Digital Transformation of Security Industry: Connotation, Realistic Dilemma, and Promotion Path-Taking Hikvision as an Example

Yuting Liu
Glasgow International College, Anderson College, 56 Dumbarton Road, Glasgow, G11 6NU, United Kingdom

Abstract: In the era of the digital economy, the security industry is undergoing a critical transition from traditional models to digitalization and intelligent transformation. Taking Hikvision Digital Technology Co., Ltd. as a case study, this paper systematically explores the essence, challenges, and implementation pathways of digital transformation in the security sector. First, it defines the core concept of digital transformation as achieving a shift from equipment manufacturing to intelligent Internet of Things solutions through technological, operational, and organizational innovation. Second, by analyzing Hikvision's practices, it examines real-world challenges in technology research and development, market adaptation, organizational management, and data security. Finally, the study distills successful experiences and proposes transformation pathways applicable to both the security and manufacturing industries. This research contributes to expanding digital transformation theories and provides actionable insights for industry practitioners.

Keywords: Security Industry; Digital Transformation; Hikvision; Smart Internet of Things; Transformation Path

1. Introduction

1.1 Research Background

New-generation information technologies such as big data, artificial intelligence, and the Internet of Things are driving profound transformations in global industries. Consequently, digital transformation has become a key factor for enterprises to enhance competitiveness [1]. The traditional security industry's reliance on video surveillance equipment has become increasingly inadequate to meet the demands of smart security. According to data from the China Security Products Association, the global security market is expected to exceed $500 billion in 2024, with digital and intelligent products and services accounting for over 60%, serving as the core driving force for industry growth [2].

As a leading enterprise in the security industry, Hikvision has evolved from a device manufacturer into a smart Internet of Things solution provider with video-centric capabilities. Its operations span over 150 countries and regions, and it has maintained the top position in the global video surveillance industry for eight consecutive years [3]. Therefore, the company's transformation experience holds significant research value and implications.

1.2 Research Significance

1.2.1 Theoretical significance

On the one hand, this study contributes to enriching the theoretical framework of digital transformation. Existing research predominantly focuses on macro-level perspectives or individual technologies, lacking systematic analysis tailored to the security industry's unique characteristics [4]. By examining the Hikvision case, this study reveals distinctive patterns in industry transformation, thereby addressing gaps in current theoretical frameworks. On the other hand, it explores new pathways for corporate value creation. Through digital transformation, Hikvision has achieved technological breakthroughs and business expansion, offering innovative approaches to corporate value restructuring [5].

1.2.2 Practical significance

First, it provides a reference for the transformation of manufacturing enterprises. Hikvision's successful transition from manufacturing to service-oriented manufacturing offers a model for enhancing value-added and competitiveness in the manufacturing sector [6].

Second, it helps enterprises avoid the risks of

transformation. The company's experience in technology application and market adaptation can guide others in identifying and addressing various risks during the transformation process [7].

Third, it drives technological advancement and structural optimization across the industry. Hikvision's transformation has catalyzed technological progress and healthy competition throughout the sector [8].

1.3 Current Research Status at Home and Abroad

1.3.1 Foreign research

Foreign research began earlier, emphasizing technology-driven and systemic transformation. For instance, Smith and Brown identified information technology as the core driver of transformation [9]. In the security sector, studies predominantly focus on technology applications and security management. For example, Brown et al. explored the role of artificial intelligence in enhancing security efficiency [10], and Miller et al. highlighted the importance of data security and privacy protection [11].

1.3.2 Domestic research

Domestic research has progressed rapidly, with digital transformation widely recognized as a systematic project [1]. Security industry studies frequently integrate corporate practices, as exemplified by Li Gang et al.'s recommendations to enhance technological innovation and business expansion [4]. While research on Hikvision primarily focuses on technological innovation and market strategies [5, 6], systematic analysis of transformation challenges and pathways requires further refinement.

1.4 Research Methods and Technical Approaches

1.4.1 Research methods

Case study method: Based on Hikvision's annual reports, industry reports, and field research, this study analyzes its transformation process and outcomes.

Literature research method: Sorting out relevant literature to clarify the theoretical basis and research direction.

Literature analysis method: Review relevant literature, clarify theoretical basis and research direction.

Descriptive statistical analysis method: By reviewing the annual reports, assess the transformation performance.

1.4.2 Technical approach

The paper follows the framework of "theoretical construction, status analysis, case analysis, problem summary, and path proposal."

First, the theoretical framework of digital transformation in the security industry is established.

