Journal of Social and Political Sciences

Zhang, H., & Jiang, Y. (2026), The Microfoundations and Security Implications of Technological Sovereignty in the Digital Age. *Journal of Social and Political Sciences*, 9(2), 66-88.

ISSN 2615-3718

DOI: 10.31014/aior.1991.09.02.719

The online version of this article can be found at:
https://www.asianinstituteofresearch.org/

Published by:
The Asian Institute of Research

The Asian Institute of Research *Social and Political Sciences* is a peer-reviewed International Journal. The journal covers scholarly articles in the fields of Social and Political Sciences, which include, but are not limited to, Anthropology, Government Studies, Political Sciences, Sociology, International Relations, Public Administration, History, Philosophy, Arts, Education, Linguistics, and Cultural Studies. As the journal is Open Access, it ensures high visibility and the increase of citations for all research articles published. The *Journal of Social and Political Sciences* aims to facilitate scholarly work on recent theoretical and practical aspects of Social and Political Sciences.

ASIAN INSTITUTE OF RESEARCH
Connecting Scholars Worldwide

ASIAN INSTITUTE OF RESEARCH
Connecting Scholars Worldwide

The Asian Institute of Research
Journal of Social and Political Sciences
Vol.9, No.2, 2026: 66-88
ISSN 2615-3718

DOI: 10.31014/aior.1991.09.02.719

The Microfoundations and Security Implications of Technological Sovereignty in the Digital Age

Hanzhi Zhang[1], Yuhang Jiang[2]

[1,2] School of Regional and Country Studies, Beijing International Studies University, Beijing, China

Correspondence: Yuhang Jiang, School of Regional and Country Studies, Beijing International Studies University, Beijing, China, 100024. Tel: 008618868092850. E-mail: 2023221443@stu.bisu.edu.cn
ORCID ID: https://orcid.org/0009-0006-8357-5003

Abstract
In the age of artificial intelligence, firms' technological capabilities have become a critical variable underpinning the logic of national security; however, the mechanisms through which micro-level technological evolution translates into macro-level security outcomes remain insufficiently understood. Taking the Chinese embodied intelligence Unitree Robotics as a case study, this article develops an analytical framework of "technological capability–mechanism–security outcome" and identifies three causal mechanisms: the Capability Effect, the Dependency Effect, and the Rule Effect. Drawing on process tracing and multi-source data, the study yields three major findings. First, firms' technological innovation capabilities can directly enhance national strategic autonomy by providing alternative pathways for critical technologies; however, such effects remain constrained by dependence on underlying hardware and software infrastructures. Second, the dependency structures generated through firms' integration into global technological systems improve operational efficiency while simultaneously introducing latent security vulnerabilities. Third, firms' technological advantages can only be transformed into stable institutional power once they are institutionalized as industry standards. These three mechanisms exhibit a progressive relationship characterized by "capability foundation–dependency constraint–rule diffusion," jointly shaping the dynamic process through which firm-level technological capabilities are converted into national security resources. By moving beyond a state-centric perspective and shifting the level of analysis from the state to the firm, this study elucidates the logic through which firms' micro-level capabilities are transformed into national security assets. It further argues that technological capability building at the firm level should be incorporated into the broader framework of national security governance.

Keywords: Artificial Intelligence, Technological Sovereignty, National Security

1. Introduction

In recent years, the rapid evolution of artificial intelligence (AI) technologies has fundamentally reshaped both the scope and boundaries of national security (Hoadley & Lucas, 2018). In frontier domains such as embodied intelligence, advanced manufacturing, and autonomous systems, critical technological breakthroughs are increasingly driven by leading technology firms (Feng et al., 2025). Through its indigenous innovation in embodied intelligence, Unitree has emerged as a pivotal node within the global technological ecosystem and as a

representative case for the study of national security in the AI era (Chen, 2025; China National Intellectual Property Administration, 2025). Similarly, Boston Dynamics and the capital and military-industrial networks underpinning it have been regarded as critical connectors of U.S. security capabilities (Scharre, 2018), while European AI firms have increasingly served as strategic vehicles for the European Union's pursuit of technological sovereignty (European Commission, 2024). These developments suggest that, in the age of artificial intelligence, firms are evolving from mere competitors in technology markets into critical nodes within national security architectures (Ren, 2024). This transformation not only reconfigures the organizational logic of technological innovation, but also raises pressing theoretical challenges regarding the mechanisms through which national security is constituted and sustained.

Existing studies on technological sovereignty largely conceptualize the state as a unitary and rational technological actor, while treating firms as passive implementers of state policy. Such perspectives overlook the agency of firms in shaping technological trajectories and innovation ecosystems. In practice, however, the pace and direction of innovation in fields such as embodied intelligence are highly contingent upon firms' micro-level research and development activities (He et al., 2025a). Firm-level technological capabilities do not merely serve national strategies in a subordinate manner; rather, they profoundly shape national security outcomes by redefining capability boundaries and restructuring dependency relations (He et al., 2025b). Accordingly, this article asks the following core question: How do firms' technological capabilities constitute the microfoundations of national technological sovereignty? Furthermore, through what pathways and mechanisms are these capabilities transformed into national-level security resources?

This article takes Unitree, a leading Chinese robotics firm, as a case study to examine how firm-level technological capabilities are transformed into national security resources. The analysis proceeds along three dimensions. First, it investigates how firms expand the boundaries of national security capabilities through breakthroughs in core technologies (Capability Effect). Second, it examines how dependency structures emerging from firms' integration into the global division of labor generate new constraints on national security (Dependency Effect). Third, it explores how firms' technological trajectories become institutionalized as industry standards and subsequently reshape governance rules in a recursive manner (Rule Effect). Building upon this framework, the article further identifies both the synergies and tensions between firms' commercial logics and national security objectives, and analyzes how this dynamic relationship influences the stability of technological sovereignty at a deeper structural level.

The contributions of this article are reflected at both the theoretical and empirical levels. Theoretically, the study moves beyond the static perspective that conceptualizes technological sovereignty solely as a state-level macro-strategy. Instead, it develops a micro–macro interactive framework centered on firms, thereby shifting the analytical focus of technological sovereignty from national strategy to firm-level capability structures. Empirically, through in-depth case analysis and process tracing, the article systematically examines the interactive dynamics between technological evolution and security governance in the field of embodied intelligence. This framework not only explains the security spillover effects associated with Unitree, but also provides a transferable theoretical tool for analyzing state–firm security relations in other strategic technological domains, including semiconductors and quantum computing.

2. Literature Review

2.1 From Sovereignty to Technological Sovereignty

Sovereignty, the cornerstone of the modern international order, was conceptualized by Jean Bodin (1576) as absolute authority and later institutionalized via the Peace of Westphalia as a territorial principle of political authority (Yang, 2011). Traditionally, this mandated exclusive state control over defined geography and populations. However, the transboundary nature of information technology is reshaping this spatial logic. Grant (1983) early identified that technological embeddedness erodes geographical constraints, while Edler et al. (2020) argue that the challenge has shifted from territorial integrity to structural dependence on external technological

systems. Consequently, external control over critical technologies poses a direct threat to national security (da Ponte et al., 2023).

In the AI era, algorithms, data, and computing power have become core strategic resources (Toffler, 2006), positioning "technological sovereignty" as the primary nexus between technology and national security (March & Schieferdecker, 2023). Despite its growing prominence, scholarship lacks a unified operational definition and a consensus framework to systematically explain how technological capabilities translate into state power.

2.2 Diverging Approaches to Technological Sovereignty

Current research diverges into three primary analytical strands based on distinct problem orientations and theoretical assumptions.

The EU-centric approach conceptualizes technological sovereignty as "strategic autonomy" attained through institutional governance. Prompted by the Snowden revelations (Maurer et al., 2015), the EU leveraged instruments like data protection and technical standards to reduce external dependencies (da Ponte et al., 2023). This strategy seeks to externalize internal regulatory norms globally, establishing a form of "normative power" (Qi & Chen, 2021; Liu, 2023). However, critics note that without robust core innovation, this approach remains a governance aspiration rather than an actualized capability.

The US-centric approach embeds sovereignty within the logic of great-power competition, prioritizing absolute technological leadership. Here, sovereignty is sustained through continuous innovation and technological superiority (Yin & Liu, 2025), reinforced by export controls and supply chain restructuring (Wang, 2025; Geng, 2025). While emphasizing capability, this approach is criticized for the "securitization" of technology, which risks distorting market mechanisms and fragmenting the global technological ecosystem.

The China-centric approach emphasizes "indigenous controllability," viewing technological sovereignty as a pillar of national modernization and security (Xi, 2018). Strategy focuses on core technology breakthroughs and industrial chain restructuring to achieve endogenous control (Gao & Yan, 2025). Key policy frameworks (State Council, 2015, 2017) aim to minimize external dependence by strengthening state-led resource allocation (Allen, 2019). Yet, an overreliance on state leadership may stifle market dynamism and international cooperation, complicating its long-term efficacy.

Despite divergent orientations, these approaches remain state-centric, treating technological sovereignty as a macro-level outcome while neglecting the micro-mechanisms of its production. Consequently, this study shifts the analytical focus to the firm level to explain the underlying logic of technological sovereignty through micro-level capabilities and behaviors.

2.3 Firm Capability Structures and the Microfoundations of Technological Sovereignty

Scholarship is increasingly shifting from the state to the firm level, emphasizing companies' foundational role in securing critical technological domains (Dibiaggio et al., 2024).

First, firms' competitive advantages manifest in full-stack innovation and ecosystem leadership, spanning R&D, industrial coordination, and trajectory guidance (Song & Li, 2024). Through resource orchestration, leading firms shape innovation pathways and ecosystem structures, directly influencing national autonomy in critical sectors (He et al., 2025b).

