national and regional level**, the focus is on techno-economic security issues from a national security perspective, including security in strategic technology domains, changes in international relations, and balancing development and security. First, security in strategic technology domains has become paramount. In recent years, major countries have strengthened technological autonomy and strategic dominance. South Korea identified 5G communications and artificial intelligence among its "Ten National Strategic Essential Technologies" in 2021, while the United States updated its "Critical and Emerging Technologies List" in 2022, identifying 19 strategic domains including AI, quantum, and space technologies. Techno-economic security in strategic domains has a pivotal effect, enabling countries to concentrate limited resources to strengthen competitive advantages, contain and deter competitors, and significantly enhance security maintenance capabilities. Second, participation in international rules and governance matters. Changes or adjustments in international trade rules, global governance patterns, and industrial structures profoundly impact a country's technological and economic development. For example, the United States and European Union established the Trade and Technology Council (TTC) in 2021 to strengthen multilateral coordination on investment review, export controls, AI, and semiconductor supply chains. Addressing the impact of international relations changes on a country's technology and economic development is a key concern at the national level. Third, balancing security and development encapsulates the contemporary theme and security environment of today's world, with all nations pursuing sustainable security and sustainable development. As a new era issue, techno-economic security requires improving systems and mechanisms, fully leveraging the advantages of the new national system, strengthening strategic national S&T capabilities, and enhancing collaborative innovation among government, industry, academia, research, and users to lay a solid foundation for development and security. Simultaneously, it necessitates optimizing policy supply at the national level, improving policy coordination and effectiveness, and pursuing extensive open cooperation to achieve higher-quality development under the premise of ensuring security, thereby ensuring higher-level security through development.

Formation and Evolution Mechanism of Techno-economic Security

Security issues emerge as internal and external factors evolve; when "dangers" and "threats" appear within or outside a system, security issues arise. Examining the techno-economic security process reveals three key aspects. First, the "dangers" or "threats" to techno-economic security are typically triggered by specific conditions that cause changes at a certain "point," usually threatening a particular element of technology, actors, or markets (under comprehensive containment, multiple points may be directly affected, but analysis can still proceed from a single point). Second, this "point" transmits to other "points," forming changes along "lines," "planes," or "volumes." For example, entire industrial or supply chains or specific industries may face comprehensive threats. Third, techno-economic security is a dynamic, evolving open system that achieves balance. Changes in techno-economic security status trigger feedback among relevant variables and intervention measures, leading to the establishment of new orders and driving a new round of techno-economic security processes. Based on this understanding, the formation and evolution mechanism of techno-economic security involves four mechanisms: environmental induction, factor transmission, multiple feedback, and spatio-temporal evolution [Figure 1: see original paper].

Environmental induction mechanism refers to techno-economic security issues triggered by environmental conditions. Factors triggering techno-economic security problems include both technological and non-technological elements. Technological factors such as technology export controls, emergence of disruptive technologies, technology safety accidents, and intellectual property disputes can trigger changes in technology acquisition, R&D, and product application. Non-technological factors including changes in international rules, establishment of exclusive strategic alliances, major strategic and policy adjustments, and industrial transfers can also induce changes in technology routes, market demand, and competitive landscapes. Additionally, sudden events such as pandemics, financial crises, and geopolitical conflicts can trigger techno-economic security status changes.

Factor transmission mechanism refers to the entire process through which technological factors create economic security impacts via progressive transmission among internal system elements. This mechanism typically involves risk sources, risk carriers, and risk transmission pathways. Risk sources are objective factors affecting techno-economic risks, with the aforementioned triggers forming important components. Risk carriers are tangible or intangible substances carrying risk factors, generally including technologies, equipment, people, enterprises, and research institutions. Risks transmit among these elements through various pathways, typically including chain, network radiation, network concentration, and network interactive patterns, with different pathways affecting transmission speed, scope, and stability. Taking high-end chips, key components, and materials vulnerable to "chokepoints" in the international industrial division system as examples, once "supply cut-off" occurs, it first directly affects relevant technology R&D and product development, subsequently impacting R&D or production activities of enterprises and institutions, leading to changes in market share and import-export trade. Due to strong technological interconnections, this risk radiates and diffuses through multiple pathways, creating a "ripple effect" that impacts broader technologies, actors, and markets, ultimately affecting overall economic security.

