https://doi.org/10.37420/j.rbcs.2026.002

Institutional Expansion of National Security Exception Clauses in AI and its Impact on Regional Technology-Business Cooperation Under the B&R Initiative

Hezhuo Tian*

School of Law, Beijing Foreign Studies University, China tianhz2003@163.com

***Corresponding author, E-mail: tianhz2003@163.com**

Abstract

As artificial intelligence technology becomes essential to the global economy, national security legislation has increasingly hindered regional technological collaboration, especially among the B&R Initiative countries. This study investigates the institutional proliferation of national security exception clauses in artificial intelligence, assessing how their extensive and inconsistent implementation escalates compliance expenses, induces market volatility, and disrupts technological exchanges. These disturbances result in systemic shocks to regional economic collaboration, particularly within the digital economy. The paper emphasizes the structural unpredictability inherent in security-oriented regulatory frameworks through different regulatory instances, including the U.S. government's inconsistent AI laws and the application of the Defense Production Act to leverage private-sector AI resources. It examines the policy rationale underlying civil-military integration and its influence on AI regulation. This study examines the legal obstacles encountered by multinational firms regarding extraterritorial regulation, restricted judicial remedies, and failures in international dispute settlement. It advocates for a stratified regulatory system and urges institutional responses at both corporate and international levels, encompassing enterprise-focused compliance initiatives and the establishment of a review mechanism inside the UN framework. The objective is to offer pragmatic solutions for multinational firms confronting these issues and to facilitate the restoration of regional technology-business collaboration while reconciling national security objectives with innovation.

Keywords: AI; National Security Exception Clauses; Regional Digital Economy Cooperation; Belt and Road Initiative; Multinational Enterprise Compliance

1 Introduction

Artificial intelligence has emerged as a crucial catalyst for global regional economic collaboration. Within the BRI framework, the progression of the Digital Silk Road persists, as nations along the route enhance collaboration in cloud computing, artificial intelligence technologies, and digital infrastructure. In this context, regulatory obstacles justified by "national security" have proliferated, breaking traditional cooperation patterns and creating systemic uncertainty within the regional technology-business ecosystem.

A sequence of commercial events, such as Huawei's market access limitations in various nations, ByteDance's compelled divestiture in the United States, India's prohibition of Chinese applications, and the fluctuating U.S. AI regulatory frameworks, collectively exemplify the issue this paper examines. The magnitude and unpredictability of these interventions cannot be attributed solely to individual policy choices; they signify a profound institutional inclination towards the broad and erratic use of national security exception clauses inside the technological sphere.

The path of U.S. AI regulation exemplifies this unpredictability effectively. On September 9, 2024, the U.S. Bureau of Industry and Security (BIS), in accordance with Executive Order 14110 regarding the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, promulgated a proposed rule instituting mandatory reporting requirements for AI enterprises that fulfill designated criteria. The regulatory basis of the rule, however, was ephemeral. Shortly after taking office on January 20, 2025, President Trump annulled E.O. 14110, and a subsequent executive order mandated all agencies to evaluate and halt operations executed under the revoked directive. The proposed reporting requirements, which had not been completed, thereby lost their authorizing basis prior to implementation. When major powers utilize security exception frameworks to implement extensive technology controls and subsequently rescind or alter those frameworks under subsequent administrations, the ensuing regulatory instability causes independent commercial detriment to enterprises and nations involved in cross-border technology collaboration. The damage arises not solely from the stipulations of any specific rule but from the inherent unpredictability of the system as a whole.

National security exception provisions originated in Article 21 of the General Agreement on Tariffs and Trade (GATT, 1947), allowing member states to implement appropriate measures to safeguard their fundamental security interests. This provision was initially conceived as a "safety valve," offering restricted exclusions for governments under extraordinary situations (Li, 2015). The subsequent evolution, from its integration into the WTO framework via Article 14 of the General Agreement on Trade in Services (GATS) and Article 73 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), to the 2019 Russia–Ukraine trade dispute where the WTO Dispute Settlement Body first subjected the clause to substantive judicial examination (WTO Panel Report, WT/DS512/R, 2019; Hahn, 1991), illustrates a gradual, though incomplete, progression towards enhanced external accountability. Recently, regional accords like the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the United States–Mexico–Canada Agreement (USMCA) have expanded member states' autonomous discretion by abolishing the WTO's specified categories of "essential security interests" (Li & Peng, 2023), directly impacting enterprises functioning in BRI markets. When a member limits AI technology transfers for national security reasons within these frameworks, impacted commercial entities have nearly no institutional recourse available.

The emergence of the AI era has broadened the conventional notion of national security, which formerly focused on military and geopolitical concerns, to encompass economic security, technological security, data security, and various other areas. This expansion obscures the distinction between international trade regulations and national security policy, diminishes enterprises' capacity to establish stable expectations for cross-border operations, and subjects the technology cooperation ecosystem of BRI countries to ongoing pressure from extraterritorial regulation.

This paper examines the various legal challenges arising from this expansion, elucidates the strategic rationale and commercial consequences of security-oriented AI regulation, systematically assesses the legal relief issues faced by multinational corporations, and proposes governance strategies that amalgamate enterprise-level and institutional responses. The objective is to offer a practical reference for multinational corporations addressing these challenges and for the comprehensive reestablishment of the regional business cooperation framework.

2 Legal Challenges in the Application of National Security Exception Clauses

2.1 Definitional Ambiguity and Expansionism

With technological advancement, the implications and scope of national security are seeing significant transformation. Conventional legal interpretations of risk were mostly restricted to tangible effects, although the nonlinear evolution of AI has transcended this constraint. The threats associated with AI are both dynamic and unpredictable, displaying significant ethical dimensions because of their profound integration inside the human social network (Zhang & Wei, 2024).

