

National Security Governance Mechanisms and Improvement Pathways for Outbound Investment in the Digital Industry

Jialu Hu

*School of Law, Renmin University of China, Beijing, China
2025101847@ruc.edu.cn*

Abstract. The advancement of the Belt and Road Initiative and the rapid development of the digital economy have made the digital industry an important growth area of China's outbound investment. Against this backdrop, establishing a regulatory framework for outbound investment in the digital industry that balances openness and security has become a significant issue in the development of foreign-related rule of law in the digital era. National security risks arising from outbound investment in the digital industry are primarily manifested in risks to data security, technological security, and the security of critical information infrastructure. To address these risks, China has gradually developed a national security governance framework centered on approval and filing procedures, supplemented by information reporting requirements, oriented toward the establishment of an outbound investment security review mechanism, and supported by related regulatory regimes such as data security governance. Nevertheless, the existing governance framework remains subject to several deficiencies. First, institutional coordination is inadequate, as reflected in fragmented regulatory oversight and the lack of effective procedural coordination between investment administration and security review mechanisms. Second, the current regime exhibits insufficient regulatory adaptability, particularly in the inappropriate delineation of the scope of approval-based administration, which fails to accommodate the distinctive regulatory needs of outbound investment in the digital industry. To address these shortcomings, it is necessary to clarify the allocation of powers and responsibilities among competent authorities, define the respective functions of approval and filing procedures, information reporting requirements, and security review mechanisms, and establish a tiered regulatory framework for outbound investment in the digital industry based on the degree of national security risk involved. In addition, the scope of approval-based administration and security review applicable to the digital industry should be more precisely defined, while a risk-identification mechanism centered on critical technologies and other relevant factors should be established and supplemented by catch-all provisions to enhance the adaptability of the regulatory framework.

Keywords: Foreign investment in the digital industry, national security governance, foreign investment management, security review of overseas investments, digital economy

1. Introduction

The digital economy refers to a set of economic activities that take data resources as a key factor of production, modern information networks as an important carrier, and the effective use of information and communication technologies as a major driving force for efficiency improvement and economic structural optimization [1]. With the deepening of the Belt and Road Initiative and the rapid growth of the digital economy, digital technologies, digital industries and digital services are being integrated into China's opening-up landscape at an accelerating pace. The development of the Digital Silk Road has continuously promoted the interconnection of digital infrastructure and international cooperation in fields such as artificial intelligence, cloud computing, big data, e-commerce and digital payment, driving the scale of China's outbound investment in the digital industry to expand continuously [2].

Chinese enterprises have actively made overseas investment arrangements in areas such as digital platforms, digital communication networks, digital services and digital infrastructure. The digital industry has gradually become an important vehicle for China to optimize its outbound investment structure and participate in the restructuring of the global industrial chain. According to the *2024 Statistical Bulletin of China's Outward Foreign Direct Investment* jointly released by the Ministry of Commerce, the National Bureau of Statistics and the State Administration of Foreign Exchange, by the end of 2024, the stock of China's outward foreign direct investment in the information transmission, software and information technology services sector reached 398.15 billion US dollars, and the stock in the scientific research and technical services sector reached 64.3 billion US dollars [3]. The flow of outbound investment in the information transmission, software and information technology services sector grew by 205.5% year on year, significantly higher than the overall growth rate of outbound investment in the same period. The digital industry has become one of the most dynamic growth areas of China's outbound investment [3].

At the same time, the data resources, algorithm models, computing facilities, digital platforms and cross-border information networks involved in outbound investment in the digital industry are highly technology-intensive, mobile and spillover-prone [4]. Unlike traditional industrial investment, which mainly focuses on capital security and industrial security, investment in the digital industry is not only accompanied by cross-border capital flows, but may also bring about issues such as cross-border allocation of data resources, diffusion of key technologies, deployment of digital infrastructure and transfer of platform governance capacity. Its impacts further extend to national security domains including data security, technological security, cybersecurity and even digital sovereignty. How to effectively prevent national security risks while promoting the high-level "going global" of the digital industry, and build a governance system for outbound investment in the digital industry that balances openness and security, has become an important topic in the development of foreign-related rule of law and the modernization of the national security governance system in the digital era.

2. National security risks of outbound investment in the digital industry

At present, China's legal norms and policy documents have not yet formed a unified definition of the "digital industry". Given that the *Statistical Classification of the Digital Economy and Its Core Industries (2021)* issued by the National Bureau of Statistics aligns the "digital industrialization" segment with the core industries of the digital economy, the term "digital industry" in this paper basically adopts the definition of core industries of the digital economy. That is, all kinds of economic activities that provide digital technologies, digital products, digital services, digital

infrastructure and digital solutions for the development of industrial digitalization, as well as economic activities that rely entirely on digital technologies and data factors [1]. Combined with the definition of "outbound investment" in the *Regulations of the State Council on Outbound Investment* (hereinafter referred to as the *Outbound Investment Regulations*), outbound investment in the digital industry can be defined as activities in which domestic investment entities invest in overseas digital industry enterprises, digital infrastructure, digital technology projects or other business entities mainly engaged in digital economic activities by contributing assets, equity or providing financing and guarantees, and obtain corresponding ownership, control rights, operation and management rights or other interests. The development of the digital economy has not only reshaped the way production factors are allocated, but also changed the sources and forms of national security risks in outbound investment [5]. The national security risks triggered by outbound investment in the digital industry are mainly embodied as data security risks, technological security risks and critical information infrastructure security risks.

2.1. Data security risks

Data has become an important strategic resource in the digital economy era [6]. Outbound investment in the digital industry is usually accompanied by cross-border data flows, and realizes domestic and overseas business linkage through data sharing, centralized storage and collaborative processing [7]. In this process, a large amount of user data, commercial data and important industry data may flow overseas continuously, thus increasing the risks of data leakage, illegal acquisition, improper use and overseas control [8].

At the national level, when overseas entities hold or carry important data related to government governance, national defense development and the operation of key industries, the risk of cyber attacks, intelligence theft and data infiltration on relevant data storage facilities and information systems will rise significantly, endangering national information security [9]. At the enterprise level, illegal data handling, unauthorized acquisition and improper use in the process of cross-border data flow are often highly technical and concealed. With the rapid development of the digital economy, overseas cyber attacks and data theft activities aimed at obtaining sensitive information, core technical materials and important data resources of Chinese tech enterprises keep increasing, and related risks keep accumulating [10]. At the individual level, although some data in isolation does not show obvious sensitivity, it may form data profiles reflecting the state of national economic operation, social governance structure and industrial layout characteristics in the process of cross-border aggregation, correlation analysis and algorithm mining. This goes beyond the scope of personal information protection and affects national security [10, 11]. In 2021, DiDi Chuxing was banned from listing in the United States because its user data processing activities had a serious impact on national security. This case reflects the close link between massive cross-border data flows and national security [12].

