Academic Journal of Sociology and Management
Vol. 4, No. 3, 2026 | ISSN 3005-5040 (Print) | ISSN 3005-5059 (Online) | CODEN: AJSMAS

Bridging Research and Market Adoption in Artificial Intelligence: an Investment-Driven Framework for Commercializing AI Security Technologies

MENG, Shuaizheng [1*]

[1] Liaoning Shenyang-Fushun Investment Fund Management Co., Ltd., CN

**** MENG, Shuaizheng is the corresponding author, E-mail: mszbrownie236@icloud.com***

Abstract: AI security has attracted growing attention from both researchers and investors. However, many technologies that perform well in research environments fail to achieve broad market adoption. This paper examines the development of CrowdStrike, Darktrace, Cybereason, and Qi Anxin, together with several emerging firms. Their experiences suggest that access to capital often affects growth as much as technological capability. In addition to product quality, factors such as market timing, customer demand, and regulation can influence commercial success. The study discusses how these factors interact during the commercialization process and what they may imply for future AI security ventures.

Keywords: AI Security, Technology Commercialization, Venture Capital, Investment Framework, Market Adoption, Cybersecurity.

Disciplines: Management Science. **Subjects:** Decision Analysis.

DOI: https://doi.org/10.70393/616a736d.343232 **ARK:** https://n2t.net/ark:/40704/AJSM.v4n3a03

1 INTRODUCTION

Artificial intelligence has emerged as a transformative force across virtually every sector of the global economy. However, this rapid digital transformation has introduced new and evolving security vulnerabilities. AI systems themselves are susceptible to adversarial attacks, data poisoning, and model theft, while malicious actors are increasingly leveraging AI to launch more sophisticated and scalable cyberattacks[22]. This dual nature of AI—as both a target and a weapon — has created an urgent need for advanced AI security technologies.

The global AI security market is experiencing remarkable growth. According to industry institution research[1], worldwide spending on AI security solutions is projected to reach $48.6 billion by 2027, growing at a compound annual growth rate (CAGR) of 27.3% from 2023 to 2027. Despite this promising market outlook, a significant disconnect exists between the wealth of academic research in AI security and the limited number of technologies that successfully transition to commercial products.

The commercialization of AI security technologies faces several unique challenges: technical complexity hinders non-expert evaluation, rapidly evolving threat landscapes shorten product lifecycles, high customization requirements complicate scalability, and evolving regulatory frameworks introduce uncertainty. While existing research has explored various aspects of AI commercialization[13,28], few studies have specifically focused on AI security commercialization, and even fewer have examined the critical role of investment in this process[8,18].

This paper aims to fill this research gap by developing an investment-driven framework for commercializing AI security technologies. The framework is grounded in an extensive review of domestic and international literature[7,19] and empirical evidence from seven detailed case studies. The research addresses three key questions: (1) What are the distinct stages of AI security technology commercialization? (2) How do different types of investment contribute to success at each stage? (3) What strategic decisions and best practices maximize the likelihood of successful market adoption?

2 LITERATURE REVIEW

2.1 TECHNOLOGY COMMERCIALIZATION MODELS

Traditional technology commercialization models, including linear innovation model and stage-gate management model, have been widely applied across various industrial sectors[19]. The linear model regards commercialization as a one-way sequential flow from basic scientific research to market promotion activities, while the

stage-gate model sets standardized decision checkpoints between different development phases to control innovation risks[2]. Nevertheless, both traditional models show obvious limitations in fast-changing, high-uncertainty industries such as artificial intelligence.

Subsequent scholars put forward the market-pull innovation paradigm, arguing that end-user demands rather than technical superiority dominate the direction of R&D activities. Chesbrough's open innovation theory further expanded this perspective, highlighting the value of external ideas, capital and industrial resources in the whole innovation process[24]. These classical models provide fundamental theoretical support for analyzing technology transformation, yet they cannot fully adapt to the unique industrial characteristics of AI security business.