Second, the paper analyzes the current situation of the industry and the motivation for transformation.

Third, it examines the motivation, path, and performance of Hikvision's transformation.

Fourth, the paper summarizes the industry's difficulties in technology, market, organization, and data security.

Finally, it proposes promotion pathways to provide references for the industry and policymaking.

2. The Connotation and Driving Factors of Digital Transformation in the Security Industry

2.1 The Connotation of Digital Transformation in the Security Industry

The digital transformation of the security industry is a systematic project, and its core connotation is reflected in profound changes at the technological, business, and organizational levels.

2.1.1 Technology level: From traditional technology to intelligent technology

Digital transformation is driving security technology to evolve from traditional analog surveillance and basic alarm systems to an intelligent framework powered by big data, artificial intelligence, the Internet of Things, and cloud computing. This evolution has transformed security capabilities from passive "seeing" to proactive "understanding and alerting." For instance, artificial intelligence-powered video analysis enables real-time risk detection, Internet of Things technology creates interconnected three-dimensional security systems, while cloud computing provides massive data storage and processing power to support intelligent decision-making.

2.1.2 Business level: Transition from equipment manufacturing to solution provision

Traditional security companies primarily focus on hardware production and sales, with a single business model that often leads to homogeneous price competition. Digital transformation is driving these enterprises to evolve from

standalone equipment manufacturers into comprehensive service providers offering "products + services + solutions." They now provide not only hardware but also tailor-made solutions covering the entire process from design and deployment to operation and maintenance. A prime example is Hikvision, whose smart Internet of Things solutions for urban, transportation, and financial sectors exemplify this business model upgrade.

2.1.3 Organizational level: From traditional hierarchy to flexible digital organization

To meet the heightened demands for agility and collaboration in the digital age, security companies must transform their traditional rigid hierarchical structures. This involves establishing cross-departmental digital transformation teams to enhance collaboration; adopting digital management tools to boost operational and decision-making efficiency; and developing flexible talent mechanisms to attract and cultivate core digital professionals who can drive the transformation.

2.2 Driving Factors of Digital Transformation in the Security Industry

The digital transformation of the security industry is driven by both external environmental factors and internal demands.

2.2.1 External driving factors

Policy support: Governments around the world have placed the digital economy and public security at a strategic level. For example, policy documents such as China's "14th Five-Year Plan for Digital Economy Development" explicitly support the digital transformation of key industries like security, providing clear policy guidance and a favorable environment for industry development [12].

Market demand evolution: Society's need for security is becoming increasingly diversified and sophisticated. From precision management in smart city governance to enterprise safety production and smart home security, there is a growing demand for smarter, more integrated security products and services. This trend is driving companies to undergo digital transformation to meet emerging market needs.

Technology-driven empowerment: The maturation and convergence of next-generation information technologies-such as big data, artificial intelligence, and the Internet of Things-have established a robust technical foundation for the security industry's digital and intelligent transformation. This advancement has not only lowered the barriers to complex applications but also unlocked new business opportunities.

2.2.2 Internal driving factors

Intrinsic need for enterprise development: In the face of intense market competition, digital transformation has become an essential strategy for businesses to seek new growth opportunities and enhance core competitiveness. Through this transformation, companies can strengthen technological innovation capabilities and optimize operational efficiency, thereby expanding market reach, reducing costs, and achieving sustainable growth. Hikvision's performance growth, achieved through sustained research and development investment and supply chain optimization, serves as a prime example.

Existing operational challenges: Traditional equipment manufacturing businesses confront multiple pressures, including shrinking profit margins, intensified homogeneous competition, and rising costs. To break through growth bottlenecks and enhance risk resilience and profitability, security companies must pursue digital transformation to expand services, increase value-added offerings, and achieve a fundamental upgrade in their business models.

3. Practice Analysis of Hikvision's Digital Transformation

3.1 Overview of Hikvision

Founded in 2001, Hangzhou Hikvision Digital Technology Co., Ltd. has evolved from a video surveillance manufacturer into a global leader in intelligent Internet of Things solutions. As of 2024, its operations span over 150 countries and regions, maintaining the top position in the global video surveillance market for eight consecutive years. The company's 2024 revenue exceeded 92.495 billion yuan, with research and development personnel accounting for over 40% of the workforce, and overseas and innovation business revenues making significant contributions [3]. Its systematic transformation journey provides a highly valuable model for studying digital transformation in the security industry.