The development of generative artificial intelligence has further amplified the data security risks of outbound investment in the digital industry. Generative AI systems rely heavily on massive amounts of data for training, optimization and iteration, and their training data usually comes from a wide range of sources covering multiple key fields such as scientific research, finance, healthcare, transportation, energy and public administration. When relevant enterprises build AI R&D centers, computing platforms or model training bases through overseas investment, large-scale cross-border aggregation and centralized processing of data will significantly increase the risks of sensitive data leakage, abuse and illegal acquisition. At the same time, since training data itself may contain sensitive information, and AI models have the ability to integrate, correlate and reconstruct

information from different sources during inference, the generated content may involve geographic information of important targets, operation status of critical infrastructure, financial security information and even national defense security information, thus forming new sources of security risks. Furthermore, core elements such as AI model parameters, training datasets and algorithm architectures have become important strategic assets in national scientific and technological competition. If they are stolen, leaked or obtained by competitors in the process of overseas investment, it may even weaken China's technological advantages and strategic initiative in the field of artificial intelligence [13].

2.2. Technological security risks

The development of the digital economy depends heavily on core technological innovation capacity, so outbound investment in the digital industry is often accompanied by cross-border transfer of key technologies. Many core technologies in the digital industry have obvious dual-use attributes and are an important foundation of national strength. For example, key technologies such as semiconductors, artificial intelligence, quantum information and high-performance computing are widely used in national defense development, military equipment research and development, and cyberspace security protection [14].

Compared with traditional industries, the core of the digital industry is more reflected in intangible knowledge assets such as algorithm models, source codes, data resources and R&D experience. Such technical assets have the characteristics of low replication cost, fast dissemination speed and concealed transfer methods, and are more likely to spread through channels such as personnel mobility, joint R&D, technical cooperation and supply chain collaboration [14]. When enterprises carry out technical cooperation, joint R&D, construction of overseas R&D centers and technology licensing through overseas investment, relevant technical knowledge, R&D achievements and innovation capabilities may spread overseas accordingly, and even be used to enhance other countries' military capabilities, intelligence capabilities or cyber attack and defense capabilities, thus having potential impacts on national security.

In addition, against the background of increasingly fierce global scientific and technological competition, the diffusion of key technologies has gone beyond the scope of pure commercial competition and gradually become an important part of strategic competition among countries. The formation of alternative innovations overseas or the mastery of key technological capabilities by competitors may also lead to the loss of competitive advantages of China's emerging industries.

2.3. Critical information infrastructure security risks

Outbound investment in the digital industry may also affect the security of critical information infrastructure. According to the *Regulations on the Security Protection of Critical Information Infrastructure*, critical information infrastructure covers important network facilities and information systems in key industries and fields such as public communication and information services, energy, transportation, finance, public services, e-government and national defense science and technology industry. Its stable operation is directly related to national security, the national economy and people's livelihood, and public interests.

With the development of the digital economy, digital infrastructure such as data centers, cloud computing platforms and AI computing facilities have gradually become an important part of critical information infrastructure, and play a fundamental supporting role in the country's economic and social operation. Some outbound investments in the digital industry involve the construction of

overseas data centers, deployment of communication networks and operation of digital infrastructure. During their overseas operation, relevant facilities may be subject to foreign government regulation, intelligence agency infiltration or cyber attacks, creating new security risks [15].

In addition, the digital infrastructure network formed by overseas investment often undertakes important functions such as cross-border data transmission, information exchange and collaborative operation of key businesses, and has gradually become an important node connecting domestic and overseas digital systems. Once relevant facilities are controlled, interfered, damaged or continuously monitored, security risks may be transmitted to the domestic side along the digital network [16]. In the Micron incident in 2023, the Cyberspace Administration of China concluded through cybersecurity review that products of the US company Micron posed major security risks to China's critical information infrastructure supply chain, and therefore prohibited operators of critical information infrastructure from purchasing its related products. This shows that the security of digital technology products and their supply chains has become an important part of critical information infrastructure security [17].

Overall, the national security risks triggered by outbound investment in the digital industry have broken through the traditional analytical framework of outbound investment that mainly focuses on capital security and industrial security, and present characteristics of concealment, persistence, dynamism and diffusion. Data, technology and digital infrastructure are intertwined and interact with each other, enabling relevant risks to spread and amplify across different fields. Therefore, it is necessary to build a national security governance system for outbound investment adapted to the development characteristics of the digital industry, and effectively embed national security considerations into the governance framework of outbound investment in the digital industry, so as to achieve a balanced coordination between high-level opening-up and national security protection.

3. Current institutional situation of national security governance for outbound investment in the digital industry

China has not established a national security governance system specifically for outbound investment in the digital industry, but has formed a governance framework composed of outbound investment management systems and regulatory systems in related fields. Among them, the outbound investment management system takes approval and filing administration and the information reporting mechanism as the core, realizes ex-ante control over some sensitive investment activities through investment exit management, and strengthens in-process and ex-post supervision over investment operation through the information reporting mechanism. Regulatory systems in related fields regulate specific behaviors in digital industry investment through rules on cybersecurity, data security, personal information protection and export control. It is worth noting that the *Outbound Investment Regulations*, which came into force on July 1, 2026, explicitly proposed the establishment of an outbound investment security review mechanism at the administrative regulation level for the first time, laying a normative foundation for the construction of China's national security review system for outbound investment. As a result, China's national security governance system for outbound investment in the digital industry has initially taken shape: based on approval and filing administration, supplemented by the information reporting mechanism, oriented toward the development of outbound investment security review, and supported by regulatory systems in related fields.

3.1. Approval and filing administration

The current overseas investment management system generally follows a basic structure with filing as the principle and approval as the exception. For investment projects within the approval scope, investors shall submit applications to the competent authorities in advance. If the competent authorities find after review that the relevant investment may harm national sovereignty, security or public interests, they have the right to refuse approval. For projects not within the approval scope, filing administration is implemented in principle. Unlike approval procedures that focus on substantive review, filing administration mainly revolves around matters such as the qualification of investment entities, the authenticity of investment and compliance with national outbound investment policy guidelines, and is dominated by formal review.

At present, the competent authorities for the approval and filing of China's outbound investment are characterized by horizontal multi-department coordination and vertical multi-level division of labor. Horizontally, the *Measures for the Administration of Overseas Investment* issued by the Ministry of Commerce and the *Measures for the Administration of Enterprise Overseas Investment* issued by the National Development and Reform Commission (hereinafter referred to as the NDRC) jointly form the basic framework for overseas investment exit management, and implement exit regulation on overseas investment from the perspectives of commercial administration and investment management respectively [18]. To strengthen inter-departmental information sharing and regulatory coordination, the Ministry of Commerce, the NDRC, the People's Bank of China and the State-owned Assets Supervision and Administration Commission of the State Council (hereinafter referred to as the SASAC) jointly issued the *Interim Measures for the Filing (Approval) Report of Outbound Investment* (hereinafter referred to as the *Interim Measures*) in 2018, attempting to build an approval and filing mechanism with the Ministry of Commerce leading information aggregation and relevant departments performing their duties and cooperating. Nevertheless, the two sets of administrative measures still operate separately at present, and a unified management system has not yet been formed.