In the context of evolving security paradigms, the United States has utilized the Defense Production Act (DPA) as a versatile administrative tool. It has been utilized to facilitate mobilization and information collection in regions deemed strategically significant. The DPA was initially established to guarantee the provision of wartime materials. Through legislative amendment and changing practices, it has been linked to priority allocation, capacity enhancement, and various forms of governmental intervention in production and supply chains. In the domain of AI, citations of the DPA have been employed to rationalize initiatives aimed at enhancing transparency in the creation of frontier models and large-scale computing. The swift alteration of the executive framework in January 2025 demonstrates that security-oriented governance can be established and disassembled rapidly. This volatility amplifies compliance uncertainty and escalates the risk of disruption for cross-border technological collaboration.

The uncertainty of “national security” is accompanied by the challenge of defining “emergency situations.” According to conventional definitions, the phrase predominantly pertains to wartime circumstances or other exigencies in international relations, such as armed combat, natural disasters, or economic crises. The immediacy, opacity, and potential destructiveness of AI technology have disrupted the traditional definition of an “emergency.” Cross-border data flows exemplify a significant concern, as data breaches or algorithmic manipulation can substantially affect national security in a brief timeframe, representing a true ’emergency’ in practical terms. The lack of explicit definitional requirements permits authorities to classify ordinary technology hazards as emergencies, thereby continually justifying the broad application of the clause.

2.2 Monopolization of Unilateral Decision-Making

The exact procedural implementation of these clauses reveals a twofold predicament: the unilateral monopoly of member states’ autonomous judgment and the significant lack of external scrutiny.

2.2.1 Fact-Finding Authority

At the fact-finding stage, governments possess practically unfettered autonomous discretion about the existence of a security concern. Due to the elevated sensitivity and confidentiality of security information, states generally base threat assessments on intelligence data that is not publicly available, preventing external entities from effectively validating the factual foundation of these assessments. In matters of national security, U.S. federal courts typically exhibit a deferential stance towards classified material summaries submitted by administrative agencies, seldom contesting their factual conclusions (Pozen, 2005).

2.2.2 Necessity Assessment and Power Asymmetry

In the context of necessity assessment, even when an objective security danger is present, the determination of which response measures are "necessary and appropriate" is solely the prerogative of the state. According to GATT Article 21, each contracting party may undertake actions it deems "necessary" to safeguard its essential security interests. This formulation designates each member state as the exclusive arbiter of the reasonableness of its trade restriction measures, thereby precluding WTO panels from independently evaluating whether a member's invocation of the security exception is vital to its security interests or conforms to the categories enumerated in Article 21(b) (Murrill, 2018). The autonomous judgment authority inherent in national security exemption clauses permits states to impose arbitrary trade restrictions during emergencies, while the lack of explicit judicial review requirements fosters potential misuse (An, 2013).

Moreover, from the viewpoint of international power dynamics, dominant nations typically wield greater discursive authority and practical autonomy in the interpretation and implementation of security exception clauses (Paulsen, 2019). Although WTO Article 21 officially grants equal independent judgment rights to all members, the actual exercise of this ability exhibits significant imbalance. Powerful nations like the United States can withstand the diplomatic and economic repercussions of unilateral security exceptions, whereas smaller states frequently refrain from contesting such actions due to apprehension of possible retaliation. This structural power disparity is especially acute for BRI countries, many of whom are developing states.

2.3 Absence of Multilateral Supervisory Mechanisms

The current international regulatory framework is deficient in robust multilateral oversight and enforcement measures. International bodies like the WTO frequently have challenges in delivering substantive rulings during disputes involving the invocation of security exceptions, a challenge stemming from the intrinsic conflict between national security and judicial oversight. On one hand, national security involves fundamental sovereign interests and has historically been considered a domain exempt from judicial review. Conversely, preserving the integrity of the international economic system necessitates that the application of national security exceptions be limited (Li & Peng, 2023).

In terms of enforcement, even when international conflict resolution agencies render decisions, practical implementation encounters significant opposition from state authority. In the U.S. steel and aluminum tariff disputes (WT/DS544, WT/DS552, WT/DS556, WT/DS564), despite litigation from various nations, the United States upheld the legitimacy of its national security measures and threatened to disengage from the WTO dispute resolution system. The intricacy of critical matters in the AI sector, including cross-border data flows and algorithmic security, intensifies the enforcement deficit, rendering international regulation largely superficial.

The aforementioned institutional deficiencies do not exist in isolation. In the field of AI, these structural attributes interact with the technology's dual-use nature and swift iteration processes to yield tangible and quantifiable commercial outcomes. This section analyzes how these processes result in normative divergence, systemic disruption of regional business collaboration, and significant legal relief challenges for international corporations working within the BRI digital economy framework.