Second, data has evolved into a critical production factor essential for knowledge creation (Central Committee of the CPC & State Council, 2020; Jiang et al., 2024).. Beyond enhancing innovation efficiency, data serves as a carrier of external knowledge that shapes a firm's absorptive capacity (Xie et al., 2020; Qu et al., 2025). Consequently, firm-level data governance is no longer just a market advantage but a cornerstone of national data sovereignty and technological security (National and Local Co-Built Innovation Center, 2024).

Finally, standards competition acts as the intermediary transforming technological capability into institutional power. Prior research has investigated the effects of technological diversification and network embeddedness on firms' standard-setting capabilities (Zou et al., 2017). Firm-led trajectories, once institutionalized as industry norms or international standards, extend influence beyond markets into the domain of global rule-making (Tian, 2024). Thus, strengthening firm standardization is vital for anchoring technological achievements (Central Committee of the Communist Party of China & State Council, 2021).

Overall, while technological sovereignty is a state attribute, its practical boundaries cam be shaped by firms' innovation, data governance, and standardization capabilities. However, current research relies on fragmented, single-dimensional analyses. A systematic framework is required to theorize how multidimensional firm capabilities embed into national technological systems through specific causal mechanisms to produce security outcomes.

2.4 Theoretical Advances and Gaps in Firm-Level Case Studies

Innovation research is shifting from outcome-oriented performance metrics toward systematic micro-mechanism analyses, following three primary trajectories.

The first trajectory focuses on capability evolution, explaining how firms achieve upgrades through organizational adjustment and technological iteration (Feng et al., 2025). While this dynamic capabilities perspective clarifies endogenous innovation (Yu et al., 2025; Yin, 2025), it remains confined to firm-level performance, neglecting broader structural impacts. Building upon this, the second strand utilizes resource orchestration and innovation ecosystems, situating firms within broader networks to examine meso-level industrial structures (Ma et al., 2025; Zhu et al., 2024). However, its focus on innovation efficiency overlooks the political implications of firm-led ecosystem evolution. The third strand situates firm behavior within geopolitics, linking corporate strategy to national rivalry (Ma & Liu, 2025). It demonstrates how firms reshape global structures via trajectory selection and standards-setting (Huo et al., 2025), which more directly addresses the macro-level implications of firm behavior, yet remains primarily descriptive, lacking systematic modeling of causal mechanisms.

Despite these advances, the literature suffers from analytical fragmentation: micro-level studies struggle to scale upward, while macro-level analyses lack traceable foundations. Theoretical integration is needed to explain how firm-level capabilities embed into national systems through specific causal pathways to determine technological sovereignty and national security outcomes.

3. Theoretical Conceptualization and Analytical Framework

This section establishes a mechanism-oriented, micro-macro analytical framework to explain the transformation of firm-level technological capabilities into national security outcomes. Departing from macro-strategic narratives or simple variable correlations, this study posits that firms trigger identifiable mechanisms through three capability dimensions—innovation provision, dependency structuring, and rule formation. These dimensions systematically transmit micro-level technological activities into macro-level security effects.

Methodologically, the impact of firm behavior on national security is defined by path dependence and contextual variation, eluding explanation through linear variables. A mechanism-based analysis is thus better suited to uncovering the generative processes of these effects, moving beyond descriptive "what happened" accounts to explanatory "how" and "why" logic.

3.1 Theoretical Conceptualization of Firm-Embedded Technological Capability

Firm-Embedded Technological Capability is conceptualized as a composite system forged through indigenous research and development, data accumulation, and standards participation. This system uniquely integrates endogenous innovativeness with exogenous embeddedness. Unlike traditional theories of firm capability, this

concept emphasizes two interrelated dimensions: first, the degree of firms' autonomous control over core technologies; and second, the embedded and dependent relationships between firms and the international technological ecosystem. While the former dictates the capacity to provide technological alternatives, the latter determines resilience against external shocks and exposure to systemic risks.

More specifically, the capability consists of three analytically distinct components. First, technological innovation capability refers to the capacity for full-stack, systemic breakthroughs and iterative advancement, rather than isolated "point" innovations. Its essence is the power to autonomously define technological trajectories. At the firm level, this manifests in strategic patenting, vertical integration of hardware/software, and full-chain R&D-to-production control; at the national level, it serves as the foundational pillar of sovereignty.

Second, data governance capability. In the AI-driven economy, data is a strategic resource with explicit security attributes. This capability encompasses both the scale of data and the firm's mastery of the entire data lifecycle—from collection and annotation to training and circulation. The distribution of this capability directly dictates national effectiveness and risk exposure in algorithmic security, privacy, and data sovereignty. Third, standards competition capability refers to firms' ability to transform technological trajectories into global industry norms through standard-setting and rule negotiation. It involves institutionalizing technological advantages, thereby shaping ecosystem structures beyond mere market competition. Here, firms act not only as technology producers but as architects of governance structures.

These components are mutually constitutive and progressive: innovation capability provides the foundation, data governance serves as the strategic asset, and standards competition represents the institutional consolidation of the previous two. Collectively, they form the micro-level foundation upon which national technological sovereignty is realized.

3.2 Theoretical Conceptualization of the Three Core Mechanisms

Building upon the foregoing capability framework, this article proposes three core mechanisms to explain how Firm-Embedded Technological Capability connects to and reshapes the foundations of national security.

3.2.1 Capability Effect: Direct Support for Strategic Autonomy

The Capability Effect describes how firms' independent, controllable and evolving innovation capabilities in core technologies directly affect a country's strategic autonomy and operational capacity, and further shape national security performance (Wang & Han, 2024). The underlying premise is that "capability itself constitutes security". By achieving breakthroughs in core algorithms and systems integration, firms provide the state with independent technological options, expanding its strategic maneuverability against blockades or supply disruptions (Roy et al., 2021). Conversely, fragmented or path-dependent capabilities undermine national autonomy. Unlike other mechanisms, the Capability Effect operates through the direct provision of technological assets, bypassing the mediation of institutional or market structures.

3.2.2 Dependency Effect: Structural Risks and Vulnerabilities

Unlike Capability Effect, Dependency Effect focuses on how a firm's internal and external structural dependencies amplify or mitigate national vulnerabilities. Embedded in global supply chains and open-source ecosystems (Tian et al., 2025), firms often develop asymmetric dependencies on critical hardware or data services. In geopolitical crises, these firm-level dependencies transform into national structural risks (He et al., 2025c). Conversely, strategies such as supply chain diversification and indigenous substitution foster technological redundancy, distributing risk and absorbing shocks (Lund et al., 2020). The essence of this effect lies in the nodes and pathways of risk transmission, making its impact highly context-dependent.

3.2.3 Rule Effect: Institutionalizing Technological Trajectories

Rule Effect refers to the process through which firms transform their technological trajectories into global norms or rule. .By leading standard-setting, firms enhance a state's agenda-setting capacity and institutional power. The central mechanism underlying Rule Effect is the "first-mover lock-in effect": once a trajectory becomes institutionalized as an industry standard, competitors must adapt, reinforcing the leader's structural advantage (Liu & Li, 2022). The extent of firms' participation in standards-setting processes directly affects a state's discursive authority and institutional influence within global technological governance. Unlike Capability Effect, Rule Effect depends less on intrinsic technical sophistication and more on broad adoption and institutionalization, thereby amplifying technological advantages and transforming them into institutional resources within international competition.

3.2.4 Interactions Among the Mechanisms: A Logic of Progression and Mutual Constitution

The three mechanisms share progressive and mutually constitutive relationships. Capability Effect lays the foundation, determining whether firms can deliver effective technological provision. Dependency Effect functions as a "stress test" for firms' capability systems by exposing critical dependencies and vulnerable linkages, thereby driving processes of adjustment and reinforcement. Rule Effect, in turn, institutionalizes technological advantages and converts them into more stable structural power. Meanwhile, rule institutionalization may constrain the evolution of technological trajectories to a certain degree, generating feedback effects on innovation. The dynamic interaction of the three mechanisms collectively shapes the inherent logic whereby firm-level technological capabilities translate into national security resources.

3.3 A Multidimensional Analytical Framework for National Security

To move beyond a reductionist view of national security as a purely technical or military concern, this study adopts a four-dimensional approach encompassing political, economic, societal, and international domains. This taxonomy captures how firm-level capabilities ripple through different sectors via distinct causal pathways, mitigating the theoretical blind spots inherent in single-dimensional analyses.

Political security centers on sovereignty, institutional stability, and strategic autonomy (Yang, 2018). Through Capability Effect and Dependency Effect, firm-level technological capabilities influence the controllability of critical technologies and the depth of external reliance; these factors, in turn, define a state's policy maneuverability and strategic resilience under external pressure.

Economic security emphasizes the stability of the national economic system, industrial competitiveness, and supply chain resilience (State-owned Assets Supervision and Administration Commission of the State Council, 2023). Firm-level technological capabilities reshape a state's structural position within the global economy by influencing industrial value chain positioning, market structures, and control over standards-setting processes. In this context, Capability Effect drives industrial upgrading into high-value segments, while the Dependency Effect risks amplifying systemic vulnerabilities during external shocks.

Societal security addresses social order, public safety, data governance, and technological ethics (Liu, 2012). As data and algorithmic systems become increasingly embedded in societal operations, firm-level technological capabilities can enhance governance efficiency yet simultaneously introduce risks—such as algorithmic bias or data misuse (Zou et al., 2021). In this dimension, the interaction between Capability Effect and Dependency Effect is particularly pronounced.