Vertically, both sets of measures adopt a hierarchical management model at the central and local levels. The Ministry of Commerce is responsible for the approval and filing of overseas investment projects of central enterprises, and provincial commercial departments are responsible for those of local enterprises. The NDRC is responsible for the approval and filing administration of projects with a single investment amount exceeding 300 million US dollars, and the rest of the projects are in principle handled by provincial development and reform departments. In addition, the State Administration of Foreign Exchange, the People's Bank of China, the Ministry of Finance and the SASAC also undertake supporting responsibilities such as cross-border capital flow management, foreign exchange administration, fiscal fund supervision and supervision of state-owned assets overseas, jointly forming a regulatory system covering all aspects of outbound investment.

The scope of approval administration specified in the two sets of measures also differs. The *Measures for the Administration of Overseas Investment* stipulates that industries subject to approval administration include those involving products and technologies restricted from export by China and those affecting the interests of more than one country or region. This shows that there is a strong correlation between China's overseas investment administration and the export control system. According to rules such as the *Export Control List of Dual-Use Items* and the *Catalogue of Technologies Prohibited or Restricted from Export by China*, technologies and products under restricted export administration cover a wide range of fields such as electronic information, computers, artificial intelligence, integrated circuits, communication networks and spatial data

processing. These fields highly overlap with digital product manufacturing, digital technology application and digital infrastructure industries, and basically cover the key technologies, core equipment and infrastructure of the digital industry. Therefore, behaviors such as technology export, overseas R&D, technology licensing and cross-border technical cooperation in digital industry investment activities have a high probability of falling into the scope of approval administration in practice.

In contrast, the scope of industries subject to approval administration in the *Measures for the Administration of Enterprise Overseas Investment* is relatively limited, mainly covering fields such as research, production and maintenance of weapons and equipment, development and utilization of cross-border water resources, and news media. Later, the supporting rule issued by the NDRC, the *Catalogue of Sensitive Industries for Overseas Investment* (hereinafter referred to as the *Sensitive Industry Catalogue*), added industries such as real estate, hotels, cinemas, entertainment and sports clubs. This catalogue was formed before the full rise of the digital economy. It mainly focuses on traditional national security risks and irrational investment risks, and lacks direct response to digital industry investment activities. Nevertheless, some digital economy formats may still fall into the approval scope due to overlapping business attributes with existing sensitive industries. For example, when digital content platforms, online game companies or streaming platforms carry out investment activities overseas, if their main business involves news and information dissemination, public opinion guidance or digital media operation, they may be classified as sensitive industries due to substantial connection with the news media sector. When domestic Internet enterprises obtain control of overseas online audio-visual platforms through overseas mergers and acquisitions, the relevant investment activities may also trigger approval procedures.

3.2. Information reporting mechanism

In addition to approval and filing procedures at the investment exit stage, China also implements continuous supervision over overseas investment projects through an information reporting mechanism. The *Measures for the Administration of Overseas Investment* requires investment entities to submit statistical data and operational information in accordance with regulations, and bear responsibility for the authenticity of investment activities. In case of major events such as termination of investment or transfer of equity in overseas enterprises, they shall also fulfill reporting obligations in a timely manner. The *Measures for the Administration of Enterprise Overseas Investment* requires investment entities to continuously report project implementation progress, major adverse events and project completion.

The information reporting mechanism has special significance in the national security governance of outbound investment in the digital industry. As mentioned above, the national security risks of outbound investment in the digital industry are persistent, dynamic and diffusive. They may not fully appear at the investment establishment stage, but gradually form and spread during operation. Since the information available to competent authorities at the investment exit stage is relatively limited, it is difficult to accurately identify potential national security impacts in the future solely by relying on ex-ante review [19]. For example, after domestic enterprises obtain control of a digital platform through overseas investment, with the expansion of user scale, continuous aggregation of data resources and continuous iteration of algorithm models, the investment may gradually involve issues such as large-scale personal information processing, cross-border data flow and accumulation of AI training data. The degree of its impact on national security may significantly exceed expectations at the time of investment establishment.

In summary, the information reporting system not only undertakes the functions of statistical management and administrative supervision, but also serves as an important tool for national security risk identification and dynamic assessment. By requiring investment entities to disclose project operation, changes in major events, reinvestment and investment exit, competent authorities can keep track of the development and changes of investment projects in a timely manner and take targeted regulatory measures according to risk evolution.

3.3. Outbound investment security review

The *Outbound Investment Regulations* proposes the establishment of an outbound investment security review system at the administrative regulation level, which conducts security review in accordance with the law on overseas investments that affect or may affect national security, as well as activities such as the transfer and disposal of related assets and equity. This regulation marks that China has formally incorporated national security review into the outbound investment governance system.

Compared with the traditional approval and filing system, outbound investment security review places more emphasis on the function of national security risk identification and prevention. In terms of regulatory scope, the review covers not only investment establishment acts, but also asset and equity disposal acts after investment is formed, indicating that the review is not limited to the investment exit stage, but may run through the entire process of investment activities [20]. For the digital industry, this means that competent authorities can take timely measures in the future against new national security risks arising during investment operation, such as cross-border data flow, key technology transfer and digital infrastructure operation, reserving institutional space for dynamic security governance of outbound investment in the digital industry.

In recent years, with the rapid development of digital technology and intensifying competition in digital technologies, major economies around the world have paid close attention to the national security risks that may arise from outbound investment in the digital industry. Major economies such as the United States, the United Kingdom and the European Union have all started to focus on such risks and have gradually established or are studying corresponding institutional arrangements. The review focuses mainly on key technology fields such as semiconductors, artificial intelligence and quantum technology. Its core goal is to prevent capital, technology and management resources from promoting the development of military, intelligence and cyber capabilities of potential competitors through outbound investment activities [21-24]. International trends show that national security review has gradually extended from traditional foreign investment supervision to outbound investment supervision, with digital technology, data resources and key technological capabilities as key concerns.

However, at present, the *Outbound Investment Regulations* only establishes the principle framework of the outbound investment security review system. Issues such as the specific setup of review bodies, the triggering conditions of review procedures and the criteria for identifying national security risks have not yet been clearly defined, and need to be detailed and improved through subsequent special legislation.