3 Generalization of Security Concepts in AI Regulation and Commercial Impact

3.1 Normative Divergence and Commercial Spillover

The broadening of national security's definition is the fundamental factor contributing to the erosion of normative boundaries, and the conflation of national security with economic interests has emerged as a principal institutional challenge facing the contemporary international economic and trade system (Shaffer,

2021). Numerous notable instances demonstrate how states have employed "national security" as a front for economic protectionism and geopolitical rivalry. In 2018, the United States enacted tariffs on steel and aluminum products pursuant to Section 232 of the Trade Expansion Act of 1962, primarily driven by economic protectionism rather than authentic security threats (Steinbock, 2018). In 2019, Japan implemented export controls on essential semiconductor materials against South Korea, citing national security, which significantly disrupted global semiconductor supply chains (Koo, 2024). In 2020, the United States instituted a series of technology restrictions on Huawei and ZTE (Bu, 2024). Additionally, India prohibited TikTok and other Chinese applications in the same year, ostensibly for data security reasons (Mishra et al., 2022). The swiftly changing U.S. AI regulatory environment, from the extensive mandatory reporting obligations established by E.O. 14110 to their retraction within hours of an administrative shift, exemplifies the latest and potentially most structurally illuminating event in this series. The commercial detriment caused by the expansion of security exceptions is exacerbated by the volatility of the frameworks themselves.

The notion of "national security" has significantly broadened, moving beyond traditional military and geopolitical aspects to include economic, technological, ecological, and public health security, among others. The emergence of the digital economy has profoundly disrupted the conventional binary analytical framework of security and economics (Farrell & Newman, 2019), rendering national security exceptions a versatile tool for evading international trade commitments.

The broadening of security principles in BRI digital economy collaboration has had considerable business spillover effects. The development of digital infrastructure in BRI nations significantly relies on international technological collaboration, whereas legislative constraints imposed by foreign states on technology providers for security reasons often directly impede the advancement of BRI cooperative initiatives. The Huawei situation in the 5G network construction sector is enlightening. The restrictions enacted by the United States and its allies impacted not only Huawei's commercial activities but also directly hindered collaborative efforts in numerous Belt and Road Initiative countries that depend on Huawei technology for digital infrastructure development, resulting in project delays, increased costs, and necessitated modifications to technological strategies.

Furthermore, the subjectivity inherent in security threat evaluations yields varied outcomes based on the specific conditions of each country. A cyberattack may pose a significant danger to a technologically advanced economy while exerting minimal impact on a nation with an underdeveloped technology infrastructure (Pinchis-Paulsen et al., 2024). The diversity of evaluation standards complicates the establishment of a cohesive notion of "national security" in international rule-making, placing developing countries involved in the BRI at a disadvantage during institutional discussions.

3.2 Systemic Shocks to Regional Business Cooperation

The broad application of national security principles is causing systemic harm to the regional business cooperation framework at three levels.

At the compliance cost level, extensive and volatile security assessment frameworks considerably elevate the operational expenses and market entry barriers for technology companies involved in cross-regional collaboration. Mandatory security assessment requirements augment the compliance load for organizations, while ongoing security assessment and reporting duties prolong R&D cycles and hinder enterprises' capacity to swiftly capitalize on market opportunities. AI firms operating in BRI markets face intricate compliance challenges from domestic regulations, which are further exacerbated by extraterritorial regulatory demands, resulting in several overlapping compliance obligations. The inherent instability of the regulatory framework implies that investments in compliance may become futile due to administrative changes, while organizations cannot confidently cease compliance preparations due to the potential for reinstated requirements under varying political circumstances.

The fluctuation of security controls is altering the investment rationale within regional technology marketplaces at the investment and innovation level. Numerous investors facing erratic security assessment environments have commenced reevaluating investment risks within the technology sector, leading to a trend where innovation capital shifts towards more stable, less politically volatile markets, thereby artificially establishing barriers to regional technological collaboration. In domains like large language models and multimodal foundation models that necessitate significant initial investment, the risks posed by regulatory uncertainty may compel enterprises to forgo pioneering innovation initiatives, consequently jeopardizing the innovation potential of the entire regional technology ecosystem.

The widespread implementation of security exception clauses is expediting the regional reconfiguration of global technology supply chains at the supply chain and technology pathway level. Countries participating in the Belt and Road Initiative are compelled to select between divergent technological trajectories. Choosing technology suppliers that adhere to Western standards may incur elevated prices and foster dependency, but sustaining technological collaboration with nations like China could subject them to threats of secondary sanctions. This drive for technological alignment not only skews conventional market decisions in regional company collaboration but also inflicts significant disruptions on the technology ecosystem of BRI digital economy cooperation.

3.3 Civil-Military Integration as a Strategic Driver

The systemic shocks outlined are not just policy byproducts; they signify a calculated strategic approach inherent in security-focused AI legislation. Regulatory measures targeting frontier AI enterprises should be perceived as transcending simple technological compliance mandates. They also demonstrate an inherent civil-military integration rationale wherein strategically significant assets are anticipated to be comprehensible to the state and, when required, accessible for national security imperatives. In the United States, advanced AI capabilities are being centralized within private enterprises. This engenders a systemic quandary for security governance. Dependence on voluntary transfers from the commercial sector may result in inadequate sight and control over capabilities deemed strategically significant. Increased administrative pressure may exacerbate distrust between the government and the innovation environment, thus undermining investment incentives.

This tension elucidates why security-oriented instruments persist over political cycles, even when specific programs are modified or terminated. For firms involved in BRI-related technological collaboration, the primary spillover is commercial. Multinational corporations operating in several jurisdictions may be required to reconfigure supply chains, modify product roadmaps, and reevaluate cooperation frameworks in light of evolving security standards. The outcome is not just increased compliance expenses but also diminished predictability regarding which collaborations would sustain viability over a medium-term planning horizon.

This strategic tension originates from profound structural issues inside U.S. governance of developing technology. The former U.S. Deputy Secretary of Defense articulated in 2020 that the United States urgently required “a democratic response to civil-military fusion” (Flournoy & Chefitz, 2020), highlighting a profound institutional issue: the technological disparity, where commercial innovation has significantly surpassed the military sector, renders previous dependence on market mechanisms for integration inadequate to achieve the strategic objective of securing the technological high ground amid great power competition.