3.2 The Motivation of Hikvision's Digital Transformation

Hikvision's transformation is driven by both external environmental factors and internal

demands.

External drivers: Firstly, national strategies such as smart cities and the digital economy have created a favorable policy environment. Secondly, market demand has shifted from standalone equipment to comprehensive, intelligent solutions. Moreover, the maturity of technologies like big data and artificial intelligence provides core support for this transformation.

Internal drivers: On one hand, as the traditional equipment market growth has peaked, companies must leverage digital transformation to unlock new growth opportunities, as evidenced by the rapid expansion of their innovative business revenue in 2024. On the other hand, to build sustainable core competitiveness, a comprehensive overhaul is required across technology, products, and business models to break free from homogenized competition.

3.3 The Specific Path of Hikvision's Digital Transformation

Hikvision drives its transformation through a tripartite approach encompassing technology, business, and organizational synergy.

3.3.1 Path of technological innovation: Building an independent and controllable research and development system

With research and development investment as its cornerstone, the company has maintained an average annual growth rate of over 20% in research and development spending over the past five years, with 2024's investment exceeding 15 billion yuan. By deepening industry-academia-research collaboration with top-tier universities and research institutions, it has made breakthroughs in key technologies, including artificial intelligence chips, intelligent algorithms, and big data platforms. For instance, its self-developed artificial intelligence chips have significantly enhanced product computing power and self-reliance, serving as the core driving force for intelligent solutions.

3.3.2 Business transformation path: From hardware sales to solutions and services

Hikvision's core transformation involves transitioning from a device supplier to a smart Internet of Things solutions provider.

Scenario-based solutions expansion: Tailored for urban, transportation, and financial sectors, it delivers integrated solutions combining hardware, software, and data. For instance, its "Smart City Security Brain" system significantly enhances urban management efficiency and emergency response speed through data fusion and analysis.

Service-oriented transformation: The company has vigorously developed value-added services, including operations and maintenance, data analytics, and cloud services, with service revenue steadily increasing. Its "Hikvision Cloud Service Platform" connects a vast number of devices, extending value from product sales to ongoing operations.

Global expansion: The company has deepened its global expansion by establishing localized research and development and supply chain systems, delivering tailored solutions to meet regional demands, and achieving steady growth in overseas market revenue, which has become a key growth driver.

3.3.3 Organizational change path: Building an agile and efficient support system

To ensure the successful implementation of the transformation, Hikvision has made significant adjustments to its organizational structure and management model.

Organizational restructuring: By dismantling departmental silos and forming agile teams for diverse business units, coupled with a dedicated digital transformation office to drive collaboration, the company has dramatically enhanced responsiveness to market shifts.

Digital transformation of management processes: By fully implementing enterprise resource planning and customer relationship management systems, it has digitized production, operations, and customer management, significantly enhancing operational efficiency and product quality.

Talent mechanism innovation: It attracts and retains a large number of digital talents through competitive compensation, equity incentives, and clear career development paths, providing core human capital for transformation.

3.4 Performance Evaluation of Hikvision's Digital Transformation

The transformation has brought comprehensive positive outcomes to Hikvision.

Financial Performance: From 2020 to 2024, the company maintained steady growth in both revenue and net profit, with profitability steadily improving as the proportion of high-value-added businesses increased.

Market Performance: Its global market

leadership has been further consolidated, with market share and influence in key sectors like smart cities continuing to expand.

Technical Performance: The cumulative number of patents has seen a significant increase, and the company has led the development of multiple national and industry standards, with its technical capabilities widely recognized.

4. The Realistic Dilemma of Digital Transformation in the Security Industry

Based on the analysis of Hikvision's case and the overall industry, the security industry faces four major challenges in the process of digital transformation: technology, market, organization, and data.

4.1 Technology Level: Core Technology Dependence and Research and Development Investment Pressure

Despite technological breakthroughs by industry leaders, the security sector remains heavily reliant on external core technologies, particularly in high-end artificial intelligence chips and critical industrial software. This dependency not only drives up production costs but also creates supply chain security risks. Meanwhile, the sustained high-intensity research and development investments required for digital transformation place immense pressure on small and medium-sized enterprises. With limited research and development budgets struggling to support cutting-edge technology development and application, the industry is experiencing increased fragmentation, leaving many companies stuck in low-value-added traditional equipment manufacturing.