International security involves states' positions within the international system, discursive authority, and rule-shaping capacity. Firm-level technological capabilities primarily exert influence through Rule Effect, as firms' participation in international standards-setting and rule negotiation processes directly affects states' institutional power and agenda-setting capacity within global technological governance (Farrell & Newman, 2019).

3.4 Operationalization and Scope of the Analytical Framework

To transform the foregoing theoretical framework into an operational analytical tool, the subsequent case analysis in this study follows the logic outlined below. First, it identifies firms' specific manifestations and evolutionary characteristics across the three dimensions of technological innovation capability, data governance capability, and standards competition capability. Second, it analyzes how these capability dimensions generate observable effects across different security domains through the three mechanisms of Capability Effect, Dependency Effect, and Rule Effect. Finally, it identifies the potential tensions between firms' developmental logics and national security objectives, as well as the mechanisms through which such tensions evolve and are mediated under specific contextual conditions.

Crucially, the framework remains agnostic as to whether firm capabilities bolster or undermine security. By explicitly accounting for negative externalities, it creates analytical space to examine misalignments between corporate growth and state imperatives. As profit-driven entities, firms may select technological trajectories that diverge from national interests—a tension that serves as a vital entry point for understanding the modern politics of technology.

In terms of applicability, although this framework originates from the frontier domain of embodied intelligence—which exhibits significant security spillover effects—its analytical logic, grounded in the mechanistic linkage between firm-level behavior and macro-level national outcomes, possesses a degree of transferability. With contextual adaptation, it is applicable to other strategic sectors, including semiconductors, quantum computing, and aerospace. Nevertheless, its boundary conditions and universal applicability warrant further validation through cross-sectoral and cross-national comparative research.

4. Methodological Design

4.1 Method Selection

This study employs a single-case design integrated with process tracing to test how firm-level capabilities influence national security. Given the deep contextuality and procedural nature of the research problem, its causal pathways elude detection via cross-sectional data. Accordingly, a qualitative research approach oriented toward mechanism identification is necessary.

4.1.1 Single-Case Study

Single-case studies are uniquely suited for uncovering complex mechanisms, identifying intervening processes, and testing theoretical models in specific contexts (Birkinshaw et al., 2011). Compared with multiple-case research, its primary advantage lies in the ability to longitudinally trace the evolution of key variables, enhancing the explanatory depth of mechanism-based analysis (Yin, 2014). This study selects Unitree as a critical case. If the mechanisms proposed in this article are supported or refined through this case, the findings may provide broader theoretical insights into the nexus between corporate capability and national security in the AI domain.

4.1.2 Process Tracing

Within this framework, process tracing is utilized to systematically examine causal mechanisms (Liang, 2025). This method validates the existence and operational pathways of mechanisms by identifying a sequence of intermediate steps linking causes and outcomes (Bennett, 2010; Beach & Pedersen, 2020), which is applied in two capacities. First, it is adopted for mechanism testing by tracing the evolution of Unitree's core technological capabilities across developmental stages. It examines how factors including rising localization of core components, expanding data ecosystems, and deeper engagement in standard-setting shape national security-related outcomes via the Capability Effect, Dependency Effect, and Rule Effect (see Figure 1). Second, it is used to construct an evidence chain by integrating multiple data sources, thereby establishing a continuous logical linkage connecting firm-level technological capabilities, causal mechanisms, and eventual national security impacts.

Index	Product	Year	Technical Characteristics	Image	Index	Product	Year	Technical Characteristics	Image
1	Xdog	2013	Prototype quadruped robot featuring a pioneering brushless motor-based actuation solution		9	FirefightingB1	2021	Equipped with 360-degree cameras for real-time fire reconnaissance, LiDAR for environmental mapping, and infrared sensors for detecting trapped individuals	
2	Laikago	2017	First-generation commercial quadruped robot developed by Unitree Robotics		10	B2	2022	The fastest industrial-grade quadruped robot, capable of running at 6 m/s with a maximum joint torque of 360 N · m	
3	Laikago Pro	2018	Upgraded version of the first-generation Laikago platform with enhanced performance and stability		11	B2-W	2023	A wheel-leg hybrid quadruped robot featuring transformable locomotion to overcome endurance limitations	
4	AlienGo	2018	A large-scale and heavyweight quadruped robot, notable for achieving dynamic backflip maneuvers		12	Go2	2023	Equipped with a 4D ultra-wide-angle LiDAR system and a peak joint torque of 45 N · m	
5	A1	2020	A compact quadruped robot recognized for high speed and stability, capable of reaching 3.3 m/s, with human-following and autonomous obstacle-avoidance functions		13	Go2-W	2023	A wheel-leg hybrid variant of Go2 featuring extended battery life and enhanced all-terrain mobility	
6	Go1	2021	The world's first consumer-grade companion quadruped robot, equipped with a 16-core CPU+GPU AI system and a maximum speed of 4.7 m/s		14	H1、H1-2	2023	Full-size electrically actuated humanoid robots capable of achieving a standing backflip, with a walking speed of 3.3 m/s and a maximum joint torque of 360 N · m	
7	B1	2021	An industrial-grade quadruped robot designed to operate in complex terrains and harsh environmental conditions						
8	InspectionB1	2021	An industrial inspection quadruped robot offering intelligent solutions for public safety and firefighting, with a top speed of 6 m/s		15	G1	2024	A humanoid robot exhibiting human-level agility, with a maximum joint torque of 120 N · m and powered by the unified large-scale robot model, UnifoLM	

Figure 1: Illustration of Unitree Robotics' Product Iteration

Source: Compiled by the author

4.2 Case Selection

Unitree Robotics is selected as the focal case, fulfilling the criteria of representativeness, data availability, and theoretical relevance (Gioia et al., 2013).

First, in terms of representativeness, Unitree Robotics is a benchmark firm in China's AI hardware sector, particularly in quadruped robotics and embodied intelligence (Xu, 2025). The company has achieved significant technological breakthroughs in motion control algorithms, autonomous perception systems, and full-system integration, and competes directly in international markets with firms such as Boston Dynamics (Chen et al., 2025). As embodied intelligence emerges as a frontier of Sino-US-EU strategic rivalry, Unitree's trajectory mirrors the micro-level dynamics of national technological sovereignty (Beijing Frontier Future Technology Industry Development Research Institute, 2025). Second, the firm offers high data transparency. Comprehensive records of financing, product iterations, and patent portfolios—supplemented by policy documents and industry analyses—enable robust cross-validation across multiple data streams. Finally, Unitree demonstrates strong theoretical fit with the proposed mechanisms. Its full-stack R&D illustrates Capability Effect; its residual reliance on critical external components provides an empirical site for Dependency Effect; and its participation in standard-setting offers a window into Rule Effect. These interactions are empirically observable across all four security dimensions, making Unitree an ideal case to test the framework's validity.

4.3 Data Sources

The data of this study are mainly drawn from four categories. First, 65 policy documents are collected from official institutions including the State Council, the National Development and Reform Commission, the Ministry of Industry and Information Technology, and the Ministry of Science and Technology. Spanning 2015–2025, these documents cover strategic plans, industrial policies and financial support concerning artificial intelligence, embodied intelligence and technological autonomy. Second, 45 corporate documents are obtained from Unitree Robotics' official website, financing announcements and public reports, covering its technological development trajectory, financing structure, international cooperation and talent composition. Third, 35 media and interview

materials are gathered from mainstream domestic media, technology outlets and international news sources, to analyze the narratives behind state support legitimacy and the firm's positioning in international competition. Fourth, 117 academic and industrial studies are reviewed to underpin theoretical analysis and provide industry background context.

4.4 Analytical Procedures and Coding Strategy

Building on the above, this study adopts a layered coding approach to process multi-source data systematically. Specifically, open coding is first used to extract key events, data points and statements from raw materials. Second, axial coding categorizes the data into three core dimensions of firms' embedded technological capabilities: technological innovation capability, data governance capability, and standard competition capability. Third, selective coding maps these dimensions to the three mechanisms: capability effect, dependency effect, and rule effect. Finally, this study further identifies the specific manifestations and potential risks of each mechanism across political, economic, social and international security dimensions. The coding framework is summarized in Table 1.

Table 1: Overview of the Coding Framework

Coding Level	Coding Type	Description	Corresponding Model Element
Level 1	Open Coding	Extraction of specific events, data, and statements from policy documents, corporate materials, media sources, and academic studies	Raw empirical materials
Level 2	Core Element Coding	Aggregation of Level 1 codes into three components of Firm-Embedded Technological Capability (FETC): Technological Innovation Capability (T-Cap), Data Governance Capability (D-Cap), and Standard Competition Capability (S-Cap)	Structure of corporate embedded technological capabilities
Level 3	Mechanism Mapping Coding	Mapping Level 2 codes onto the three mechanisms: Capacity Effect (CE), Dependency Effect (DE), and Rule Effect (RE)	Theoretical mechanism
Level 4	Security Dimensions and Potential Risks	Identification of the specific impacts and potential risks of each mechanism across the four dimensions of political, economic, social, and international security(T1–T9)[1]	Multidimensional Impacts on National Security

Source: Compiled by the author

Within the security domain, the four core dimensions—political, economic, social, and international security—are further divided into nine sub-dimensions: Supply Chain Resilience (SCR), Technological Sovereignty (TS), National Narrative (NN), Public Service Resilience (PSR), Data Security and Governance (DSG), Military Application Risk (MAR), International Discourse Power (IDP), Industrial Competitiveness (IC), and Asymmetric Dependence (AD). Accordingly, this study focuses on potential risks (T) stemming from tensions between corporate commercial logic and national security goals, and identifies nine key risk points. These include the tension between commercial iteration speed and national-level reliability requirements; the conflict between international open-source norms and core technology protection; trade-offs between cross-border commercial data

[1] T1: Commercial iteration speed vs. military/national-grade reliability requirements; T2: International open-source sharing logic vs. core technology protection and autonomy; T3: Corporate entertainment-oriented promotion (e.g., Spring Festival Gala) vs. serious national technological image; T4: Embodied intelligence's generalized environmental data needs vs. personal privacy and geospatial information security boundaries; T5: Cross-border flow/cooperation of commercial data vs. national data sovereignty and security regulation; T6: Global commercial exports vs. sensitive technology diffusion and dual-use (military) risks; T7: De facto corporate standard formation vs. exclusion or politicization by international standards organizations; T8: Low-price strategies for market share vs. long-term R&D investment and profit protection; T9: Deep integration into global markets vs. international geopolitical sanctions and decoupling risks

flows and national data sovereignty; and risks arising from deep global market integration amid geopolitical decoupling. Table 2 presents an example of coding correspondence.