Multiple feedback mechanism refers to the feedback effects on diverse elements including technology, actors, and markets after techno-economic security status changes. Multi-level perspective theory posits that socio-technical systems can be divided into macro-level landscape, meso-level socio-technical regime, and micro-level technological niches, with feedback mechanisms operating between and within these three levels. If we view techno-economic security as a dynamically balanced socio-technical system, changes in its security status create pressure on system elements, causing state changes and adjustments among different elements. When new triggers are introduced, different resources and elements undergo reconfiguration and adjustment, inducing a new round of techno-economic security changes through induction and transmission mechanisms, forming a feedback cycle. For example, when techno-economic security levels decline—such as through chip "supply cut-off"—pressure is exerted on chip application markets, leading to extended delivery cycles and unstable supply; on chip application actors, causing difficulty in product acquisition and rising costs; and on technology R&D, hindering technology cooperation and introduction. In response, interventions such as expanding procurement sources, stockpiling inventory, and increasing R&D support can create opportunities for chip autonomy and controllability, maintaining system dynamic balance.

Spatio-temporal evolution mechanism refers to the dynamic changes in techno-economic security elements, status, functions, and structures over time and space. In the temporal dimension, the process from trigger to transmission to feedback exhibits phased patterns and characteristics in techno-economic security status, risk priorities, and future trends, requiring temporal scale analysis to assess development trends and foresee future risks. In the spatial dimension, techno-economic security risks form spatial evolution patterns through transmission among elements, industrial spatial transfer and diffusion, and regional radiation and migration. As era themes shift, international situations change, and national security strategic needs evolve, techno-economic security must undergo continuous accumulation and improvement, deepening and adjustment, and renewal and iteration, requiring sustained in-depth exploration of its evolutionary internal logic and patterns.

These four mechanisms—environmental induction, factor transmission, multiple feedback, and spatio-temporal evolution—constitute the formation and evolution mechanism of techno-economic security, overlapping and influencing each other. Different triggers, technological actors, and development stages produce different characteristics in the formation and evolution of techno-economic security issues, necessitating further research within this framework to identify key variables and elements, reveal correlations among variables, mechanisms of action, and causal relationships.

Evaluation Framework for Techno-economic Security

Correctly understanding the connotation, research issues, and formation mechanism of techno-economic security provides the foundation for its assessment. According to security studies theory, security research must consider the security referent object, specific security threats, security guarantor subjects, and security safeguarding approaches. Based on this theoretical analysis and extension, combined with existing research on the "three capabilities" model for techno-economic security assessment and four types of techno-economic risks and key elements, techno-economic security's key elements can be decomposed into technology (T), market (M), actors (A), and policy (P). These elements collectively determine whether the entire techno-economic system is secure (S) under certain trigger conditions through transmission and feedback mechanisms. Accordingly, this paper proposes the TMAPS (Technology-Market-Actors-Policy-Security) model for techno-economic security evaluation [Figure 2: see original paper], providing a reference for identifying and assessing techno-economic security risks.

Technology (T) is the starting point of techno-economic security research. Scholars have explored how to identify technological risks from a security perspective, including indicators such as technology criticality, technology gaps, and technology autonomy and controllability, as well as safety hazards, technology maturity, and vulnerability before large-scale application of new technologies. From a technological risk perspective, techno-economic security must address both weak-link technologies and leading technologies, current technologies and future technologies. For weak-link technologies, risk identification and assessment should focus on source diversity, external dependence, substitutability of technology supply, technology industrialization levels, and technology export control and supply conditions. For leading technologies, assessment should concentrate on leading performance in technology or markets, degree of leadership, sustainability of competitive advantages, and competitor technology development. For future technologies, assessment should examine technology maturity, industrial readiness, technology competitiveness, and technology control conditions.

Market (M) represents the concrete manifestation of technology's impact on economic security. Industrial organization theory posits that markets comprise products, enterprises, consumers, and their transactional, competitive, and cooperative relationships. From a competitive game perspective, market risks primarily stem from industrial and supply chain stability, market share and recognition, and international market integration. Assessing industrial and supply chain risks requires evaluating dependence on global industrial and supply chain systems and the vulnerability, structure, spatial layout, and changes of industrial and supply chains. Assessing market position risks examines discourse power in pricing, bargaining, and standard-setting. International market integration assesses the degree of integration into other countries' and global markets, the degree of market demand from other countries, and the controls or restrictions imposed by other countries.