4.2 Market Level: Fragmented Demand and Homogeneous Competition

Security application scenarios are highly diverse, ranging from smart cities to small and medium-sized enterprise surveillance systems, with varied demands exhibiting significant fragmentation. This requires enterprises to provide highly customized solutions, substantially increasing research and development, deployment, and operational costs while posing severe challenges to their rapid response and cost control capabilities. On the other hand, in the mid-to-low-end market with relatively low technical barriers, products and services suffer from severe homogenization. Companies are trapped in cutthroat price wars, with profit margins continuously squeezed, making it difficult to accumulate the necessary capital for transformation.

4.3 Organizational Level: Shortage of Digital Talents and Organizational Inertia

The successful transformation of traditional security enterprises urgently requires versatile professionals who master both security operations and digital technologies. However, the industry currently faces a significant talent gap, particularly in high-end fields like artificial intelligence algorithms and big data analytics, which severely hinders technological implementation and innovation. Moreover, the entrenched hierarchical structures and rigid management models prevalent in traditional security firms create strong organizational inertia. Departmental silos, communication barriers, and management's concerns about potential uncertainties from change often impede the adoption of agile, collaborative digital workflows, resulting in sluggish transformation processes.

4.4 Data Level: Security Risks and Governance Challenges

As digitalization advances, security enterprises handle massive sensitive data involving personal privacy and public safety (e.g., video recordings, facial information), making them high-value targets for data breaches and cyberattacks. However, some companies lack adequate data security awareness and capabilities, with weak security frameworks exposing them to severe internal and external risks. Meanwhile, integrating and governing multi-source heterogeneous data poses a significant challenge. Inconsistent data standards and uneven quality hinder effective data fusion and analysis, preventing full utilization of data as a production factor. This directly impacts the efficiency and effectiveness of intelligent solutions.

5. The Promotion Path of Digital Transformation in the Security Industry

Based on the analysis of the connotation, case practice, and realistic dilemma of the transformation, this paper proposes a systematic promotion path for the digital transformation of the security industry from four dimensions: technology, market, organization, and data.

5.1 Technical Level: Strengthening

Independent Innovation and Collaborative Research

Enterprises should prioritize core technology research and development as a strategic priority, achieving breakthroughs through sustained investment to overcome critical bottlenecks. Industry leaders should focus on "chokepoint" areas like high-end artificial intelligence chips and foundational software, striving for self-reliance while proactively sharing technical capabilities to elevate the sector's overall standards. Small and medium-sized enterprises may concentrate on algorithm optimization and product innovation for specific applications, pursuing a "specialized, refined, distinctive, and innovative" development path. At the governmental level, active efforts should be made to establish industry-academia-research collaborative innovation platforms, including forming industry innovation alliances and joint laboratories, to facilitate technology resource sharing and commercialization, thereby shortening the research and development to application cycle.

5.2 Market Level: Deepening Scenario Insights and Differentiated Competition

Enterprises must accurately identify and address fragmented market demands. For the complex needs of governments and large corporations, highly customized end-to-end solutions can be provided. For small and medium-sized enterprises with standardized requirements, modular and configurable product portfolios can be developed to balance customization with cost efficiency. Simultaneously, companies should focus on building differentiated competitive advantages: industry leaders can dominate high-end markets through technological integration capabilities, while small and medium-sized enterprises should specialize in niche sectors (such as community and rural security). By offering scenario-specific, cost-optimized products and services, they can establish localized market advantages and avoid low-level homogeneous competition.

5.3 Organizational Level: Optimization of Talent Structure and Management Model

Addressing the talent shortage requires a dual approach of "attracting and nurturing" talent. Enterprises should strengthen collaboration with universities and vocational institutions to develop customized programs that cultivate interdisciplinary professionals with both industry expertise and digital skills. Simultaneously, they must establish competitive talent acquisition and incentive mechanisms to attract high-caliber professionals. Internally, continuous training systems should be implemented to enhance employees' digital literacy. Organizational management should embrace flat and agile structures, such as forming cross-functional digital transformation teams to break down departmental silos. Management must demonstrate strong commitment to transformation, incorporating its effectiveness into performance evaluations to overcome organizational inertia and ensure strategic execution.

5.4 Data Level: Building a Data System with Equal Emphasis on Security and Governance

Data security is the lifeline of industry development. Enterprises must establish a comprehensive security management system covering the entire data lifecycle, strictly implement data classification, access control, and encrypted transmission, and continuously conduct security risk assessments and compliance audits-particularly when handling sensitive data like personal biometric information. Simultaneously, they should develop a unified data governance framework, establish standardized protocols, integrate fragmented data resources, and enhance data quality and usability. By building an enterprise-level data platform, enterprises can break down information silos, achieve unified data management, analysis, and application, fully unlock the value of data assets, and empower business innovation and intelligent decision-making.