Three causes propel this strain. The limited efficacy of technology innovation conversion within the framework of previous civil-military integration is evident, as defense sector investments in non-traditional innovation constitute a mere 0.055% of procurement budgets. This starkly contrasts with private technology firms, which generally allocate over 20% of their revenue to research and development, resulting in a “valley of death” dilemma where innovative technology fails to be effectively transformed into military capability (Lewis, 2021; Northrop, 2024). A crisis of confidence has emerged between the U.S. government and tech-

nological companies due to conflicting beliefs. The 2018 Google incident exemplified Silicon Valley's perception of technology as a means for societal advancement rather than military application, hence intensifying private companies' opposition to "civilian-to-military" involvement. Third, the inadequate operational efficiency of U.S. official institutions results in the potential termination of programs deemed essential in official strategic documents due to bureaucratic dysfunction (Chapman, 2024), thereby undermining the trust between defense agencies and the innovation ecosystem.

In the burgeoning AI sector, leadership in domestic innovation in the United States has transitioned from the government to the private sector. Technology behemoths like Google and Meta allocate significantly greater resources to AI research and development compared to conventional defense contractors, with their R&D spending as a percentage of revenue surpassing that of the five leading defense firms by a factor of five (Alden et al., 2019). Survey data indicating that 80% of Silicon Valley executives assessed their connection with the Department of Defense as "poor" or "very poor" implies that administrative coercion is improbable to rectify the fundamental trust deficit. Scholars contend that the challenge facing the United States is not inadequate defense expenditure but rather that the U.S. military is being challenged by adversaries employing more effective strategies (Brose, 2019). Furthermore, they assert that governments should base economic interventions on a comprehensive strategic framework instead of resorting to simplistic security exceptions (Rodrik, 2024).

The spillover consequences of this strategic orientation are particularly significant from a regional business collaboration standpoint. The strategy of subjecting private enterprise AI technology to national regulation, via mandatory reporting, investment scrutiny, or export restrictions, imposes heightened compliance demands on multinational corporations involved in BRI technology collaboration. This may compel certain enterprises to prioritize non-commercial political factors in their regional market strategies, thereby jeopardizing the integrity of the commercial ecosystem within BRI digital economy cooperation (Darby & Sewall, 2021; Koo, 2024).

3.4 Legal Relief Predicaments for Enterprises

In addition to undergoing technical examination by government entities, enterprises, especially non-U.S. firms, encounter many legal impediments in asserting their rights inside the judicial system.

3.4.1 Domestic Judicial Relief

Enterprises encounter many obstacles in domestic court redress, such as limited standing, reversed burden of proof, and judicial deference. U.S. federal courts use a rigorously restricted approach to the standing of corporate plaintiffs, making it challenging for them to get the constitutional rights protections afforded to individual people. TikTok's legal challenge against the Protecting Americans from Foreign Adversary Controlled Applications Act, asserting a violation of the First Amendment's free speech provision, ultimately failed, as the justices determined that national security supersedes TikTok's free speech assertions (TikTok Inc. v. Garland, 2024). Firms encounter an inequitable allocation of the burden of proof; when the government asserts a national security concern, the resulting information asymmetry and confidentiality render it nearly impossible for firms to gather adequate evidence for a robust defense. In the Huawei and WeChat cases, the U.S. government utilized think-tank research and expert evaluations to conclude that the companies represented national security dangers, while the companies were unable to obtain critical data to prove otherwise. This implicit reversal of the burden of proof effectively undermines firms' right to pursue litigation. Moreover, post-9/11 U.S. judicial practice has embraced a widespread inclination to defer to administrative decisions related to national security (Chesney, 2009), allowing administrative agencies latitude for "deference, respect, and restraint" while avoiding unnecessary political disputes (Huo, 2021). In WeChat Users Association v. United States, "national security interests" are often cited to bypass standard court review processes (Hao, 2022).

3.4.2 Non-Litigation and International Channels

The scope for firms to resolve conflicts through lobbying and market adjustments is diminishing at the level of non-litigation relief. In 2012, Huawei invested tens of millions of dollars in lobbying but was unsuccessful in altering the U.S. government's assessment of security threats; similarly, ByteDance's lobbying efforts in 2019 proved useless (Hao, 2022).

In the realm of international dispute resolution, enterprises ostensibly have access to international dispute settlement mechanisms; however, the operational collapse of the WTO Appellate Body has rendered the dispute resolution process ineffective, hindering the international mechanism's ability to deliver prompt and efficient relief. Furthermore, the United States has always adopted a utilitarian approach to international law, prioritizing domestic law over international law according to an absolute national interest criterion (Zhang, 2013).

It is clear that multinational corporations, especially non-U.S. firms involved in BRI technology collaboration, encounter complex legal challenges regarding national security exception clauses, necessitating the urgent development of more equitable institutional frameworks. The simultaneous failures in judicial, lobbying, and international spheres indicate that no existing relief mechanism for enterprises is sufficient, requiring a multifaceted institutional approach that tackles the issue concurrently at the enterprise, regulatory, international, and regional levels.

4 Governance Pathways: Enterprise Strategies and Institutional Responses

The remedy gaps identified in Section 3.4 indicate that enterprise-level actions are inadequate and that concurrent institutional change at several levels is necessary. This section presents a stratified response framework. Proactive compliance strategies at the enterprise level ensure instant operational resilience. A tiered classification structure at the regulatory level limits the definitional scope for invoking security exceptions. A specialized adjudication body at the international institutional level provides the independent review capability now lacking in global governance. At the regional level, BRI-specific coordinating entities transform these principles into enforceable procedural mandates. The four elements are interdependent: without regulatory definitional clarity, enterprise compliance strategies are inherently reactive; without regional coordination, international mechanisms cannot effectively address sector-specific harms; without enterprise-level participation, multilateral norm-setting lacks the necessary technical foundation for credibility.