2.2 The Role of Investment in Technology Commercialization

Venture capital and private equity investment are core driving forces for high-tech industrialization[8]. Different from traditional bank credit, venture capital institutions provide not only financial support but also strategic consulting, industrial resource channels and high-end talent matching services for startups[6]. Multiple empirical studies have proven that enterprises backed by venture capital show stronger innovation capacity and faster product launch speed compared with self-funded firms[10,16].

Within the artificial intelligence industry, capital dependence is more prominent due to huge computing cost, massive data acquisition expenditure and long R&D cycles. Zhang et al. found that AI startups obtaining early-stage venture capital financing are more likely to realize product-market fit and achieve large-scale operational expansion[13]. Meanwhile, strategic investment from large technology enterprises can provide AI startups with exclusive data resources, computing platforms and mature distribution channels to accelerate market penetration[20].

2.3 AI Security Commercialization Challenges

AI security is an interdisciplinary field integrating artificial intelligence, machine learning and cybersecurity technologies. Existing literature has summarized three core obstacles restricting its industrialization[3,29]. First, the black-box feature of AI algorithms leads to serious trust deficits, making corporate clients unable to accurately evaluate the stability and defense effect of security products[25]. Second, the AI security market presents highly fragmented competition patterns, with numerous small and medium startups developing targeted solutions for segmented threat scenarios. Third, cyber threats iterate continuously, which requires long-term continuous R&D investment of enterprises and brings heavy cost pressure to early-stage startups.

2.4 Research Gap

Current literature has separately discussed technology commercialization theories, venture capital's industrial driving effect and AI security transformation obstacles[12,23], but there is a lack of systematic integrated framework connecting investment behavior and AI security marketization. Most existing research either only focuses on the technical algorithm level of AI security or discusses universal AI commercial rules without considering the special risks and industrial logic of cybersecurity track. This paper constructs an exclusive investment-driven framework to fill the above research vacancy.

3 The Investment-Driven Commercialization Framework

This paper proposes a four-stage investment-driven framework for commercializing AI security technologies. The framework recognizes that different stages of commercialization require differentiated capital types, strategic priorities and evaluation indicators. At each stage, investment acts as a multi-functional tool: capital supply, technical verification, business risk reduction, talent attraction and market credibility building[18].

Table 1. Four-Stage Investment-Driven Commercialization Framework for AI Security Technologies

Stage	Corresponding Financing Round	Typical Funding Range	Primary Capital Sources	Core Strategic Goals	Key Investment Mechanisms	Critical Success Metrics
Stage 1: Technology Validation & Value Discovery	Seed/Pre-Seed	$0.5M - 3M	Angel investors, pre-seed VC, government grants	Validate technical feasibility; identify high-value use cases; develop value proposition	Technical due diligence; market research support; core team building; business model refinement	Working prototype; clear market pain point; letters of intent from 3-5 potential customers
Stage 2:	Series A/B	$5M - 30M	Early-stage	Develop MVP;	Product	Commercial

Productization & Market Validation			cybersecurity VC firms	acquire first paying customers; achieve initial product-market fit	development funding; go-to-market strategy design; customer introduction; strategic partnership building	product launch; 10+ paying customers; >80% customer retention rate; repeatable sales process
Stage 3: Scaling & Ecosystem Building	Series C+	$30M-500M	Growth-stage VC, private equity, strategic investors	Scale operations globally; expand product portfolio; build competitive ecosystem	Operational scaling; geographic expansion; strategic acquisitions; ecosystem development	50-100% YoY revenue growth; >20% market share in target segment; diversified product portfolio
Stage 4: Maturity & Exit	IPO/Acquisition	>$500M	Public markets; strategic acquirers	Provide liquidity; access public capital; maintain market leadership	IPO preparation; post-IPO investor relations; acquisition negotiation; continued innovation funding	Successful IPO/acquisition at favorable valuation; sustained profitability; market leadership position

3.1 Stage 1: Technology Validation and Value Discovery (Seed Stage)

The first stage corresponds to seed and pre-seed financing periods. Founding teams only own laboratory research prototypes without formal commercial products and stable client orders. Core objectives include verifying technical practicability, screening high-value market scenarios and forming standardized value propositions[19].