Actors (A) are the carriers for maintaining techno-economic security. Universities, research institutes, and enterprises are the main actors in technology R&D, transfer, and application. Technology risks affect economic security through actors, and improving techno-economic security status must rely on relevant actors. Actor risks should be identified and assessed from external threats, technological innovation capabilities, and market development capabilities. External threats include technology controls, intellectual property disputes, and investment restrictions. Technological innovation capability assessment should aim to address technological weaknesses, maintain technological advantages, and resolve technological risks, analyzing quantitative and qualitative indicators related to technology route selection, patent portfolios, and emerging technology deployment and development, including high-value patents, intellectual property licensing fees, and R&D investment structure. Market development capability assessment should aim to develop international markets, maintain competitive advantages, and resolve market risks, focusing on actors' ability to transform key core technologies into products, the market competitiveness of key products, and market actors' profitability, financing capabilities, and investment, merger, and market coordination capabilities.

Policy (P) is the means for safeguarding techno-economic security. Promoting R&D and application of risky technologies and resolving various risks require policy support, yet policies themselves can also induce techno-economic security issues. Policy risks mainly include external restrictive policies and internal policy defects that create techno-economic security risks. External restrictive policies are reflected in major strategic adjustments by competitors and targeted policy measures, with risks assessed through restrictive or sanctioning policy tools and their severity, including the number and types of entities controlled by competitors, control levels and intensity, and the scope of controlled technology fields. Internal policy risks are assessed through the degree of protection for techno-economic security and responsiveness to risks, including deployment of key core and emerging technologies in priority areas, support for breakthrough technology R&D and commercialization, intellectual property protection, strengthened open cooperation, and formulation of technology standards and norms.

Security (S) is the final outcome of the combined effects of the four variables above. Based on the breadth, length, and depth of impacts generated by the four key elements of technology, market, actors, and policy, the level of techno-economic security is comprehensively determined. Breadth refers to the scope of impact, assessed by the number of enterprises involved, industrial fields, and economic losses. Length refers to the duration of impact, assessed by the weight of key elements, correlation with risks, and cumulative effects. Depth refers to the severity of impact, assessed by the degree of change in relevant indicators caused by risk points, such as supply chain disruption, cost increases, and extended cycles.

Based on the TMAPS model analysis, this paper constructs a techno-economic security evaluation framework from five dimensions: technology, market, actors, policy, and security . For different elements, the framework conducts comparative analysis from both internal development levels and external controls and restrictions based on a competitive perspective. This evaluation framework provides a general and comprehensive analytical structure for identifying and assessing techno-economic security risks. However, at specific levels of technology, enterprise, industry, and nation/region, targeted indicators can be selected based on their priorities to conduct assessments using integrated quantitative and qualitative methods.

Conclusion and Outlook

The current complex and volatile international situation has increased uncertainty in the global techno-economic environment. Both the practical need to safeguard techno-economic security and theoretical exploration as an emerging discipline necessitate in-depth research on techno-economic security theories and methods. Based on a disciplinary development perspective, this paper discusses foundational issues including key issues, formation and evolution mechanisms, and evaluation frameworks for techno-economic security. It defines key techno-economic security issues at four levels—technology, enterprise, industry, and nation/region—and proposes an analytical framework for techno-economic security formation and evolution comprising environmental induction, factor transmission, multiple feedback, and spatio-temporal evolution mechanisms. On this basis, it presents the TMAPS model from five dimensions—technology, market, actors, policy, and security—to provide foundational support for in-depth techno-economic security research, strengthened assessment, and risk prevention.

However, as an interdisciplinary field, techno-economic security research involves multiple disciplines including economics, national security studies, management, and political science, requiring further advancement in theoretical research and disciplinary development. As a component of national security studies, techno-economic security's position and role within the national security system, as well as its research boundaries and foundational theories, need further clarification. Future research should deeply explain techno-economic security occurrence and evolution mechanisms, analyzing relationships among different variables and their probabilities, degrees, and pathways of impact on techno-economic security for specific technology and industrial domains. Assessment methodologies should be strengthened, with more targeted identification, monitoring, evaluation, and early warning of techno-economic security risks conducted under the TMAPS framework in combination with specific contexts, providing decision-making support for safeguarding techno-economic security.

References

1. NSTC. *Critical and Emerging Technologies List Update*. (2022-02-17)[2022-09-28]. https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf.