Table 2: Data Coding Mapping (Excerpt)

Index	Original Material Type	Core Content Summary	FETC Core Element	Mechanism	Security Sub-dimension	Potential Risk
1	Website Updates	Unitree released the H1 humanoid robot, highlighting self-developed high-performance joint motors.	T-Cap	CE	SCR	T1
2	Media Interview	Founder discusses collaboration with international AI giants on embodied intelligence data.	D-Cap	CE	DSG	T5
3	Policy Document	Made in China 2025 emphasizes independent innovation capability.	T-Cap	CE	TS	–
4	International Commentary	Kharon report points to potential connections between Unitree and the PLA.	S-Cap	DE	MAR	T6
5	Academic Research	Influence of open-source robotics communities on technology dissemination and talent development.	T-Cap	RE	TS	T2
6	Early Development	Pricing strategy of Unitree's early products in the international market.	S-Cap	DE	IC	T8
7	Core Patents	Authorization of Unitree's patented electric-drive leg joint technology.	T-Cap	CE	TS	–
8	Local Policy	Hangzhou municipal government explicitly supports Unitree as a benchmark enterprise.	S-Cap	RE	NN	–

Source: Compiled by the author

4.5 Reliability and Validity Analysis

To ensure the reliability and explanatory validity of the findings, this study implements procedural controls from both reliability and validity perspectives.

In terms of reliability, multi-source data triangulation and temporal tracking are used to reduce single-source bias and the risk of spurious or idiosyncratic interpretations. Specifically, by integrating hierarchical coding with process tracing, the study repeatedly compares the manifestation of the same phenomenon across different data sources, ensuring consistency and traceability in the abstraction from empirical materials to theoretical constructs. In terms of validity, the case is cross-validated within the three-mechanism framework by comparing the differential effects of each mechanism across various security dimensions, thereby mitigating bias from a single explanatory pathway. Meanwhile, key policy documents and major international events are introduced as contextual references to conduct external consistency checks on the analytical results. In addition, counterfactual reasoning is used to explore how firms' developmental trajectories and their security implications might vary under different institutional environments or external constraints, strengthening the robustness of causal inference.

5. Case Analysis: The National Security Effects of Unitree's Firm-Embedded Technological Capability

The Multidimensional Impact Model of Firm-Embedded Technological Capability on National Security posits that firms' technological capabilities generate compound effects across political, economic, societal, and international security dimensions via three mechanisms: Capability Effect, Dependency Effect, and Rule Effect. To evaluate this framework's explanatory power, this study utilizes Unitree to trace how corporate practices embed into national security structures. The analysis reveals that corporate capabilities do not yield security dividends linearly; instead, they redefine national resilience through a dynamic interplay between technological autonomy, structural dependencies, and rule formation.

To ensure analytical rigor, case materials were systematically coded, and the key evidence was consolidated in Appendix. The following sections utilize this evidence to examine each mechanism's operation and its subsequent security implications.

5.1 Capability Effect: The Direct Empowerment of National Strategic Capacity through Technological Autonomy

The Capability Effect centers on how a firm's autonomous and controllable innovation directly empowers national strategic capacity. In Unitree's case, this mechanism translates micro-level R&D activities into a macro-level foundation for technological sovereignty.

From a political security perspective, the autonomy embedded in firm-level capabilities is intrinsically linked to a state's strategic autonomy. This relationship is constitutive: by internalizing core technological breakthroughs, firms provide the state with "technological exit options"—insulating policy flexibility from external blockades or institutional exclusion. Unitree's full-stack strategy serves as a micro-level anchor for national sovereignty in embodied intelligence. Data indicate that the localization rate of Unitree's joint motors, reducers, and controllers now exceeds 90%. Notably, its H1 humanoid robot has reached a peak torque of 360 Nm, effectively disrupting the long-standing dominance of Japanese and German firms (Unitree, 2023). This vertical integration provides the state with a scalable alternative in critical sectors, fortifying strategic resilience against external restrictions (Jia et al., 2025). Such capability functions as a strategic security asset: it guarantees "availability at critical moments" (Yin et al., 2026)—the ability to sustain critical industrial operations without reliance on external actors—thereby fundamentally reinforcing national strategic autonomy.

Within the economic security dimension, firm-level capability reshapes a state's structural position in global competition. While political security concerns the attainability of autonomy, economic security focuses on its sustainability through industrial competitiveness. Here, the Capability Effect operates through a material logic: optimizing industrial cost structures and value chain distribution. Unitree has upended the global pricing architecture of quadruped robotics by leveraging cost-performance synergies. According to Gaogong Intelligent Industry Research Institute data, Unitree captured 69.75% of the global market in 2024, with 23,700 units sold across 100 countries (GGII, n.d.). This technology-driven dominance acts as a strategic buffer; a state bolstered by such global leaders is inherently more resilient to external economic shocks. By internalizing the most cost-intensive segments—including LiDAR and reducers—Unitree has enabled cost reductions that outpace the decline in end-product prices. This vertical integration further generates systemic spillovers: as a domestic cluster of upstream suppliers emerges around Unitree's ecosystem, the resulting industrial density enhances the supply chain resilience of the entire national economy.

In terms of societal security, the Capability Effect manifests through the concretion of concrete application scenarios. Once a firm's technological threshold is crossed, its capability functions as a proactive security asset. Powered by self-developed 4D LiDAR and motion control algorithms, Unitree robots are deployed in high-risk environments—including power inspection, firefighting, and port automation—where complex variables and human risk are structural constants. For instance, the deployment of Unitree-based platforms at Ningbo Port yielded a 30% efficiency gain while significantly mitigating manual safety hazards. This empirical evidence underscores that a firm's contribution to public security is a verifiable outcome rather than an abstract potential. By embedding their capabilities into critical infrastructure, firms evolve from mere vendors into co-constructors

of societal security. This organic transformation translates technological mastery directly into societal resilience, bypassing the need for external institutional mediation.

Within international security, technological breakthroughs contributes to a state's asymmetric leverage. The logic is direct: the presence of a global leader like Unitree shifts the state into a superior structural position within the international order. As other states and organizations draft governance frameworks for embodied intelligence, the technological practices established by Chinese firms have become an unavoidable reference point. This "reference effect" constitutes a form of international influence that transcends traditional institutional constraints and dependency structures. Unitree's market and technical leadership provides the state with the material basis for discursive power, ensuring that national standards are not merely participants in, but architects of, global technological rules.

However, the realization of the Capability Effect is non-linear and carries significant costs. Evidence suggests that Unitree's residual reliance on external chips (e.g., Horizon J5) and simulation software (e.g., MathWorks' Simulink) creates "hidden chokepoint" risks. Such dependencies lead to extreme computational inefficiency, where a single robot's demand can equal the resource allocation of ten servers, severely throttling algorithmic iteration. Consequently, robots like the Unitree Go2 still face critical bottlenecks in foundational industrial software and high-performance computing. This highlights that technological sovereignty is a systemic undertaking; without the simultaneous localization of hardware and software ecosystems, isolated breakthroughs remain vulnerable to broader structures of external dependency.

5.2 Dependency Effect: The Dialectical Unity of Technological Embeddedness and Security Vulnerability

While the Capability Effect underscores the security dividends of autonomy, the Dependency Effect highlights how structural linkages formed during development can paradoxically amplify national risks. In globalized ecosystems, firms act as conduits for risk transmission through supply chain embeddedness, cross-border data flows, and reliance on external infrastructure.

Politically, external dependence in critical sectors evolves into structural constraints on strategic autonomy. Unitree's technological architecture exhibits a "dual structure": while hardware components (motors, reducers, controllers) are largely localized, the foundational "brain"—including high-performance chips and industrial simulation software—remains externally sourced (Integrity Tech Group, 2025). This asymmetric dependence allows external actors to exert systemic pressure through a few critical chokepoints, potentially paralyzing national strategic decision-making in the embodied intelligence domain. This structure challenges the binary view of "autonomous controllability". Technological sovereignty is not a zero-sum condition but a continuum of autonomy (Yang et al., 2025). Autonomy in specific segments is a necessary but insufficient condition for security; as long as bottleneck technologies remain external, strategic sovereignty remains fragile. Furthermore, Unitree's compliance with extraterritorial frameworks (e.g., GDPR, EU AI Act) transcends mere corporate cost—it functions as an institutional constraint on national data sovereignty, coupling domestic technological systems with external governance environments.