4.1 Enterprise-Level Compliance Strategies

In light of the aforementioned structural relief challenges, multinational firms must not assume a passive stance toward national security exception concerns. The development of a proactive compliance strategy is the most readily implementable approach at the organizational level.

The primary objective is to establish a robust regulatory intelligence capability. The dynamic and evolving characteristics of national security exemption clauses necessitate that companies operating inside BRI jurisdictions engage in ongoing surveillance of legislative changes in critical markets, especially the United States, the European Union, and significant BRI partner nations. This is not solely a legal compliance role but an essential component of commercial risk management. Recent experience illustrates that regulatory reach can be broadened through executive action with minimal parliamentary involvement and can be similarly revoked swiftly, resulting in insufficient adjustment time for firms in either scenario. Organizations that sustain dedicated regulatory intelligence functions, whether via internal legal teams or specialist outsourced counsel, are more adept at anticipating and addressing changes in compliance requirements prior to causing operational interruption.

The secondary aim is the proactive localization of data architecture and technology supply chains. The primary business risk arising from the increase of security exceptions is that current technological designs, designed for efficiency rather than regulatory compliance, may rapidly become non-compliant. Organizations involved in BRI digital economy collaboration must evaluate if their existing data storage, processing, and transmission setups render them susceptible to extraterritorial regulatory jurisdiction, especially under legislation like the Cloud Act. When possible, architectural segregation between data environments governed by several regulatory countries mitigates compliance risk and diminishes the influence of any single authority in a security-related difficulty.

The third priority entails the strategic diversification of technology partnership portfolios. The technology-alignment pressure faced by BRI countries generates reciprocal risks for firms providing technology to those markets. Organizations that cultivate varied supplier relationships and eschew profound reliance on a single vendor are more adept at adapting when security-driven constraints impact certain supply chain partners. This is equally crucial for firms obtaining investment. Over-reliance on finance from a single jurisdiction engenders susceptibility to investment screening mechanisms, such as the Committee on Foreign Investment in the United States (CFIUS) procedure.

The fourth priority is engaging in industry standard-setting and the development of multilateral norms. Individual enterprises generally lack the institutional authority to directly contest applications of national security exception clauses in most international forums; however, industry associations and multilateral technical standard organizations offer indirect avenues for enterprises to influence the normative landscape. Organizations with substantial investments in BRI digital economy collaboration should proactively engage with entities like the International Telecommunication Union and nascent AI governance forums, providing technical expertise to delineate clearer definitional boundaries between commercial AI and security-sensitive applications. This involvement fulfills a dual purpose: it mitigates regulatory ambiguity that facilitates broad security-exception claims while simultaneously fostering technical consensus for effective multilateral governance.

4.2 A Tiered Regulatory Framework: The Technology Gap Flow Mechanism

The progression of technology and national security demonstrates a multifaceted relationship. As an emerging technology possessing both commodity and weapon attributes, AI encounters difficulties in international governance, where traditional trade regulations and weapons control frameworks have proven inadequate. International economic and trade regulations insufficiently address the military characteristics of AI, enabling nations to evade restrictions by invoking national security exceptions; simultaneously, arms control frameworks such as the Nuclear Non-Proliferation Treaty are irrelevant due to the commercial significance of AI. This paper proposes a hierarchical management framework to address the dual governance gap, based on the "Technology Gap Flow Mechanism," which classifies AI into three categories—highly militarized, dual-use, and predominantly commercial—according to the extent of military-civilian technical disparity. This classification immediately limits the interpretive framework within which nations can invoke security exceptions against standard commercial technology, thus establishing a strong regulatory foundation for BRI-related AI collaboration. For companies engaged in BRI digital collaboration, this boundary-setting feature alleviates compliance uncertainty stemming from unregulated security-exception usage and ensures dependable channels for legitimate commercial AI activities.

For extensively militarized AI, stringent review and regulatory measures must be instituted, referencing weapons control frameworks like the Wassenaar Arrangement, alongside the creation of an AI military application registration system to guarantee transparency in technological advancement and implementation.

A control list for military-civilian dual-use AI should be formulated based on technical performance metrics, including computational capacity and model scale, alongside security measures such as end-use assess-

ments and data segregation, with a technology flow monitoring system instituted to oversee cross-border dissemination.

International trade regulations may persist for commercial AI, augmented with fundamental security norms like data privacy and algorithmic transparency, thereby integrating AI into the regulatory framework of international trade agreements.

This tiered approach possesses substantial practical importance for firms involved in BRI digital economy collaboration. Commercial AI represents the primary component of BRI technological collaboration. The clear classification of this matter within international trade regulations would establish a stable and predictable regulatory framework for associated collaboration, diminishing the compliance uncertainty that presently compels enterprises to adopt defensive market strategies and obstructing extraterritorial entities from disrupting normal regional commercial technology cooperation under the pretext of security.

4.3 An International Specialized Adjudication Body

The tiered regulatory framework offers a theoretical basis for AI regulation; nevertheless, effective implementation necessitates the creation of a specialized international adjudication body to assess the appropriateness of national security clause applications.