3.4. Regulation in related fields

In addition to the special outbound investment management system, systems such as cybersecurity, data security, personal information protection and export control also play an important role in national security governance for outbound investment in the digital industry. Investors' overseas

investment activities can be divided into three stages: the investment exit stage, the investment operation stage and the investment exit stage [25]. Relevant data governance rules cover the entire life cycle of outbound investment in the digital industry and constitute an important part of its national security governance system.

At the investment exit stage, investors usually need to identify, evaluate and integrate the data resources, user information and technical assets of domestic and overseas enterprises in the process of investment decision-making, due diligence and transaction arrangement. At this stage, the data classification and grading protection system, data security risk assessment system and personal information protection rules established by the *Cybersecurity Law*, the *Data Security Law* and the *Personal Information Protection Law* have already begun to play a restrictive role. In the investment operation stage, investors and target enterprises need to frequently carry out domestic and overseas data sharing, cross-border retrieval and centralized processing. For such cross-border data flows, China has formed a regulatory system composed of the *Measures for Security Assessment of Data Outbound*, the *Measures for Standard Contracts for Personal Information Outbound* and the *Provisions on Promoting and Regulating Cross-Border Data Flows*. At the investment exit stage, when digital industry investors sell data centers or divest digital businesses, relevant digital assets may be transferred along with the transaction. In this process, activities involving important data, core data or large-scale personal information still need to comply with data security administration and personal information protection requirements. In addition, the security protection obligations imposed on operators of critical information infrastructure by the *Regulations on the Security Protection of Critical Information Infrastructure* may also restrict the transfer and disposal of assets related to digital infrastructure.

Overall, the current system has built a comprehensive regulatory network through multiple rules such as overseas investment administration, data security governance and cybersecurity protection, gradually embedding national security into all links of outbound investment activities in the digital industry. However, regulatory systems in related fields mainly regulate specific behaviors such as data processing, network operation and technology flow. Their function is to make up for the deficiencies of the special outbound investment management system, but they cannot replace the outbound investment management system itself. Therefore, the improvement of national security governance for outbound investment in the digital industry still depends on further optimization of the internal structure of the outbound investment management system and effective connection between various systems.

4. Institutional deficiencies of national security governance for outbound investment in the digital industry

Although China has formed a relatively comprehensive national security governance system for outbound investment in the digital industry, the current system still cannot fully respond to the new demands of the digital economy era. In general, the deficiencies of the current system are mainly reflected in two aspects. First, there is insufficient internal coordination in the national security governance system for outbound investment, and the functional positioning and procedural connection between relevant systems have not been clarified. Second, the current scope of approval administration has low adaptability to outbound investment in the digital industry, with both normative imbalance and lagging rule updates.

4.1. Insufficient coordination of the governance system

At present, China's outbound investment management system faces prominent coordination dilemmas. On the one hand, the current approval and filing system has long suffered from overlapping functions and repeated procedures caused by fragmented management. On the other hand, the relationship between the newly established outbound investment security review system and the existing approval and filing system and information reporting system has not been clarified, which may aggravate procedural connection obstacles within the institutional system.

First, the parallel management model of the Ministry of Commerce and the NDRC has, to a certain extent, caused repeated operation of approval and filing procedures. Although the two departments have different focuses in institutional design—the former is mainly responsible for managing new overseas investment projects, and the latter focuses on risk control of investment projects in sensitive countries, regions and industries—in practice, their management scopes inevitably overlap to a large extent, and the resulting coordination costs keep rising [26]. The current system has not yet established a unified acceptance platform, review platform and information sharing mechanism. Investment entities often need to submit similar application materials to different competent authorities for the same investment matter and accept parallel review [26]. At the same time, the hierarchical management standards within the two departments are also inconsistent, resulting in the same project possibly facing repeated supervision by different departments and authorities at different levels. For example, when a local enterprise carries out overseas investment with a single investment amount exceeding 300 million US dollars, it needs to go through corresponding procedures with the provincial commercial authority and also file an application with the National Development and Reform Commission [27].

The cumbersome institutional arrangements not only increase the compliance costs of enterprises, but also reduce the efficiency of administrative resource allocation. National security risk identification essentially relies on information integration and comprehensive judgment, while the fragmented management pattern easily leads to regulatory information scattered among different departments, increasing coordination costs in the risk identification process. Especially in the digital industry, investment activities usually involve multiple factors such as data resources, key technologies and digital infrastructure at the same time, and their impact on national security is highly comprehensive and cross-cutting. If relevant information is scattered among different competent authorities, it will be difficult to form unified standards and overall judgments for national security risk assessment, thus affecting governance effectiveness.

Second, the *Outbound Investment Regulations* does not clarify the relationship between the outbound investment security review system and the current approval and filing and information reporting systems, giving rise to new problems of institutional connection. Specifically, it remains unclear whether security review should serve as a review link in the approval procedure or operate as a special procedure independent of the approval and filing process; whether investment projects that have completed approval or filing may still be subject to security review; how security review for asset transfer and equity disposal connects with the information reporting mechanism in the operation stage; and how to realize case transfer, risk early warning and information sharing among different competent authorities. None of these issues have been clearly addressed by current norms.

The uncertainty in institutional positioning and connection may not only cause procedural duplication, but also lead to regulatory gaps. On the one hand, some investment projects have already undergone substantive review involving national security factors at the approval stage, but due to the lack of clear procedural division of labor, they may still be repeatedly included in the

security review procedure later, increasing the compliance burden of enterprises and reducing administrative efficiency. On the other hand, national security risks in the digital economy often evolve dynamically. For projects that are not within the approval scope but gradually generate national security risks during investment implementation and operation, if there is a lack of effective risk monitoring and procedural connection mechanisms, relevant risks may remain outside the regulatory system [28]. Therefore, it is necessary to further clarify the functional positioning and procedural relationship between approval and filing, information reporting and security review systems, and build a well-structured and coherently connected governance system for outbound investment in the digital industry.

4.2. Insufficient adaptability of the approval scope

In the current system, the design of the approval administration scope cannot effectively address the national security risks in outbound investment in the digital industry. The current *Measures for the Administration of Overseas Investment* and *Measures for the Administration of Enterprise Overseas Investment* have respectively defined different industries for approval administration. The former is based on export control rules and has the problem of over-generalized approval administration; the latter still centers on the classification of traditional sensitive industries, showing problems of narrow coverage and insufficient response to the digital economy. In addition, the current approval industry identification rules lack sufficient adaptability to the new technologies, new formats and new business models that continue to emerge in the development of the digital economy, and are prone to creating new regulatory gaps.

4.2.1. Normative imbalance of approval-administered industries

As mentioned above, the *Measures for the Administration of Overseas Investment* directly borrows relevant rules of the export control system when determining the scope of approved industries. However, although both the export control system and the outbound investment approval system take safeguarding national security as an important goal, they differ significantly in regulatory objects, intervention methods and institutional functions, so their regulatory scopes should not be exactly the same [29].