Economically, dependency structures dictate supply chain resilience and industrial competitiveness. Unitree exemplifies the tension between these forces: while localizing hardware boosts autonomy, the persistent reliance on external chips creates "substitutive vulnerability." In this non-linear process, the advancement of partial autonomy may concentrate previously dispersed risks into a few critical nodes, generating new forms of systemic risk exposure. Within Global Value Chains, this reflects a hierarchical segmentation: while China holds approximately 38% of the downstream market, it faces acute upstream dependence in foundational materials and components (Li & Shi, 2022). This "downstream strength, upstream weakness" leaves the state vulnerable to cascading shocks. Beyond supply chains, dependence triggers a "path-locking" effect: long-term adaptation to external software ecosystems (e.g., Simulink) creates organizational routines that inhibit indigenous innovation, structurally constraining long-term industrial competitiveness. The computational demand of a single robot, for instance, is estimated to be equivalent to that of approximately ten servers, raising the technological adoption threshold for the industry as a whole. Effective governance requires a shift from compliance-based defense to

resilience-oriented mechanisms grounded in dynamic adaptation (Cheng & Chen, 2025). Managing dependency must escalate from a corporate operational issue to a national strategic priority. This necessitates a comprehensive monitoring and early-warning system across the entire technological chain, ensuring that the state can respond to "chokepoint" risks with systemic agility.

In the realm of societal security, the centralization of data resources, coupled with dependencies embedded in governance processes, creates a dual-layered risk exposure. Through its robotic systems, Unitree has established an intensive data-centric architecture; a single G1 robot reportedly generates approximately 2 TB of environmental perception and motion data daily. While this data-control capacity optimizes operational stability, it also implies that any vulnerability along the governance chain can escalate into a systemic public security incident. The March 2025 Go1 device key leakage serves as a critical empirical case: despite the relative autonomy of Unitree's core algorithms and hardware, security flaws in third-party cloud services facilitated unauthorized access to device control. This incident underscores a pivotal reality in interconnected ecosystems—the "weakest link" in security governance often resides beyond the firm's direct jurisdictional perimeter (Wang, 2024).

Regarding international security, the Dependency Effect extends into the spheres of institutional and regulatory frameworks. Unitree's expansion into European and North American markets necessitates rigorous alignment with extraterritorial mandates like the GDPR. Such data-localization requirements have reportedly increased the firm's IT infrastructure expenditures by 20–30%. These compliance burdens and technical adaptations, dictated by external institutional environments, do more than just increase operational overhead; they objectively constrain the state's strategic maneuverability within global data governance competition. In effect, while global market integration yields economic dividends, it simultaneously creates conduits through which external institutional power may penetrate and reshape domestic governance structures.

In summary, the Dependency Effect reveals a critical theoretical proposition: technological autonomy does not necessarily translate into security autonomy. The deeper firms become embedded within global technological networks, the more complex the dependency structures they confront. Consequently, firms may simultaneously stabilize and destabilize national security structures. This finding provides an important supplement to traditional security paradigms centered on "autonomy and controllability".

5.3 Rule Effect: The Institutionalization of Technological Advantage and State power

The Rule Effect denotes the process by which firms institutionalize their technological trajectories into industry norms or international regulations. By engaging in standard-setting and institutional practices, firms bolster the state's agenda-setting capacity and structural power within the international system. This mechanism serves as a vital bridge, translating micro-level innovation into the architecture of macro-level institutional order.

Politically, a firm's capacity to compete in standard-setting directly shapes the state's discursive authority, agenda-setting capacity, and institutional leverage. In contemporary strategic competition, standards have evolved from technical coordination tools into primary arenas for great-power rivalry. A salient trend is the "over-securitization" of digital standards, particularly in U.S. policy, where technical norms are increasingly framed as frontline instruments to constrain strategic competitors (Xing & Yang, 2026). This discursive construction of technological issues as "existential threats" reflects a political response to the relative shifting of global power dynamics. Against this backdrop, firms like Unitree—possessing substantive technical advantages—function as strategic assets for safeguarding technological sovereignty. When domestic firms propose competitive solutions adopted by international bodies such as the ISO/IEC or ITU, they provide the state with tangible leverage in regulatory competition (Zhang, 2025). International standard-setting is increasingly characterized by a competition among divergent institutional logics. Currently, a tripartite divergence has emerged: the U.S. model emphasizes market-led self-regulation; the EU model prioritizes rights protection and harmonized frameworks; and the Chinese model favors state-guided risk governance. In this context, standards act as carriers of specific governance philosophies (Guest & Wei, 2025). The technological paradigm embodied by Unitree—defined by high performance and cost accessibility—offers a pragmatic reference for China's participation in global robotics governance. This strengthens the state's bargaining power by providing a "proven path" that other actors can adopt. However, the

Rule Effect faces endogenous limitations. First, its sustainability is contingent on continuous technological leadership; once iteration slows, standards risk losing their diffusion potential or becoming targets for external containment. Second, the evaluation of standards is undergoing a "de-technologization" process—technical superiority alone no longer guarantees dominance, as outcomes are increasingly dictated by coalition-building and "softer" forms of institutional power. In public security governance, the Rule Effect is reflected in how firm-led standards reinforce national security infrastructure. In frontier domains like embodied intelligence, technical protocols developed by industry leaders—such as safety testing and risk assessment frameworks—are increasingly integrated into the national public security architecture, as underscored by China's Guiding Opinions on Implementing the Foundational Public Security Standardization Initiative. Unitree's collision-testing procedures and safety redundancy designs provide the state with ready-to-adopt technical specifications. This practice-driven rule provision significantly reduces administrative friction in governing emerging technologies while enhancing the systemic responsiveness and flexibility of the national regulatory framework.

In economic terms, a firm's capacity to shape rules exerts structural influence on national interests by redefining competition norms, market access, and value-chain distribution. In the digital era, control over standard-setting authority increasingly shapes the distribution of gains within global value chains (GVCs). Unitree's trajectory exemplifies the transition from technological advantage to rule-shaping influence. The Mobile Robot Collision Testing Standard led by Unitree has been adopted as a benchmark in the "robot safety certification credit" market. This "monetization of standards"—reminiscent of carbon credit systems—reconfigures the logic of industrial valuation and market competition. This process reflects the "first-mover lock-in effect." Once a technological trajectory is institutionalized, competitors are compelled to adapt, thereby reinforcing the structural advantages of the pioneer. Unitree pioneered this paradigm by substantially modifying open-source algorithms originally developed by Boston Dynamics. The result reduces costs by 40% while maintaining approximately 90% of motion performance, redefining global expectations of "safe, usable, and affordable" robotics. Once this trajectory evolves into a de facto standard, its influence transcends individual commercial interests and develops into a structural advantage for the state in global robotics competition. The struggle over pricing power and Standard-Essential Patent (SEP) licensing further underscores the Rule Effect's implications. Developed economies have historically utilized SEP regimes to lock developing nations into low-value segments, undermining their core competitiveness and supply-chain security. Although the embodied intelligence sector has yet to establish a rigid SEP regime like telecommunications, Unitree's estimated 60–70% global market share has positioned its technological paradigm as a practical reference point in international negotiations. This represents a bottom-up pathway for rule construction. This parallels China's integrated control in rare earths—spanning extraction to standard-setting (Woods, 2025)—with a parallel logic emerging in robotics: firms act as primary drivers, while their standards serve as micro-level carriers of national industrial competitiveness. From a governance perspective, the institutionalization of the Rule Effect involves a converging relationship between technical standards and formal law. Standards are increasingly utilized as agile regulatory instruments that complement rigid legal frameworks. The EU AI Act's "harmonized standards" mechanism illustrates this convergence, where compliance with technical norms serves as evidence of fulfilling mandatory legal requirements. This institutional innovation demonstrates that firm-led standards can evolve into integral components of national governance. For China, the strategic imperative lies in utilizing policy instruments, such as the National New-Generation AI Standards System, to transform firm-level technical expertise into national industrial governance resources. This evolution enables the Rule Effect to transcend corporate practice and evolve into a component of national security strategy. From a societal security perspective, the Rule Effect manifests as a stabilizing force that shapes public expectations regarding technological risk. As robotic systems permeate public spaces, safety transcends mere product performance, becoming a primary determinant of collective societal perception. Unitree's standardized collision-testing procedures and safety redundancy designs provide clear, verifiable boundaries for technological risk. This transition—moving from abstract technological uncertainty to manageable, institutionalized risk—is pivotal. By providing these practice-driven rules, firms significantly reduce administrative friction in frontier technology governance, enhancing the system's overall responsiveness and flexibility.

In the domain of international security, the strategic weight of the Rule Effect is particularly pronounced. When a technological trajectory—defined by specific performance, cost, and application metrics—achieves transnational dominance, its underlying security logic acquires the necessary conditions for international institutionalization.

With an estimated 60-70% global market share, Unitree's technological paradigm has evolved into a de facto reference point for international comparisons and rule negotiations. This status indirectly bolsters the state's discursive authority and bargaining leverage within global governance systems. However, the sustainability of this influence is fragile, contingent upon continuous technological leadership and a relatively open international environment. Should technological iteration stagnate or geopolitical volatility intensify, these standards risk losing their diffusion potential, potentially devolving into instruments used by external actors for technological containment.

5.4 Interactions Among Mechanisms and the Compound Effects of Multidimensional Security

In the Unitree case, the Capability, Dependency, and Rule Effects do not operate as discrete silos; instead, they form a web of reciprocal reinforcement. The Capability Effect serves as both the material substratum and the source of legitimacy for the other two mechanisms. Absent substantive technological mastery, a firm can neither anchor meaningful dependency structures nor exert rule-shaping influence. The Dependency Effect functions as a procedural "stress test" for the Capability Effect, exposing latent vulnerabilities and charting the course for iterative enhancement. Simultaneously, the Rule Effect acts as the institutionalized expression of technological prowess, allowing localized advantages to crystallize into structural power at the industrial and national tiers. Crucially, however, a "rule-heavy" trajectory may trigger institutional ossification, potentially stifling radical innovation and eroding market adaptability.