4.3.1 Institutional Design

The institutional framework of this specialized entity should adhere to three fundamental principles: limited authorization, procedural guarantees, and substantive fairness. An International Security Exception Clause Review Committee should be constituted as a subsidiary body of the UN General Assembly, rather than the Security Council, to circumvent the institutional limitation imposed by the veto power of permanent members, which could render the committee functionally ineffective.

The Committee should implement a multi-disciplinary composition model of legal experts, security specialists, and technology professionals, establishing an organizational structure that integrates law, security, and technology. In growing fields like cybersecurity and technology security, legal analysis alone cannot adequately evaluate the validity and seriousness of security concerns; a thorough assessment by expert technical judgment is essential.

4.3.2 Review Standards and Enforcement

The primary duty of the Committee should be the thorough examination of nations' claims regarding security exceptions. Utilizing previous judicial practices of the International Court of Justice, the Committee would possess the authority to differentiate and validate the components of national security exception clauses that pertain to subjective state judgment from those that are subject to objective assessment criteria. The Committee may implement a three-tier review standard when examining particular circumstances. The initial layer entails evaluating if the invoking state is exercising its rights in good faith. The second layer entails performing a need assessment of the specific actions implemented under the national security clause, determining the availability of less restrictive alternative measures. The third layer necessitates the use of proportionality and evidence assessment, obligating the invoking state to furnish adequate proof that substantiates both the existence of the threat and the proportionality of the response measures.

To avert the Committee's decisions from devolving into mere formalities due to insufficient enforcement authority, appropriate enforcement measures must be instituted. The Committee may investigate novel linkage mechanisms with international financial institutions, including the International Monetary Fund and the World Bank, beyond the conventional reporting to the General Assembly and Security Council. This would involve integrating compliance with security exception rules into national risk assessments and loan conditionalities, thereby augmenting the economic repercussions of non-compliance.

For enterprises, a functioning international adjudication body addresses one of the problems identified in Section 3.4, the absence of any neutral forum in which the evidentiary basis for a security exception invocation can be independently assessed. Even in instances where enterprises do not possess direct standing before such an entity, the presence of a legitimate adjudication mechanism generates indirect commercial advantages by elevating the reputational and diplomatic repercussions of baseless security exception claims, consequently diminishing their frequency of utilization.

4.4 Regional Coordination Within the BRI Framework

In addition to the UN-level Review Committee, the establishment of regional coordination mechanisms inside the BRI digital economy cooperation framework holds significant supplemental importance for preventing national security exception provisions from undermining regional business collaboration.

Regional coordination mechanisms emphasize the establishment of procedural regulations for invoking security clauses within designated regions or sectors, reflecting internal self-restraint among members regarding the use of security exception clauses, and creating a governance network with distinct functional divisions in conjunction with the UN-level external oversight mechanism. In contrast to the ex post oversight of the Security Exception Review Committee, which is initiated upon request, regional mechanisms can implement thorough ex ante consultation, ongoing evaluation, and ex post review systems for national security exception clause applications, effectively monitoring member states' security exception activities and preventing abuse at its origin.

Building upon the values and structure of the Digital Silk Road Cooperation Initiative, provisions for transparency notifications about security exceptions may be incorporated into current BRI digital economy cooperation agreements, subject to the following precise stipulations.

The ex ante notification mechanism stipulates that when a party intends to invoke national security exception clauses that may impact the technology-business cooperation of other members, the invoking state must furnish prior notification, detailing the purpose, specific measures, and anticipated duration of the security exception application. This requirement fulfills a procedural role and exemplifies the idea of good faith (Kong, 2018), aligning with the BRI's internal tenets of "extensive consultation, joint contribution, and shared benefits." The review term stipulation mandates that, subsequent to notice, an appropriate review duration of no less than sixty days be instituted, during which other states may provide inquiries and recommendations concerning the pertinent actions. The invoking state must assess received opinions via appointed professionals and deliver a clear answer with articulated justifications.

The sunset clause, based on the WTO's Anti-Dumping Agreement provision, mandates periodic reviews of security exception clause invocations post-implementation and stipulates automatic expiration after a specified duration unless the invoking state can prove the ongoing necessity of the measure, thereby circumventing the issue where activated security exception clauses cannot be rescinded by any entity other than the invoking state.

The temporary freeze mechanism and regional compensation mechanism are, respectively, based on the interim measures system of the European Court of Human Rights and the EU's energy solidarity mechanism. The temporary freeze mechanism allows the regional coordinating body to implement interim measures mandating an invoking state to halt its acts upon identifying a legitimate and impending threat of irreparable harm, thereby supplementing the inherent constraints of the protracted security review process. The regional compensation mechanism creates a fund for compensating affected commercial entities, thereby increasing the institutional costs associated with the misuse of national security exceptions and encouraging member states to evaluate the necessity and proportionality of such measures more rigorously. This mechanism is especially crucial for small and medium-sized developing BRI nations, offering tangible protection for their legitimate business interests when affected by security exception implications.

The BRI regional coordination structure generates commercial value for firms that extends beyond its official legal obligations. The ex ante notice system provides advance information on impending regulatory changes, enabling businesses in impacted markets to commence contingency planning prior to the implementation of restrictions. The compensation method establishes a precedent that commercial harm resulting from security exception measures constitutes a recognizable injury deserving of redress, altering the default assumption that firms must bear such expenses without recourse.

4.5 Insights from China's AI Governance Practices

Unlike U.S. and European AI legislation, China's AI legislative progress prioritizes a regulatory framework that harmonizes development with security, concentrating on establishing a cohesive system of interdependent rules. The legislative trajectory demonstrates a progression from soft law to hard law, incorporating targeted legislation that addresses specific AI risks while maintaining room for development and exploration of AI, deemed the most suitable approach for the present and foreseeable future (Ding X., 2024).