2. Xiao Y. The new trends of EU technology security risk monitoring and early warning mechanism. *Global Science, Technology and Economy Outlook*, 2022, 37(4): 31-37. (in Chinese)

3. Cabinet Office. *The Economic Security Promotion Act: Outline*. (2022-05-11) [2022-09-28]. https://www.cao.go.jp/keizai_{{{anzen}}_{{hosho}}}/doc/gaiyo.pdf. (in Japanese)

4. Australian Government. *The Action Plan for Critical Technologies*. (2021-11-17) [2022-04-24]. https://www.industry.gov.au/sites/default/files/2022-08/ctpco-action-plan-critical-technology.pdf.

5. *A Holistic Approach to National Security Reading Book for Cadres* writing group. *A Holistic Approach to National Security Reading Book for Cadres*. Beijing: People's Publishing House, 2016. (in Chinese)
6. Liu Y J. The bio-security and biological threats in the contemporary national security system. *Frontiers*, 2020, (20): 46-57. (in Chinese)
7. You G R, Zhang B, Zhang S M, et al. National science and technology security: Concept, characteristics, formation mechanism and evaluation framework. *Military Operations Research and Systems Engineering*, 2019, 33(2): 5-10. (in Chinese)
8. Lei J S. Basic issues of national economic security. *Management Review*, 2006, 18(7): 3-7. (in Chinese)
9. Liu Z P, Dai T, Li X X, et al. The concept and connotation of techno-economic security: From the perspective of emerging discipline construction. *Studies in Science of Science*, 2018, 36(3): 410-417. (in Chinese)
10. Liu Z P, Cheng Y L, Dai T, et al. Research on the mechanism of technological dependence on economic security—Based on the perspective of techno-economic security. *Studies in Science of Science*, 2022, doi: 10.16192/j.cnki.1003-2053.20220706.001. (in Chinese)
11. Dai T, Liu Z P, Gan Q, et al. Thinking on issues of techno-economic security evaluation. *Bulletin of Chinese Academy of Sciences*, 2020, 35(12): 1448-1454. (in Chinese)
12. Liu Y. Theoretical and practical research on global supply chain security. *Asia-Pacific Security and Maritime Affairs*, 2022, (4): 29-49. (in Chinese)
13. Liu J Y. Interpretation of the true meaning of sustainable security from the perspective of international strategy. *International Review*, 2014, (6): 1-17. (in Chinese)
14. Li W L. National security: Problems, logic and its discipline construction. *Journal of International Security Studies*, 2020, 38(4): 3-23. (in Chinese)
15. Liu C X, Shu T, Wang S Y, et al. Supply chain disruption risk conduction route based on the small world network. *Systems Engineering-Theory & Practice*, 2015, 35(3): 608-615. (in Chinese)
16. Dijka M, Yarime M. The emergence of hybrid-electric cars: Innovation path creation through co-evolution of supply and demand. *Technological Forecasting and Social Change*, 2010, 77(8): 1371-1390.
17. Liu Z P, Dai T, Li Y J, et al. A study of the "three capabilities" model of techno-economic security evaluation. *Science Research Management*, 2018, 39(5): 77-85. (in Chinese)
18. Chen J, Yang Z, Zhu Z Q. The solution of "neck sticking" technology during the 14th Five-Year Plan period: Identification framework, strategic

change and breakthrough path. *Reform*, 2020, (12): 5-15. (in Chinese)

19. Zhao S J, Dong X H. Causes analysis and countermeasures of science and technology security risks in China in the new era. *Scientific Management Research*, 2021, 39(3): 27-32. (in Chinese)
20. Li T J, Zhao X J. The exploration on ensuring industrial chain and supply chain security in New China. *Journal of Management World*, 2022, 38(9): 31-41. (in Chinese)

Cheng Yanlin is an Assistant Research Fellow at the Institutes of Science and Development, Chinese Academy of Sciences (CASISD). Her primary research interests focus on R&D evaluation and transformation of scientific and technological achievements. E-mail: chengyanlin@casisd.cn

Dai Tao is a Professor at the Institutes of Science and Development, Chinese Academy of Sciences (CASISD) and Deputy Director of the Third Party Evaluation and Research Support Center, CASISD. His current research interests include S&T management and evaluation, and techno-economic evaluation. E-mail: daitao@casisd.cn

Responsible Editor: Yue Lingsheng

Note: Figure translations are in progress. See original paper for figures.