From a multidimensional security perspective, these mechanisms frequently trigger divergent outcomes across different domains. While the Capability Effect fortifies political sovereignty and bolsters societal resilience through diffusion, its impact on international security remains deeply ambivalent. It enhances a state's bargaining leverage but simultaneously provokes strategic anxiety and preemptive countermeasures from geopolitical rivals, potentially fueling a security dilemma in the technological sphere. Similarly, while the Dependency Effect unveils economic vulnerabilities, the resulting governance imperatives may paradoxically catalyze the construction of resilient institutional arrangements. Collectively, these dynamics indicate that the nexus between firm-embedded capability and national security is not a linear causal chain. It is, instead, a complex adaptive system—dynamic, multidimensional, and fundamentally contingent on the broader geopolitical and socioeconomic context.

6. **Conclusion**

Against the backdrop of profound transformations in the relationship between national technological sovereignty and national security in the age of artificial intelligence, this study addresses the central question of how firms become the micro-foundations of national technological sovereignty. Building upon this inquiry, the article develops a multidimensional analytical model explaining how Firm-Embedded Technological Capability influences national security. Through an in-depth case study and process tracing of Unitree, the study systematically examines the theoretical proposition that firms' technological capabilities generate compound effects across political, economic, social, and international security dimensions through three interconnected mechanisms: the Capability Effect, Dependency Effect, and Rule Effect. The study makes systematic contributions at three levels: theoretical construction, empirical findings, and policy implications.

6.1 Theoretical Contribution: Beyond State-Centric Approaches to Technological Sovereignty

The primary contribution of this research is its theoretical extension and paradigmatic revision of technological sovereignty studies. Whether focusing on the rule-shaping approach represented by the European Union, the technology leadership model represented by the United States, or the autonomy-and-controllability pathway represented by China, existing studies have generally treated the state as a singular and rational technological actor, while comparatively neglecting the agency of firms in technological innovation, capability accumulation, and trajectory selection. Even when firms are considered, they are often narrowly conceptualized as passive implementers of state policy.

By refocusing the analytical lens on the firm-level micro-foundations, this study demonstrates that technological sovereignty is not a static attribute of the state, but a dynamic emergence—continuously generated and diffused through corporate capability structures. Specifically, the Capability Effect illustrates how breakthroughs in core algorithms, hardware, and system integration coalesce into the material bedrock of national strategic autonomy. The Dependency Effect unmasks how the asymmetric linkages inherent in global networks can metastasize into national security risks. Simultaneously, the Rule Effect reveals firms' capacity to institutionalize their technological trajectories into industry norms, thereby bolstering the state's rule-based power and structural leverage within the international system.

This micro–macro framework transcends the state-centricity that has long constrained technological sovereignty discourse, addressing the conspicuous underrepresentation of corporate agency in international political economy and security studies. We contend that in the AI era, firms are no longer mere market competitors; they have become constitutive forces within the national security architecture. This shift necessitates a fundamental rethinking of the interplay between states, markets, security, and the logic of innovation.

6.2 Empirical Findings: The Multidimensional Security Effects of Firm-Embedded Technological Capability

Empirically, this research validates and recalibrates the proposed framework through a rigorous analysis of Unitree as a critical case. The findings culminate in three core propositions that redefine our understanding of firm-level security impacts.

First, the impact of firms' technological capabilities on national security is both non-linear and context-dependent. The Capability Effect is not an automatic byproduct of innovation; its security dividends hinge on the structural integrity and internal coherence of the technological ecosystem. Unitree's trajectory reveals that localized breakthroughs—if divorced from an autonomous substrate of foundational software and hardware—remain shackled by "hidden bottlenecks" that dilute their strategic utility. This finding suggests that the micro-foundations of technological sovereignty are highly systemic in nature, such that external dependence at any critical node may become a structural vulnerability within the broader security architecture.

Second, the Dependency Effect operates through a dialectical duality in which resilience and vulnerability are mutually constituted. Although firms may strengthen system resilience through data centralization and ecosystem integration, these processes simultaneously generate new risks in data governance and computational infrastructure. Moreover, while integration into international markets creates economic gains, it can also open channels through which external institutional power penetrates domestic governance structures, constraining the state's strategic flexibility in international security affairs. This finding challenges the assumption that technological autonomy necessarily produces security autonomy.

Third, the Rule Effect functions as the primary mechanism through which corporate technological superiority is transformed into national institutional power. Once firms' technological trajectories achieve broad market adoption in performance, cost efficiency, and applicability, the technological logics and security norms embedded within them acquire the basis for institutionalization. Firm-led standard-setting not only reshapes industrial competition, but also provides states with institutional leverage in international technology governance. Yet the durability of such rule-shaping influence depends on the continued maintenance of technological leadership and on an international institutional environment that remains open enough to sustain it. Together, these factors define the endogenous limits of the Rule Effect.

6.3 Policy Implications: Firm-Embedded Technological Capability as a Strategic Lever for Governance

The findings offer critical signposts for contemporary policy, particularly as China navigates the dual pressures of accelerated technological catch-up and intensifying strategic rivalry. The analysis yields strategic imperatives at three distinct levels of governance.

First, firms' technological development should be embedded within the national security governance framework rather than treated merely as a subset of industrial or science and technology policy. Alongside support for the autonomous development of critical technologies, the state should establish systematic assessment mechanisms targeting firms' technological capability structures, critical dependency nodes, and participation in rule-making processes. Security governance must therefore move beyond traditional concerns with products, projects, and institutions to include firms' technological trajectories, supply-chain configurations, and data governance practices.

Second, the governance of dependency structures and data should become a central component of technological sovereignty strategies. The study shows that even when substantial localization of core hardware has been achieved, firms may remain externally dependent on computing infrastructure, industrial software, and data governance systems, all of which can generate systemic security risks. Accordingly, alongside breakthroughs in "hard technologies" such as semiconductors and foundational software, policymakers should strengthen governance over "soft" dependency structures, including open-source ecosystems, cloud services, and cross-border data flows, thereby building a resilience-oriented framework across the technological value chain.

Third, states should encourage technologically advanced firms to participate in international standard-setting and rule negotiations so that firm-level technological leadership can be converted into national institutional influence. Because the Rule Effect depends heavily on first-mover advantages and market acceptance, states should support firms through institutional backing, strategic resource allocation, and international cooperation networks, facilitating the incorporation of firms' technological trajectories into international normative systems. At the same time, policymakers should remain alert to the lock-in effects that institutionalized regulation may impose on innovation and seek a balance between institutionalization and flexibility. More broadly, this study suggests that reliance on macro-level technology strategies or industrial policies alone is increasingly insufficient to address the security challenges of technological competition in the AI era. The identification, assessment, and strategic guidance of key firms' technological capability structures—and their alignment with national security objectives—are becoming a new frontier of state governance capacity.

6.4 Research Limitations and Future Directions

The conclusions of this study should be understood in light of several limitations, which also suggest directions for future research.

First, the external generalizability of the case remains limited. This study adopts a single-case design and process-tracing methodology, both of which are effective for mechanism identification and causal inference. However, as a leading firm in embodied intelligence, Unitree exhibits distinctive developmental trajectories, technological choices, and institutional conditions. Whether the analytical framework proposed here can be extended to other sectors—such as semiconductors, quantum computing, or biotechnology—or to firms in different national contexts requires further comparative research.

Second, the quantitative validation of mechanism intensity remains underdeveloped. This study relies primarily on qualitative evidence to demonstrate the existence and operation of the proposed mechanisms. The relative strength, threshold conditions, and interaction effects of the Capability Effect, Dependency Effect, and Rule Effect across different security dimensions have not yet been systematically measured. Future research may construct indicator systems and employ large-scale datasets or mixed-method approaches to test and refine the theoretical propositions advanced here.

Third, the moderating role of institutional environments requires further theoretical elaboration. The case analysis suggests that industrial policy, legal regulation, open-source ecosystems, and international institutional environments significantly shape both the direction and magnitude of firms' technological capabilities' security effects. Yet, due to constraints of scope and methodology, this study does not fully examine the mechanisms through which these institutional factors operate. Future research may investigate how the relative importance of

the three mechanisms varies across institutional contexts and how states can design institutional arrangements that maximize the positive security spillovers generated by firms' technological capabilities.

Fourth, the rapid evolution of technology gives the study's conclusions a transitional character. Artificial intelligence and embodied intelligence technologies continue to evolve rapidly, while firms' technological capability structures, dependency configurations, and rule-shaping influence remain in flux. As a result, the conclusions presented here primarily reflect the current techno-institutional configuration. Future studies may adopt longitudinal designs to trace how the three mechanisms evolve across different stages of firm development, thereby constructing more temporally sensitive theoretical models.

In sum, this study seeks to build a theoretical bridge between technological sovereignty research and national security theory by taking firms as the analytical point of departure. The robustness of this bridge—and its capacity to support broader theoretical development and empirical validation—depends on continued scholarly inquiry. Nevertheless, the study advances a fundamental proposition: in the age of artificial intelligence, any attempt to understand the formation of national technological sovereignty must engage seriously with firms' micro-foundations. Firms are no longer merely carriers of national technological capability; they are increasingly the key arenas in which technological sovereignty is produced, sustained, and contested.

Author Contributions: Conceptualization, Hanzhi Zhang and Yuhang Jiang; Methodology, Hanzhi Zhang; Formal Analysis, Yuhang Jiang; Investigation, Hanzhi Zhang and Yuhang Jiang; Writing–Original Draft Preparation, Hanzhi Zhang and Yuhang Jiang; Writing–Review & Editing, Hanzhi Zhang and Yuhang Jiang; Supervision, Hanzhi Zhang; Project Administration, Yuhang Jiang. All authors have approved the submitted version and agree to be personally accountable for their own contributions and for ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated, resolved, and documented in the literature.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest. The funding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

Informed Consent Statement/Ethics approval: Not applicable.