From the standpoint of national security, China embraces a more comprehensive and realistic multidimensional security framework, dismissing a singular approach to security understanding. The Holistic National Security Concept underscores five pairs of interrelationships, emphasizing foreign and internal security; territorial and citizen security; traditional and non-traditional security; development and security challenges; and self-security and collective security. Regarding security governance, based on the principle of a "Community of Shared Future for Mankind," China promotes the harmonious interplay between technological innovation and safety growth through inclusive and prudent regulation (Sun, 2024). In legislative practice, China employs an "experimental first, phased and categorized" regulation strategy for new technological applications, establishing safety baselines while allowing room for innovative advancement. This specific legislative approach offers an instructive institutional framework for reconciling innovation with security.

From a commercial governance standpoint, China's "inclusive and cautious" regulatory approach offers significant insights for businesses operating in BRI markets. The structured and classified regulatory framework offers AI companies distinct compliance expectations, hence mitigating confusion in cross-regional activities. The "experimental first" regulatory flexibility maintains a space for exploration of innovative business models, preventing the suppression of technical innovation due to excessive regulation. China's promotion of equal development rights and the utilization of artificial intelligence in international cooperation, while opposing technological monopolies and exclusive alliances, offers significant policy guidance for establishing inclusive technology governance mechanisms within the Belt and Road Initiative framework.

The principle of "harmonious coexistence" inherent in esteemed traditional Chinese culture offers governance ideas for the regulation of national security issues. According to the ideology of peaceful coexistence, security must be universal, equitable, and inclusive; common security can only be attained by acknowledging and addressing the legitimate security concerns of all parties. The Global Security Initiative Concept Paper emphasizes that strategic communication between governments may foster mutual trust, resolve conflicts, manage disputes, and eradicate the underlying causes of crises. Entities participating in proactive communication and equitable dialogue within multilateral coordination frameworks, addressing each other's legitimate security apprehensions and averting national security exception clauses from evolving into tools of unilateralism and protectionism, can endeavor to establish an international security milieu defined as "common, comprehensive, cooperative, and sustainable".

China's regulatory model, albeit informative in its organized and categorized methodology, functions within a unique institutional and political framework that may not be directly applicable to other multinational governance contexts. The practical significance of this experience resides not in complete adoption

but in its illustration that security and innovation goals may be implemented within a cohesive legislative framework—a notion relevant across various jurisdictional situations.

5 Conclusion

The rapid advancement of AI technology is leading to an unparalleled revolution in the scope and modalities of the application of national security exemption clauses. The clause has evolved from functioning as a "safety valve" for member states in extraordinary situations during the GATT period to being a mechanism often utilized for the enforcement of extensive technological regulations, subsequently altered with each administrative transition. This broad application has significantly influenced state economic and trade relations, technological innovation, and the advancement of the digital economy. Recent U.S. instances of executive-driven AI reporting and transparency initiatives, initially justified by national security concerns and subsequently rescinded in the January 20, 2025, package, exemplify not the specific content of any rule but rather reveal a persistent pattern of framework instability. This unpredictability results in autonomous economic detriment. Organizations may invest significantly in compliance readiness, only to witness the legal foundation dissolve, while BRI partner nations grapple with establishing solid expectations for technological collaboration pathways.

The issues arising from the broadening and proliferation of national security concepts, exacerbated by the structural instability of the frameworks that implement these concepts, can no longer be adequately resolved within the current international regulatory framework. In this context, companies engaged in BRI technological collaboration sometimes encounter complex legal relief challenges. Domestic court remedies are ineffectual because of security discretion; non-litigation avenues like lobbying and negotiation have limited effectiveness on security matters; and international dispute resolution procedures fail to offer timely and effective protection due to operational failures.

This study provides a comprehensive array of enterprise-level and institutional approaches to address this problem. Multinational corporations involved in BRI digital economy collaboration must focus on enhancing their regulatory intelligence capabilities, proactively reorganizing their data infrastructures and technology supply chains for regulatory resilience, diversifying their technology partnerships, and actively participating in the development of multilateral norms to influence the parameters of commercial AI governance. At the institutional level, implementing a stratified and classified regulatory framework grounded in the "Technology Gap Flow Mechanism" would facilitate distinct control strategies that mitigate the proliferation risks associated with highly militarized technologies while allowing sufficient latitude for commercial innovation. A Review Committee for the International Security Exception Clause within the UN General Assembly framework would furnish the essential review capability currently lacking in international governance, therefore dismantling the state monopoly on security determinations. Integrating the BRI digital economy cooperation framework into regional coordination mechanisms, featuring ex ante notification, review periods, sunset clauses, temporary freeze mechanisms, and regional compensation funds for comprehensive oversight, would produce tangible commercial advantages for enterprises in impacted markets. Leveraging China's inclusive and prudent AI governance experience, the advancement of transparent and equitable international consultation procedures can avert national security exception provisions from transforming into tools of unilateralism and hegemonic politics.

As an evolving strategic technology, AI is transforming international security frameworks and regional business environments at an unparalleled pace. This significant transformation of national security exception clauses impacts not only the stability of the international trade order but also directly influences the operational landscape of multinational corporations, the future direction of BRI digital economy collaboration, and the robust advancement of global technological innovation ecosystems. A governance system that merges enterprise-level resilience strategies with multilevel institutional coordination, while incorporating

diverse stakeholder participation and multidimensional value considerations, is essential to safeguard national legitimate security interests without unduly hindering technological innovation and commercial collaboration. This signifies both a commitment to the essence of international rule of law and a necessity for global governance in the era of AI.