6. Research Conclusions and Prospects

6.1 Research Conclusions

This study takes Hikvision as a typical case to systematically explore the connotation, challenges, and pathways of digital transformation in the security industry, with the following key findings:

First, the digital transformation in the security industry represents a systemic overhaul spanning three dimensions: technology, business, and organizational structures. Technologically, it marks the shift from traditional surveillance to intelligent Internet of Things systems.

Operationally, it involves transitioning from equipment manufacturing to solution delivery. Organizationally, it requires establishing flexible, digitally-driven management models. These three interconnected dimensions collectively form the core essence of this transformation.

Second, the transformation of the industry is driven by external factors such as policy, market demand upgrading, and technology development, as well as internal factors such as enterprises' need to break through growth bottlenecks and build core competitiveness.

Third, Hikvision has achieved effective transformation through a synergistic approach of "technological innovation-business transformation-organizational change." The company has consistently invested in research and development, strengthened industry-academia-research collaboration, and made breakthroughs in core technologies. It has actively expanded its smart Internet of Things solutions and global services, while digitally restructuring its organizational framework and management models, significantly enhancing overall corporate performance.

Fourth, the industry still faces practical difficulties, including dependence on core technologies and the pressure of research and development costs, the fragmentation of market demand and homogenized competition, the shortage of digital talents and organizational inertia, as well as data security risks and insufficient governance capabilities.

Fifth, the transformation should be promoted from four dimensions: strengthening independent innovation and collaborative research in technology, deepening scene insight and implementing differentiated competition in the market, optimizing talent structure and management mode in organization, and constructing a management system with equal emphasis on security and governance in data.

6.2 Limitations and Prospects

6.2.1 Limitations of the study

This study has the following limitations: First, by focusing on Hikvision as a single leading enterprise, its resources and capabilities surpass those of most small and medium-sized enterprises, and the generalizability of the conclusions requires validation across more diverse corporate types. Second, the cited data and circumstances are primarily up to 2024, and with rapid technological advancements, the research findings need continuous updates. Additionally, the study primarily employs qualitative analysis, with evaluations of transformation performance heavily relying on publicly available financial and market data, while the exploration of "intangible" performance metrics such as organizational capabilities and innovation culture remains insufficient.

6.2.2 Future outlook

Future research could be deepened in the following aspects: First, expanding comparative case studies of security enterprises across different scales and specialized sectors to enhance the applicability and precision of conclusions. Second, closely monitoring the impact of emerging trends such as generative artificial intelligence, global supply chain shifts, and data security regulations on industry transformation. Third, adopting more comprehensive quantitative research methods to establish a multi-dimensional performance evaluation system for a holistic assessment of transformation outcomes. Fourth, conducting cross-industry comparative studies to draw lessons from other sectors' transformation experiences, thereby enriching both the theoretical framework and practical applications of digital transformation.

References

[1] Zhang Qi et al. (2023). Digital Transformation and Corporate Competitiveness. Management World.

[2] China Security Products Industry Association. (2024).2024 Global Security Industry Market Analysis Report.

[3] Hikvision Digital Technology Co., Ltd. (2024). Annual Report of Hikvision Digital Technology Co., Ltd. 2024.

[4] Li Gang, et al. (2022). Research on innovative models in the security industry. China Security.

[5] Wang Rui et al. (2023). Hikvision's Technology Innovation and Enterprise Value: A Study. Science and Technology Management Research.

[6] Liu Chang et al. (2024). Analysis of the Path of Service-oriented Transformation in Manufacturing Industry. China Industrial Economy.

[7] Zhao Xin et al. (2023). Risk Identification and Response in Enterprise Digital Transformation. Enterprise Management.

[8] Chen Chen et al. (2024). Research on the Evolution of Industry Competitive Landscape. Economic Research.

[9] Smith, J., & Brown, A.[9] Smith, J., & Brown, A. (2021). The core of digital transformation: Information technology drivers. Harvard Business Review.

[10] Brown, A., et al. (2023). AI applications in security and efficiency enhancement. International Journal of Security Studies.

[11] Miller, K., et al. (2022). Data security and privacy protection in the digital era. Journal of Cybersecurity.

[12] State Council. (2021). "14th Five-Year Plan for Digital Economy Development". Beijing: People's Publishing House.