Declaration of Generative AI and AI-assisted Technologies: This study has not used any generative AI tools or technologies in the preparation of this manuscript.

References

Allen, G. C. (2019). *Understanding China's AI strategy: Clues to Chinese strategic thinking on artificial intelligence and national security.* Center for a New American Security. https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy

Beach, D., & Pedersen, R. B. (2020). *Process-tracing methods: Foundations and guidelines (W. Wang, Trans.)*. Gezhi Press.

Beijing Frontier Future Technology Industry Development Research Institute. (2025, December 19). *Global embodied AI technology industry development trends (2026).* NetEase. https://www.163.com/dy/article/KH5OG9M30511UMKQ.html

Bennett, A. (2010). Henry Brady and David Collier, eds., *Rethinking social inquiry (2nd ed.).* Rowman & Littlefield.

Birkinshaw, J., Brannen, M. Y., & Tung, R. L. (2011). From a distance and generalizable to up close and grounded: Reclaiming a place for qualitative methods in international business research. *Journal of International Business Studies, 42*(5), 573–581. https://doi.org/10.1057/jibs.2011.19

Bodin, J. (1576). *Les six livres de la république.*

Chen, J., Guo, A.-F., Zhou, J., et al. (2025). How new technology companies achieve catch-up and leadership: A case study based on Unitree Robotics. *Tsinghua Management Review,* (Z1), 100–111.

Chen, R. (2025). Unitree: The future light of scientific and technological innovation. *Financial Expo,* (4), 68–69.

Cheng, Z.-H., & Chen, P.-W. (2025). Resilience governance transformation of urban public data security: Dilemma, mechanism, and reconstruction. *Urban Problems,* (5), 25–34. https://doi.org/10.13239/j.bjsshkxy.cswt.250503

Communist Party of China Central Committee, & State Council. (2020, April 9). *Opinions on building a more complete system and mechanism for market-oriented allocation of factors of production.* https://www.gov.cn/gongbao/content/2020/content_5503537.htm

Communist Party of China Central Committee, & State Council. (2021, October 10). *National Standardization Development Outline.*

Da Ponte, A., Leon, G., & Alvarez, I. (2023). Technological sovereignty of the EU in advanced 5G mobile communications: An empirical approach. *Telecommunications Policy, 47*(1), 102459. https://doi.org/10.1016/j.telpol.2022.102459

Da Ponte, A., Leon, G., & Alvarez, I. (2023). Technological sovereignty of the EU in advanced 5G mobile communications: An empirical approach. *Telecommunications Policy, 47*(1), 102459. https://doi.org/10.1016/j.telpol.2022.102459

Dibiaggio, L., Nesta, L., & Vannuccini, S. (2024). *European sovereignty in artificial intelligence: A competence-based perspective.* SSRN. https://doi.org/10.2139/ssrn.5061172

Edler, J., Blind, K., Frietsch, R., et al. (2020). *Technology sovereignty: From demand to concept: 02/2020. Perspectives—Policy Brief.* https://doi.org/10.24406/publica-fhg-300409

European Commission. (2024). *The EU Artificial Intelligence Act.* https://artificialintelligenceact.eu/the-act/

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security, 44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

Feng, Y.-C., Cao, X.-R., Wu, A.-Q., et al. (2025). How do specialized, sophisticated, unique, and innovative enterprises break growth lock-in? A case study based on Mingfei Technology. *Management World, 41*(10), 190–210. https://doi.org/10.19744/j.cnki.11-1235/f.2025.0140

Feng, Y.-C., Cao, X.-R., Wu, A.-Q., et al. (2025). How do specialized, sophisticated, unique, and innovative enterprises break growth lock-in? A case study based on Mingfei Technology. *Management World, 41*(10), 190–210. https://doi.org/10.19744/j.cnki.11-1235/f.2025.0140

Frost & Sullivan, & Toubao Research Institute. (2025, August 28). *AI empowers thousands of industries white paper (Chinese version).* https://www.frostchina.com/content/insight/detail/68ac0ef02cd88e5f3d8b4cb5

Gao, H.-W., & Yan, G. (2025). Promoting Chinese modernization through independent and controllable key core technologies: Theoretical logic, key levers, and implementation paths. *Economist,* (8), 98–107. https://doi.org/10.16158/j.cnki.51-1312/f.2025.08.004

Geng, Z. (2025). U.S. competition with China over international digital technology standards and its impact. *Northeast Asia Forum, 34*(6), 95–109, 126. https://doi.org/10.13654/j.cnki.naf.2025.06.007

GGII (Gaogong Intelligent Industry Research Institute). (n.d.). *GGII official website.* http://www.gg-ii.com

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods, 16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Grant, P. (1983). Technological sovereignty: Forgotten factor in the 'hi-tech' razzamatazz. *Prometheus, 1*(2), 239–250.https://doi.org/10.1080/08109028308628930

Guest, O., & Wei, K. (2025). *China's generative AI regulatory path: National legal framework and platform governance.* Carnegie Endowment for International Peace.

He, J.-H., Su, Y., Li, L., et al. (2025). A case study on the leading role of technology-leading enterprises in emerging technology innovation ecosystems. *Management Review, 37*(8), 276–288. https://doi.org/10.14120/j.cnki.cn11-5057/f.2025.08.008

He, X., Dai, T., Cheng, Y.-L., et al. (2025). Technology risk assessment methods and empirical research: From the perspective of "dependence-control-gap." *Studies in Science of Science,* 1–24. https://doi.org/10.16192/j.cnki.1003-2053.20250923.001

He, Y.-L., Xu, Z., & Li, Z.-Y. (2025). Value orientation, logical mechanism, and cultivation path of embodied AI from the perspective of new quality productive forces. *Journal of Xi'an University of Finance and Economics.* https://doi.org/10.19331/j.cnki.jxufe.20251111.002

Hoadley, D. S., & Lucas, N. J. (2018). *Artificial intelligence and national security.* Congressional Research Service.

Huo, Y., & Sun, H. (2025). How technology-leading enterprises realize innovation ecosystem substitution in a "chokepoint" context: A single-case exploration of Huawei's HarmonyOS ecosystem. *Forum on Science and Technology in China,* (9), 9–20. https://doi.org/10.13580/j.cnki.fstc.2025.09.010

Jia, Y.-Q., Xu, L., Tao, Y., et al. (2025). Research on system security for embodied AI. Posts & Telecommunications Design Technology, (7), 41–45. https://doi.org/10.12045/j.issn.1007-3043.2025.07.007

Jiang, X.-J., Gong, J.-X., & Li, Q.-F. (2024). Data, data relations, and the innovation paradigm in the digital age. *Social Sciences in China,* (9), 185–203.

Li, B., & Shi, G.-W. (2022). Technology, trust, and institution: Will we be safer? *Journal of Dialectics of Nature, 44*(1), 78–84. https://doi.org/10.15994/j.1000-0763.2022.01.009

Liang, Q.-Y. (2025). The application of and reflections on causal mechanisms and process tracing: A review of Process-Tracing Methods: Foundations and Guidelines. *Review of Social Research Methods, 7*(1), 311–324.

Liu, X.-L., & Li, B. (2022). International technical standards and great-power competition: The case of information and communication technology. *Contemporary Asia-Pacific Studies,* (1), 40–58, 158.

Liu, Y. (2023). The EU's technological sovereignty strategy and its realization in the U.S.–EU game over cross-border data flows. International Law Studies, *(6)*, 64–85.

Liu, Y.-J. (2012). *Social security issues in the national security system.* Journal of the Central Institute of Socialism, (2), 95–99. https://doi.org/10.3969/j.issn.1002-0519.2012.02.025

Lund, S., DC, W., & Manyika, J. (2020). *Risk, resilience, and rebalancing in global value chains.*McKinsey Global Institute.

Ma, L.-N., Chu, J.-Q., Zhang, X., et al. (2025). How does ecosystem strategy drive the dynamic evolution of innovation cooperation networks? A dual case study of NVIDIA and Huawei. *Nankai Business Review,* 0–29.

Ma, T.-Y., & Liu, X.-L. (2025). Disruptive innovation: A path for Chinese enterprises to resist Western strategic containment: The digital economy market in Southeast Asia as an example. *Studies in Science of Science*, 0–13. https://doi.org/10.16192/j.cnki.1003-2053.20251208.002

March, C., & Schieferdecker, I. (2023). Technological sovereignty as ability, not autarky. *International Studies Review, 25*(2), viad012. https://doi.org/10.1093/isr/viad012

Maurer, T., Skierka, I., Morgus, R., et al. (2015). Technological sovereignty: Missing the point? In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace (pp. 53–68).* https://doi.org/10.1109/CYCON.2015.7158468

National and Local Co-built Embodied AI Robotics Innovation Center. (2024). *AI embodied intelligence data acquisition specification: Plan No. 2024-1780T-SJ.* Ministry of Industry and Information Technology.

National Intellectual Property Administration. (2025, August 13). Layout a new chess game for robotics industry intellectual property. *Intellectual Property News.* http://www.cnipa.gov.cn/art/2025/8/13/art_55_201001.html

Qi, C.-H., & Chen, G. (2021). A review of the EU data sovereignty strategy based on textual analysis and its implications. *Journal of Intelligence, 40*(8), 95–103, 80. https://doi.org/10.3969/j.issn.1002-1965.2021.08.013

Qu, Y., Zheng, F. F., & Wang, L. S. (2025). The impact of public data openness on technological innovation of agricultural enterprises. *Journal of Henan Agricultural University.* Advance online publication. https://doi.org/10.16445/j.cnki.1000-2340.20250922.004

Ren, B.-P. (2024). The logic of new quality productive forces formed by the transformation of productive forces modernization. *Economic Research Journal, 59*(3), 12–19.