References

Agreement on Trade-Related Aspects of Intellectual Property Rights, Article 73. (1994).

Alden, E., Faskianos, I., Haass, R., & Sewall, S. (2019). Technology and national security: Maintaining America's edge. The Aspen Institute Press.

An, B. (2013). Analysis of WTO national security exception clauses. Journal of International Trade, (3), 125–131.

Brose, C. (2019). The new revolution in military affairs. Foreign Affairs, 98(3), 122–134.

Bu, Q. (2024). Behind the Huawei sanction: National security, ideological prejudices or something else? International Cybersecurity Law Review, 5(1), 255–285.

Bureau of Industry and Security, U.S. Department of Commerce. (2024). Establishment of reporting requirements for the development of advanced artificial intelligence models and computing clusters. (accessed 23 October 2025).

Chapman, J. (2024). American military-civil fusion at risk with the loss of the Shift Fellowship. War on the Rocks. (accessed 6 November 2025).

Chesney, R. M. (2009). National security fact deference. Virginia Law Review, 95(6), 1361–1432.

Comprehensive and Progressive Agreement for Trans-Pacific Partnership, Article 29.2: Security Exceptions. (2018).

Darby, C., & Sewall, S. (2021). The innovation wars: America's eroding technological advantage. Foreign Affairs, 100(2), 142–153.

Ding, S. (2025). U.S. civil-military technology integration policy and its generative logic under great power competition. International Economic Review, (2), 12.

Ding, X. (2024). China's AI legislation in global comparative perspective. Comparative Law Research, (4), 13.

Executive Order No. 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. (2023). The White House.

Farrell, H., & Newman, A. (2019). Weaponized interdependence: How global economic networks shape state coercion. International Security, 44(1), 42–79.

Flournoy, M., & Chefitz, G. (2020). Sharpening the U.S. military's edge: Critical steps for the next administration. Center for a New American Security. (accessed 6 November 2025).

Hahn, M. J. (1991). Vital interests and the law of GATT: An analysis of GATT's security exception. Michigan Journal of International Law, 12(3), 599–602.

Hao, M. (2022). Judicial pathways for Chinese technology enterprises defending rights in the United States: The WeChat users case as a reference. Contemporary American Review, (1), 39–44.

Huo, Z. (2021). Research on bills of attainder under the U.S. Constitution: Developing from the Huawei v. United States case. Administrative Law Review, (6), 42.

Kong, Q. (2018). National economic security and the application of WTO exception rules. Social Science Journal, (5), 138.

Koo, M. G. (2024). Securitizing high-technology industries: South Korea–Japan dispute over materials–parts–equipment products. Business and Politics, 26(1), 1–22.

Lewis, J. A. (2021). National security and the innovation ecosystem. Center for Strategic and International Studies. (accessed 6 November 2025).

Li, W. (2015). On the application of WTO national security exception clauses under the new security landscape. Journal of China University of Political Science and Law, (3), 99.

Li, Z., & Peng, D. (2023). Types, evolution, and Chinese practice of digital trade exception rules. Pacific Journal, (2), 71.

Mishra, M., Yan, P., & Schroeder, R. (2022). TikTok politics: Tit for tat on the India-China cyberspace frontier. International Journal of Communication, 16, 820–841.

Murrill, B. J. (2018). The "national security exception" and the World Trade Organization. Congressional Research Service.

New York Times. (2018). The business of war: Google employees protest work for the Pentagon. (accessed 10 December 2025).

Northrop, K. (2024). What happened at America's own military-civil fusion fair. The Wire China. (accessed 6 November 2025).

Paulsen, M. (2019). Trade multilateralism and U.S. national security: The making of the GATT security exception. Michigan Journal of International Law, 40(3), 1–56.

Pinchis-Paulsen, M., Saggi, K., & Mavroidis, P. C. (2024). The national security exception at the WTO: Should it just be a matter of when members can avail of it? What about how? World Trade Review, 23(3), 265–285.

Politico. (2024). Conservatives prepare attack on Biden's AI order. (accessed 19 December 2025).

Pozen, D. E. (2005). The mosaic theory, national security, and the Freedom of Information Act. The Yale Law Journal, 115(3), 628–679.

Rodrik, D. (2024). Reimagining the global economic order. Review of Keynesian Economics, 12(3), 389–404.

Shaffer, G. (2021). Trade law in a data-driven economy: The need for modesty and resilience. World Trade Review, 20(3), 1–20.

Steinbock, D. (2018). America's new steel and aluminum protectionism. China-US Focus. (accessed 30 November 2025).

Sun, Z. (2024). Threat, security, and peace: A comparative textual study of Chinese and American national security concepts. International Relations Research, (5), 141.

TikTok Inc. v. Garland, No. 24-1113. (2024). U.S. Court of Appeals for the D.C. Circuit. (accessed 13 November 2025).

White House. (2025). Initial rescissions of harmful executive orders and actions. (accessed 19 April 2025).

World Trade Organization. (2019). Russia—Measures Concerning Traffic in Transit: Report of the Panel, WT/DS512/R.

Zhang, L., & Guo, R. (2020). Analysis of "national security exception" clauses in international trade rules. International Forum, (3), 71.

Zhang, X. (2013). On international rule-making for network information security cooperation. Zhongzhou Academic Journal, (10), 52.

Zhang, X., & Wei, Y. (2024). Research on fundamental issues in China's AI legislation. Law and Social Development, (6), 9–10.