The export control system mainly targets the cross-border transfer of goods, technologies and services, and regulates specific products or technologies themselves. Although relevant restrictive measures may affect specific transactions, they usually do not directly affect the overall industrial layout and internationalization strategy of enterprises [30]. In contrast, the outbound investment management system directly acts on investment activities themselves, which concerns enterprises' access to overseas markets, resource allocation and global operation layout, and has a more far-reaching impact on business operations. For this reason, the export control system can establish a relatively broad regulatory system around controlled items, while the outbound investment approval system should focus on investment activities with higher national security risks and leave lower-risk investment matters to filing procedures, so as to achieve a balance between national security protection and investment freedom [31].

The direct introduction of export control rules into the approval scope by the *Measures for the Administration of Overseas Investment* easily leads to over-generalized approval administration in the digital industry. The digital industry is highly technology-intensive, and fields such as artificial intelligence, integrated circuits, communication networks, cloud computing and data processing are all related to the export control system to varying degrees. Even if the relevant investment itself is

not accompanied by the actual export of controlled products or technologies, it may still be included in the approval scope simply because its industry involves export-restricted technologies. As a result, the basis for applying approval administration has gradually shifted from national security risk identification to technical relevance judgment, turning the key supervision that should target high-risk investments into broad coverage based on technical attributes. Although the regulatory model that replaces substantive risk judgment with technical relevance helps reduce regulatory loopholes, it also increases the institutional transaction costs of enterprises and may dampen their enthusiasm for international technical cooperation and global resource allocation. In addition, for investment projects that also involve technology export, investment entities still need to apply for export licenses in accordance with export control rules after going through approval procedures, thus being subject to the dual constraints of approval administration and export control. The lack of effective distinction between the two systems in scope easily causes procedural overlap and regulatory duplication, further increasing the compliance burden of enterprises.

In sharp contrast, the *Measures for the Administration of Enterprise Overseas Investment* has significantly insufficient coverage of outbound investment in the digital industry. This measure and its supporting *Sensitive Industry Catalogue* were formulated before the full rise of the digital economy. Its risk identification mainly revolves around traditional security fields such as national defense security, resource security and ideological security, and does not take the digital industry and its related data security, technological security and digital infrastructure security as independent considerations. As the digital economy has gradually become an important part of national competitiveness, traditional industry classifications can no longer fully reflect the national security impacts that may arise from digital industry investment activities.

Against this background, investment in the digital industry is not only subject to dual administration by commercial departments and development and reform departments, but also faces different procedural arrangements for the same project due to the obvious differences in the approval scopes of the two departments. For example, when an integrated circuit design enterprise makes overseas investment, it may be subject to approval procedures according to the *Measures for the Administration of Overseas Investment* because it involves export-restricted technologies, but only needs to fulfill filing obligations according to the *Measures for the Administration of Enterprise Overseas Investment*. Therefore, the problem of the current approval scope is not simply excessive regulation or insufficient supervision, but a structural imbalance of both over-broad and over-narrow scope across different systems. Over-reliance on export control logic has led to some digital industry investments being improperly included in the approval scope of the Ministry of Commerce, while following traditional sensitive industry classifications has left some digital industry investments with high national security risks outside the approval system of the NDRC. Together, these two factors make it difficult for the current system to accurately identify national security risks in the digital industry, and also lead to waste of administrative resources and increased institutional operation costs.

4.2.2. Lagging rules for the approval scope

In addition to normative imbalance, the current rules for the approval scope also face obvious lag problems. As mentioned above, the *Measures for the Administration of Enterprise Overseas Investment* and its supporting *Sensitive Industry Catalogue* mainly rely on industry classification to identify national security risks and determine the approval scope by enumerating specific industries. This method had strong certainty and operability in the era of traditional industries. However, national security risks in the digital economy era often do not attach to a specific industry, but

manifest as cross-industry and cross-field new risks such as transfer of data control rights, spillover of key technologies, deployment of digital infrastructure and diffusion of algorithm capabilities [32]. Therefore, industry classification can no longer accurately reflect the real risk structure of digital industry investment activities, and the method of identifying national security risks solely by industry cannot adapt to the trend of cross-field diffusion of national security risks in the digital economy context.

In comparison, the *Measures for the Administration of Overseas Investment* does not completely rely on industry classification, but takes products and technologies as risk identification elements, breaking through the limitations of traditional regulation and having greater flexibility. When the export control catalogue is adjusted, the relevant approval scope can also change accordingly, thus enhancing the system's ability to respond to emerging risks to a certain extent. However, this flexibility is still essentially based on the premise that the export control system can identify national security risks in a timely and accurate manner. In fact, the export control system also faces the practical dilemma that rule updates lag behind technological development. Due to the highly dynamic nature of technological innovation, there is often a long time lag for emerging technologies from R&D breakthroughs and commercial application to being included in the control catalogue, and this problem is particularly prominent in the digital economy. Therefore, even taking products and technologies as the basis for risk identification, it is difficult to completely overcome the institutional limitations caused by the faster evolution of risks than rule updates [31].

Essentially, both the traditional identification model based on industry classification and the catalogue management model centered on controlled technologies are static regulatory tools based on existing risk cognition. National security risks in the digital economy era are highly dynamic, cross-field and diffusive, and the evolution of risk forms is often faster than institutional adjustment. When risk identification rules cannot respond to technological innovation and business model changes in a timely manner, the risk detection capability of the system will gradually weaken. Some outbound investments in the digital industry with high national security sensitivity may remain outside the current approval administration system, thus forming new regulatory gaps. Therefore, it is necessary to establish a more flexible and forward-looking risk identification mechanism to meet the national security governance needs brought by the development of the digital economy and changes in the international competition pattern.

5. Institutional Improvement of national security governance for outbound investment in the digital industry

In response to the aforementioned institutional deficiencies, the improvement of national security governance for outbound investment in the digital industry should be carried out from two aspects: the overall coordination of the outbound investment management system and the institutional adaptability to the special risks of the digital industry. On the one hand, optimize the allocation of powers and duties of competent authorities in the approval and filing system, and clarify the relationship between the existing outbound investment management system and the outbound investment security review system. On the other hand, according to the particularity of national security risks in the digital industry, define the scope of approval administration and security review, and establish a tiered management system based on risk identification.