Roy, N., Posner, I., Barfoot, T., et al. (2021). *From machine learning to robotics: Challenges and opportunities for embodied intelligence.* arXiv. https://doi.org/10.48550/arXiv.2110.15245

Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war. W. W. Norton & Company.*

Song, J., & Li, X.-Q. (2024). The Belt and Road Initiative and the balance of ambidextrous innovation in participating enterprises: Insights based on strategic tripod theory. *Management Review, 36*(3), 73–85. https://doi.org/10.14120/j.cnki.cn11-5057/f.2024.03.009

State Council. (2015, May 8). *Made in China 2025 (State Council Document No. 28 [2015]).*

State Council. (2017, July 8). *New Generation Artificial Intelligence Development Plan (State Council Document No. 35 [2017]).*

State-owned Assets Supervision and Administration Commission of the State Council. (2023, November 13). *Strengthening safeguards for national economic security.* http://www.sasac.gov.cn/n2588025/n2588134/c29337116/content.html

Tian, S., Lai, X., Dong, L., et al. (2025). Digital capabilities, integration into global innovation networks, and enterprise innovation performance. *Systems, 13*(3), 212. https://doi.org/10.3390/systems13030212

Tian, Y. (2024). Toward an integrated theory of international competition: Geopolitical competition, technological competition, and international institutional competition. *Studies of International Politics, 45*(1), 5, 9–27.

Toffler, A. (2006). *The power shift. CITIC Press.*

Unitree Robotics. (2023). *Unitree H1 humanoid robot.* https://www.unitree.com/cn/h1

Wang, W. (2025). The ideological foundation and discourse construction of U.S. technological nationalism. *Contemporary World*, (8), 46–51. https://doi.org/10.12451/202509.02223

Wang, W.-G., & Han, X. (2024). Enterprises' strategic technological innovation and the level of industrial autonomy and controllability. *China Industrial Economics, (8),* 43–60. https://doi.org/10.19581/j.cnki.ciejournal.2024.08.003

Wang, X.-X. (2024). Competition in the robotics industry lies in technology selection. *Manager, (10)*, 16–18.

Woods, D. (2025). A Stackelberg model of China's rare earths strategic lead. *Journal of Chinese Political Science.* https://doi.org/10.1007/s11366-025-09921-w

Xie, K., Xia, Z.-H., & Xiao, J.-H. (2020). The enterprise realization mechanism through which big data becomes a real factor of production: A product innovation perspective. *China Industrial Economics, (5),* 42–60. https://doi.org/10.19581/j.cnki.ciejournal.2020.05.014

Xi, J. (2018, May 29). Speech at the 19th Academician Assembly of the Chinese Academy of Sciences and the 14th Academician Assembly of the Chinese Academy of Engineering. *People's Daily, 02.*

Xing, L.-J., & Yang, H.-D. (2026). The pan-security turn of U.S. digital technology standards and its global impact. *Contemporary International Relations, (3),* 119–136, 139.

Xu, X.-X. (2025, October 23). *Unitree Robotics tears off regional labels, aiming at the global industrial high ground of humanoid robots.* https://doi.org/10.28571/n.cnki.nmrjj.2025.002962

Yang, D.-Z. (2018, April 20). *Political security is the foundation of national security. Ministry of National Defense of the People's Republic of China.* http://www.mod.gov.cn/gfbw/jmsd/4809950.html

Yang, W., Wen, J., Wang, F., & Liu, X. (2025). Trade dependency and technological specialization in the ICT supply chain: Structural dynamics and strategic autonomy in major economies. *Telecommunications Policy*. https://doi.org/10.1016/j.telpol.2025.103037

Yang, Z.-W. (2011). *A historical study of international law. Higher Education Press.*

Yin, H.-Y., Wang, Y.-Z., & Su, G.-Y. (2026). Generation mechanism, ethical risks, and regulation paths of the "uncanny valley" effect in humanoid embodied agents. *Journal of Kunming University of Science and Technology (Social Science Edition),* 1–16.

Yin, J.-C., & Liu, H.-Z. (2025). The behavioral logic of U.S. compound leadership in artificial intelligence under great-power technological competition. *Contemporary Asia-Pacific Studies, (5),* 87–115, 170–171.

Yin, J.-Q. (2025). Digital technology application and green innovation in small and medium-sized enterprises: Theoretical analysis, empirical testing, and case validation. *Journal of Wuxi Vocational Institute of Commerce, 25*(5), 17–26. https://doi.org/10.13659/j.cnki.wxsy.2025.05.012

Yin, R. K. (2014). *Case study research: Design and methods. SAGE Publications.*

Yongxin Zhicheng. (2025, December). *"Digital wind tunnel" embodied AI native security solution white paper.* Yongxin Zhicheng Technology Co., Ltd.

Yu, K.-F., Zhan, T.-Y., Xiong, T.-Y., et al. (2025). How do specialized, sophisticated, unique, and innovative enterprises continuously enhance organizational agility? An exploratory case study of Jindalai Environmental Protection. *Chinese Journal of Management, 22*(9), 1606–1617. https://doi.org/10.3969/j.issn.1672-884x.2025.09.003

Zhang, T. (2025). Regulating artificial intelligence through technical standards: Jurisprudence based on cooperative regulation. *Comparative Law Study, (4),* 169–187.

Zhu, A.-M., Wang, H., & Li, W.-S. (2024). The implementation mechanism of modularity-driven evolution of focal firms' innovation ecosystems: A case analysis based on DJI. *Journal of Shenyang University of Technology (Social Science Edition), 17*(4), 400–410. https://doi.org/10.7688/j.issn.1674-0823.2024.04.08

Zou, S.-M., Zeng, D.-M., Zhang, L.-F., et al. (2017). Network relationships, technological diversification, and enterprises' technological standardization capability. *Science Research Management, 38*(9), 12–20. https://doi.org/10.19571/j.cnki.1000-2995.2017.09.002

Zou, Y., He, Y., Lin, W., et al. (2021). China's regional public safety efficiency: A data envelopment analysis approach. *The Annals of Regional Science, 66*(2), 409–438. https://doi.org/10.1007/s00168-020-01025-y

Appendix

Table. Representative Events Illustrating the National Security Impacts of Unitree's Firm-Embedded Technological Capability

Core Dimension	Mechanism	Security Sub-dimension	Potential Risks	Supporting Evidence
Technological Innovation Capability	Capability Effect	Economic Security (Supply Chain Resilience)	Commercialization Speed vs. Military-Grade Reliability Requirements	Unitree reports that approximately 80% of its motors and reducers are self-developed; "Made in China 2025" emphasizes indigenous innovation;the "Guiding Opinions on Accelerating the Transformation and Upgrading of Traditional Manufacturing Industries" advocate industrial upgrading through technological innovation.
	Capability Effect	Political Security (Technological Sovereignty)	International Open-Source Collaboration vs. Core Technology Protection	Unitree promotes open-source educational initiatives; the "14th Five-Year Plan" encourages the development of open-source communities; the "Implementation Plan for the 'Robot+' Application Initiative" promotes the practical application of robotics technologies.
	Rule Effect	Political Security (National Narrative)	Commercial Entertainment Orientation vs. Serious Technological Image	Unitree's H1 and Go2 robots appeared at the Spring Festival Gala; the Hangzhou municipal government officially identified Unitree as a benchmark enterprise for policy support; the "Guiding Opinions on Accelerating Scenario Innovation to Promote High-Quality Economic Development through Advanced Artificial Intelligence Applications" encourage AI-driven innovation.
	Capability Effect	Societal Security (Public Service Resilience)	Boundaries of Data Collection vs. the Generalization Requirements of Embodied Intelligence	The Go2 and H1 are positioned as new forms of embodied intelligence; Unitree robots have been deployed in power inspection and firefighting reconnaissance; the "Three-Year Action Plan for Data Elements X" promotes the strategic utilization of data resources.
Data Control Capability	Rule Effect	Societal Security (Data Security and Governance)	Commercial Data Accumulation vs. State Data Security Regulation	Unitree has engaged in cooperation with Google and NVIDIA; the "Interim Measures for the Administration of Generative Artificial Intelligence Services" establish regulatory requirements for generative AI; the "Ethical Norms for the New Generation of Artificial Intelligence" provide governance principles for AI development.
	Dependency Effect	International Security (Risks of Military Applications)	Commercial Export Expansion vs. Sensitive Technology Diffusion	A Kharon report alleged links between Unitree and the PLA; the United States initiated a Section 232 investigation; the "Guidelines for the Innovative Development of Humanoid Robots" emphasize the establishment of secure and reliable industrial supply chains.
Standard-Setting Capability	Rule Effect	International Security (International Discursive Power)	Formation of De Facto Standards vs. Exclusion from International Standard-	Unitree reportedly holds a 60–70% share of the global quadruped robotics market; the United Nations adopted resolutions on AI governance; the "Guidelines for Building a Comprehensive Standardization System for the National Artificial Intelligence Industry" promote AI standardization strategies.

	Rule Effect	Economic Security (Industrial Competitiveness)	Setting Organizations Low-Price Strategy vs. Long-Term Profitability and R&D Investment	Wang Xingxing suggested that “robot taxes” may become feasible in the future; Unitree has initiated IPO listing guidance procedures.
	Dependency Effect	International Security (Asymmetric Dependence)	International Market Penetration vs. Risks of International Sanctions	Unitree products have been exported to dozens of countries worldwide; international media outlets have highlighted their potential military applications; “Made in China 2025” emphasizes global industrial expansion strategies.