5.1. Coordination of the outbound investment security governance system

5.1.1. Clarify the boundaries of powers and duties of approval and filing authorities

As mentioned above, although the *Interim Measures* has initially established a cross-departmental collaboration and information sharing mechanism, the current approval and filing system has not yet formed a unified acceptance platform, review platform and collaborative decision-making mechanism. Therefore, it is necessary to adjust the power allocation of approval and filing authorities and promote the establishment of a coordinated and efficient outbound investment regulatory system. There are two main reform paths for the power allocation of approval and filing authorities: first, integrate the existing two sets of approval and filing management systems and vest management authority in a single competent authority; second, retain the existing dual-department management framework, clarify the responsibility boundaries of different departments, and avoid overlapping powers and repeated reviews as much as possible [26].

From the perspective of comparative law practice, countries that implement outbound investment examination and approval or approval administration tend to adopt a relatively centralized management model. For example, South Korea concentrates the functions of enterprise outbound investment declaration and approval on the Bank of Korea and its authorized institutions. Although the US outbound investment security review mechanism emphasizes the collaborative participation of multiple departments, the acceptance of investment declarations, initiation of procedures and implementation of final investment restriction measures are all centralized in the Secretary of the Treasury [22, 33]. A unified examination and approval mechanism helps form stable and consistent review standards, improve administrative efficiency, and reduce the institutional transaction costs of investment entities caused by multiple declarations [34].

However, it can be inferred from Article 27 of the *Outbound Investment Regulations* that it does not adopt a single competent authority model, but continues the institutional structure of joint administration by commercial departments and development and reform departments. This article stipulates that for outbound investment activities prohibited by the state, the NDRC and the Ministry of Commerce shall order the suspension of implementation "in accordance with the division of responsibilities", still granting law enforcement functions of outbound investment administration to both departments. Furthermore, Article 15 stipulates that outbound investment security review "shall be jointly implemented by the competent investment department and the competent commercial department of the State Council together with other relevant departments of the State Council", incorporating the newly established outbound investment security review function into the dual-department management framework as well. It can be seen that under the current institutional system, the possibility of building a single-authority management model is relatively limited.

Against this background, a more feasible reform path is to clarify the responsibility boundaries of different departments through a unified institutional framework. Article 72 of the *Legislation Law* stipulates that for matters involving the scope of functions and powers of more than two departments of the State Council, administrative regulations may be formulated by the State Council, or rules may be jointly formulated by relevant departments. Accordingly, to clarify the division of responsibilities between development and reform departments and commercial departments in outbound investment administration, the existing *Measures for the Administration of Overseas Investment* and *Measures for the Administration of Enterprise Overseas Investment* should be integrated as a whole to build a unified approval and filing system framework. Within this framework, specific powers should be reasonably allocated according to the functional positioning of the two departments, so as to reduce regulatory overlap and overlapping responsibilities at the

institutional level [27]. From the perspective of facilitating enterprise compliance, a unified working mechanism can be established with reference to the foreign investment security review procedure. Alternatively, a unified platform can be responsible for accepting investment project declarations and collecting information, and then determine the specific competent authority according to the main types of risks involved in the project. For example, for investment projects mainly involving cross-border data flow and digital service export, the commercial department shall be responsible for review; for investment projects involving major digital infrastructure construction or strategic resource allocation, the development and reform department shall be responsible for review; for digital industry investment projects involving multiple national security risks at the same time, a joint review mechanism can be established, with relevant competent departments participating in review and decision-making together.

On the basis of clear horizontal responsibility boundaries, some problems of overlapping powers and hierarchical dislocation caused by vertical multi-level administration can also be effectively alleviated. Since the power allocation of authorities at different levels will be based on unified rules and clear division of labor, the situation where the same investment project applies different review standards or is repeatedly reviewed by authorities at different levels will be significantly reduced. Therefore, retaining the hierarchical division of labor between central and local, national and provincial authorities under the unified institutional framework will not weaken regulatory coordination, but will help balance regulatory efficiency and administrative resource allocation, and realize the overall optimization of the outbound investment management system [35].

5.1.2. Build a tiered management framework for outbound investment

To clarify the relationship between the approval and filing system, the information reporting system and the outbound investment security review system, it is first necessary to determine whether the newly established outbound investment security review system will replace some functions of the existing systems. In fact, the three differ significantly in scope of application, stage of action and institutional function. The approval and filing system mainly acts at the investment exit stage and conducts ex-ante administration of overseas investment activities. The information reporting system covers the investment operation and exit stages and realizes dynamic supervision through continuous information submission. The outbound investment security review system takes national security risks as the core review object, and its scope of application is not limited to before investment implementation, but runs through the entire life cycle of investment activities. It can be seen that the approval and filing system and the information reporting system mainly undertake normalized regulatory functions, while the outbound investment security review system aims to implement key control over specific investment activities that may affect national security. The three are not mutually substitutive, but should jointly form a well-structured and functionally complementary outbound investment management system.

On this basis, it is necessary to further clarify the division of labor and connection mechanism among the three systems. In this regard, reference can be made to China's foreign investment management system. In the field of foreign investment, the security review system only applies to investment activities in specific fields and with specific investment methods, thus realizing effective division of labor with the general access management system. Comparative law practice also shows that outbound investment security review is usually positioned as a special review mechanism above general investment management procedures, and only applies to investment activities with high national security risks. For example, the US outbound investment security review system only

applies to investment activities in fields such as advanced semiconductors, artificial intelligence and quantum information technology [22].

Based on this, the construction of the outbound investment security review system should adopt a tiered management approach, allocating differentiated regulatory measures according to the degree of national security risks that investment activities may generate. For general overseas investment projects, in principle, the whole process of supervision shall be realized through the filing and information reporting system. For investment projects with certain national security sensitivity, they can be included in the approval scope, supplemented by continuous information reporting obligations. For major investment projects that may affect national security, the security review procedure shall be initiated before investment implementation. At the same time, since the *Outbound Investment Regulations* extends the objects of security review to activities such as asset and equity disposal after investment implementation, the information reporting system can also form a linkage with outbound investment security review and become an important risk identification mechanism for security review. In the future, China can try to establish a procedural connection between information reporting and security review. When investment entities report major matters that may affect national security, such as major technology transfer and cross-border flow of important data, the competent authorities can initiate the security review procedure in a timely manner, so as to realize precise governance and dynamic control of national security risks in outbound investment in the digital industry.

5.2. Definition of the tiered management scope for the digital industry

On the basis of the aforementioned tiered management framework, it is necessary to respond to the special regulatory needs of outbound investment in the digital industry and improve the adaptability of outbound investment approval administration and security review systems to the digital industry. To this end, it should first be clarified that according to the *Outbound Investment Regulations*, safeguarding national security undoubtedly constitutes the core goal of national security governance for outbound investment in the digital industry, but promoting the high-quality development of outbound investment in the digital industry is also an important value that needs to be balanced. Therefore, the administration of outbound investment in the digital industry should seek a reasonable balance between security protection and development promotion, avoiding both uncontrolled national security risks and unnecessary restrictions on the international development of enterprises caused by excessive regulation.

After clarifying the value objectives, it is necessary to further delineate the scope of classified administration of outbound investment in the digital industry, and clarify which investment activities are suitable for filing administration, which should be included in approval administration, and which should be subject to security review. As mentioned above, using traditional industry classification as the basis for delineating the scope of approval and security review cannot adapt to the new national security risks generated by the digital economy. The idea of the *Measures for the Administration of Overseas Investment* taking products and technologies as the basis for delineating the approval scope has certain rationality. However, there is still room for improvement in this approach. On the one hand, the expression "involving products and technologies restricted from export" is too broad. A large number of digital industry investments that do not have significant national security risks may also be included in the approval scope, thereby increasing enterprise compliance costs and dampening the enthusiasm of enterprises for international technical cooperation and global resource allocation. On the other hand, relying solely on technical elements for identification cannot fully reflect the multi-dimensional national security risks that may arise

from digital industry investment, such as data security, infrastructure security and control transfer. Therefore, future institutional reform should not only appropriately narrow the current approval scope, but also introduce more risk identification elements to improve the matching degree between regulatory measures and national security risks.

In recent years, the exploration of outbound investment security review systems by the United States and the European Union shows that key technologies have become an important entry point for national security governance in the digital economy era. Whether the United States focuses on regulating investment in advanced semiconductors, artificial intelligence and quantum information technology, or the European Union focuses on the risks of technology leakage and outflow of key capabilities, their common feature is to establish a classified management system around strategically significant key technologies [36]. Given that the national security risks faced by China's outbound investment in the digital industry have certain commonalities with those of the United States and the European Union, China can learn from their institutional experience in the future and gradually build a classified management system centered on key digital technologies [6]. At the security review level, a key technology list can be established to include technical fields with major strategic value and security impact, such as advanced semiconductors, artificial intelligence and quantum information technology, into the key review scope. At the approval administration level, a sensitive technology list with a wider coverage can be established to include technical fields that may involve technology diffusion but have not yet reached the level of major national security risks into the approval scope.

In addition, national security risks in the digital industry do not entirely come from technology itself, but may also arise from factors such as data control rights, infrastructure control rights and the allocation of key digital resources. Therefore, the delineation of the future management scope should not take technology as the sole standard, but should also draw on the experience of the foreign investment security review system to establish a diversified risk identification system. The *Measures for the Security Review of Foreign Investment* not only includes investment involving key technologies into the review scope, but also includes fields such as important agricultural products, important energy and resources, major equipment manufacturing and important infrastructure into the regulatory scope, and carries out risk identification around key elements of national security [37]. For outbound investment in the digital industry, fields such as important data, large-scale personal information and critical information infrastructure are also of great national security significance. In the future, the above elements can be included in the consideration factors for delineating the management scope, and a multi-dimensional identification mechanism can be formed in combination with the technology list system, so as to build an outbound investment management system more in line with the development characteristics of the digital economy.

However, it should be acknowledged that the tiered management system formulated based on multi-dimensional elements is still based on existing risk cognition, while emerging technologies, new digital services and new business models continue to emerge, and the forms of national security risks are also constantly changing. If the management scope completely relies on enumerative provisions, institutional adjustment often lags behind the emergence of risks, thus forming regulatory gaps. Therefore, a dynamic adjustment mechanism should be established to authorize competent authorities to regularly revise the key technology list, sensitive technology catalogue and relevant supporting rules according to changes in the national security situation, technological development trends and industrial competition patterns, so as to improve the system's ability to respond to emerging risks. At the same time, open catch-all provisions should be set up as institutional supplements. Drawing on the experience of the foreign investment security review

system, the standard of "affecting or may affect national security" established by the *Outbound Investment Regulations* can be used as the triggering condition for security review. For investment activities that are not included in the relevant list but involve the transfer of control of important data, deployment of key digital infrastructure, diffusion of core algorithm capabilities or other activities that may affect national security, the competent authorities still have the right to initiate approval procedures or security review procedures in accordance with the law. Of course, to avoid excessive expansion of regulatory boundaries caused by open provisions, their application conditions, initiation procedures and review standards should still be clarified through special legislation, and necessary procedural constraints and relief mechanisms should be established. While enhancing institutional adaptability, it is necessary to ensure the reasonable expectations of investment entities for regulatory behaviors and realize the coordination and unity between national security governance and the principle of the rule of law [38].

6. Conclusion

The global expansion of the digital economy is reshaping the operational logic of international investment activities and constantly expanding the boundaries of national security governance. As data, technology, algorithms and digital infrastructure have gradually become important strategic resources in international competition, outbound investment in the digital industry has evolved from a simple capital export activity to a composite behavior with both economic interests and national security interests. The national security risks triggered by outbound investment in the digital industry are more concealed, dynamic and spillover-prone. The traditional outbound investment management model centered on capital flow and industrial layout can no longer fully respond to the new requirements of national security governance in the digital economy era.

In recent years, China has gradually built a national security governance mechanism for outbound investment in the digital industry, with the outbound investment management system as the core and supplemented by regulation in related fields such as data security and cybersecurity. However, with the accelerated evolution of digital technology innovation and the international competition pattern, the current system faces great challenges in coordination and adaptability, which affects the effectiveness of national governance. The improvement of national security governance capacity depends not only on procedural coordination and optimized allocation of powers and duties, but also on risk identification and prevention mechanisms that conform to the laws of digital economy development, focusing on achieving precise matching between regulatory resources and national security risks.

At present, China is in the critical initial stage of the 15th Five-Year Plan period. The high-quality joint construction of the Belt and Road Initiative continues to deepen in the direction of digitalization and intelligence, and the construction of the Digital Silk Road keeps expanding the space for China's digital economy international cooperation [39]. Coordinating development and security under the guidance of the overall national security outlook has become an important value orientation for the governance of outbound investment in the digital industry [40]. Looking ahead, based on the degree of national security risks, we should promote filing administration, approval administration and security review to form a well-structured and orderly connected tiered governance system. At the same time, around the core elements of national security such as key digital technologies, important data and critical information infrastructure, we should build a dynamic, forward-looking and adaptable risk identification mechanism. By continuously improving the national security governance system for outbound investment in the digital industry, while safeguarding national security and development interests, we will better promote the digital industry

to participate in international division of labor and global resource allocation, and provide solid legal guarantee for the high-level opening-up of the digital economy, the construction of a higher-level open economic system and the advancement of Chinese-style modernization [41].

References

- [1] National Bureau of Statistics. (2021). Statistical classification of the digital economy and its core industries (Decree No. 33 of the National Bureau of Statistics). [Z].
- [2] Sarafanov, I. (2025, October 24). The value of the Digital Silk Road for win-win cooperation. *Economic Daily*, p. 11. [N].
- [3] Ministry of Commerce, National Bureau of Statistics, State Administration of Foreign Exchange. (2025). 2024 statistical bulletin of China's outward foreign direct investment [R].
- [4] UNCTAD. (2021). *Digital economy report 2021: Cross-border data flows and development* [R]. Geneva: United Nations.
- [5] Dai, X. (2025). New trends and challenges of global factor division of labor in the digital economy and China's new opening-up measures. *Tianjin Social Sciences*(5), 104-111. [J].
- [6] Chaisse, J. (2024). National security unbound: US investment screening from inbound to outbound. *Georgetown Journal of International Law*, 56, 461-465. [J].
- [7] OECD. (2022). *Cross-border data flows: Taking stock of key policies and initiatives*. Paris: OECD Publishing.
- [8] OECD, & WTO. (2025). *Economic implications of data regulation: Balancing openness and trust*. Paris: OECD Publishing.
- [9] United Nations General Assembly. (2015). *Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security* (A/70/174).
- [10] Xu, W., & Chen, K. (2025). Conflicts and responses between cross-border data flow and national data security governance: Taking the "US Congress passing the TikTok divestment act" as the entry point. *Wuhan University International Law Review*(3), 35-53.
- [11] Cheng, X. (2021). On the personal information processing rules in China's personal information protection law. *Tsinghua University Law Journal*(3), 55-73.
- [12] Cyberspace Administration of China. (2022, July 21). *Relevant person in charge of the Cyberspace Administration of China answers reporters' questions on the decision of imposing administrative penalties related to cybersecurity review on DiDi Global Inc. in accordance with the law*. https://www.cac.gov.cn/2022-07/21/c_1660021534364976.htm.
- [13] Jiang, H. (2024). On national security review of generative artificial intelligence applications. *Social Sciences in Yunnan*, (4), 72-79.
- [14] OECD. (2018). The digital economy, multinational enterprises and international investment policy. *OECD Business and Finance Policy Papers No. 46*. Paris: OECD Publishing.
- [15] OECD. (2019). Digital security and resilience in critical infrastructure and essential services. *OECD Digital Economy Papers No. 281*. Paris: OECD Publishing.
- [16] OECD. (2019). Good governance for critical infrastructure resilience. *OECD Reviews of Risk Management Policies*. Paris: OECD Publishing.
- [17] Cyberspace Administration of China. (2023, May 21). Products sold by Micron in China fail to pass cybersecurity review. *Cyberspace Administration of China*. https://www.cac.gov.cn/2023-05/21/c_1686348043518073.htm.
- [18] Erie, M. S., & Zhang, J. (2023). *A comparison of inbound and outbound investment regulatory regimes in China: Focus on environmental protection*. Cambridge University Press.
- [19] OECD. (2015). *Digital security risk management for economic and social prosperity: OECD recommendation and companion document*. Paris: OECD Publishing. <https://doi.org/10.1787/9789264245471-en>
- [20] Ministry of Justice. (2026, June 1). *Safeguarding outbound investment with institutional innovation and providing legal guarantee for higher-level opening-up*. Ministry of Justice. https://www.moj.gov.cn/pub/sfbgw/zcjd/202606/t20260601_535862.html
- [21] Executive Office of the President. (2023, August 9). *Executive order 14105—Addressing United States investments in certain national security technologies and products in countries of concern* (Executive Order No. 14105).
- [22] US Congress. (2025, December 18). *Comprehensive outbound investment national security act of 2025, in National Defense Authorization Act for Fiscal Year 2026* (Statute at Large 139 Stat. 718 - Public Law No. 119-60).
- [23] Reuters. (2024, April 18). *Britain to examine whether some outward investment undermines national security*. Reuters. <https://www.reuters.com/world/uk/britain-examine-whether-some-outward-investment-undermines->

national-security-2024-04-18/?utm_source=chatgpt.com

- [24] European Commission. (2025, January 15). *Commission recommendation (EU) 2025/63 of 15 January 2025 on reviewing outbound investments in technology areas critical for the economic security of the Union* (OJ L 2025/63, C/2025/39).
- [25] Han, L. (2018). *International investment law*. Beijing: Renmin University of China Press.
- [26] Du, J., & Ji, X. (2025). Assessing the outward foreign investment regulatory regime in China: A unified outward foreign investment law on the horizon? *Asia Pacific Law Review*, 33(1), 125–148.
- [27] Yu, J., & Chen, Z. (2013). A tentative discussion on the reform of China's overseas investment approval system. *Jurists Review*(2), 43–51.
- [28] Ding, L., & Ren, H. (2023). Risk issues of personal data use from the perspective of digital economy. *Journal of Jinan University (Philosophy and Social Sciences)*, 45(9), 83–93.
- [29] Yin, W., & Zhu, Y. (2025). The US outbound investment security review mechanism and China's responses. *Journal of International Economic Cooperation*(3), 58–69.
- [30] Shou, C., & Tan, Z. (2024). The impact of export control policies on enterprise investment: Evidence from the US entity list policy. *Collected Essays on Finance and Economics*(4), 16–26.
- [31] Huang, Y., & Cheng, H. (2026). Development course, evolution logic and challenge responses of China's export control. *Journal of International Economic Cooperation*(3), 35–43.
- [32] OECD. (2025). Economic security in a changing world. In *New approaches to economic challenges*. Paris: OECD Publishing.
- [33] Bank of Korea. (2026, July 13). Administrative bodies. *Bank of Korea*. <https://www.bok.or.kr/eng/main/contents.do?menuNo=400189>.
- [34] OECD. (2020). One-stop shops for citizens and business. In *OECD best practice principles for regulatory policy*. Paris: OECD Publishing.
- [35] Howlett, M., Vince, J., & Del Río, P. (2017). Policy integration and multi-level governance: Dealing with the vertical dimension of policy mix designs. *Politics and Governance*, 5(2), 69–78.
- [36] U.S. Department of the Treasury. (2026, July 13). Outbound investment security program. *U.S. Department of the Treasury*. <https://home.treasury.gov/policy-issues/international/outbound-investment-program>.
- [37] Qian, J. (2024). On the connection between foreign investment security review and international investment treaties. *Wuhan University International Law Review*(3), 108–125.
- [38] Shen, W., & Chen, R. (2023). On the due process of China's foreign investment national security review and its optimization path. *International Business Research*(2), 72–84.
- [39] National People's Congress. (2026). *Outline of the 15th five-year plan for national economic and social development of the People's Republic of China*. 2026-03-13.
- [40] Hu, E., & Wu, X. (2024). Adhering to the overall national security outlook and promoting in-depth integration of development and security. *Guangming Daily*, 2024-04-14(2).
- [41] Ministry of Commerce, former Cyberspace Administration of the Central Committee, Ministry of Industry and Information Technology. (2021). *Guidelines for outbound investment and cooperation in the digital economy*. 2021-07-20.