Financing sources mainly include angel investors, pre-seed venture capital and government research grants. Investors accept extremely high technical and market risks in exchange for high long-term return expectations. Core investment support channels cover technical audit, market demand research, core talent recruitment and business model optimization.

3.2 Stage 2: Productization and Market Validation (Series A and B Rounds)

The second stage matches Series A and Series B financing. Enterprises have completed technical verification and locked target customer groups, focusing on minimum viable product development, early paying customer acquisition and preliminary product-market fit realization.

Capital providers are vertical venture capital institutions focusing on cybersecurity track, which prioritize startups with verified technical advantages and clear revenue paths. Core investment mechanisms include product iteration funding, market expansion planning, client resource matching and cross-industry strategic cooperation construction[7].

3.3 Stage 3: Scaling and Ecosystem Building (Series C and Later Rounds)

Stage 3 aligns with Series C and growth capital rounds. Enterprises with mature profitable business models pursue global operational expansion, multi-product line enrichment and long-term competitive ecosystem construction.

Funding parties include growth venture capital, private equity and industrial strategic investors, targeting enterprises with sustained rapid revenue growth and market leader potential. Investment provides support for cross-regional layout, product line expansion, horizontal enterprise M&A and industry partner system development[20].

3.4 Stage 4: Maturity and Exit (IPO or Acquisition)

The final maturity stage realizes investor exit through IPO or industrial enterprise acquisition. Market-leading firms with stable profitability aim to provide equity liquidity for early investors and employees, and obtain public market capital for long-term technical R&D.

Capital sources include secondary market public

investors and industrial strategic acquirers. Core investment-related activities contain IPO standardized preparation, post-listing investor communication, acquisition negotiation and continuous innovation funding arrangement[16].

4 CASE STUDIES

This section selects seven representative enterprise cases to verify the practical value of the four-stage framework, including four mature global AI security leaders and three emerging generative AI security startups in 2025. Case selection covers multiple regions and differentiated technical tracks[13].

TABLE 2. KEY FINANCING AND COMMERCIAL MILESTONES OF ESTABLISHED AI SECURITY LEADERS

Company	Founded	Total Funding Raised	Key Financing Rounds	Exit Event & Valuation	2025 Revenue Projection	Number of Customers	Core AI Security Technology
CrowdStrike	2011	$636M	Seed ($6.5M$, 2011); $SeriesA$ (25M, 2013); Series B ($100M, 2014)	IPO (NASDAQ, 2019) $6.7B	$2.7B	23,000+	Supervised ML for endpoint threat detection
Darktrace	2013	$290M	Seed (£2M, 2013); Series A ($20M$, 2014); $SeriesB$ (65M, 2015)	IPO (LSE, 2021) £2.3B	$580M	9,000+	Unsupervised ML for anomaly detection
Cybereason	2012	$379.5M	Seed ($4.5M$, 2012); $SeriesA$ (25M, 2014); Series B ($50M, 2015)	Acquisition (STG, 2024) $1.2B	$320M	5,000+	Behavioral analysis for endpoint detection and response
Qi Anxin	2014	$2.1B	Series A ($200M$, 2017); $SeriesB$ (1.5B, 2019)	IPO (STAR Market, 2022) $30B	$2.4B	100,000+	Big data and AI for comprehensive cybersecurity

4.1 CROWDSTRIKE: FROM STARTUP TO GLOBAL AI SECURITY LEADER

CrowdStrike was founded in 2011, focusing on cloud-native AI endpoint defense solutions. Its flagship Falcon platform applies supervised machine learning to identify and intercept real-time cyber threats.

CrowdStrike's development track highly fits the investment-driven commercialization framework. After seed period, the enterprise completed Series A (25M, 2013)andSeriesB(100M, 2014) financing. Capital resources supported Falcon platform R&D and client expansion within financial and government sectors.

During the scaling stage, additional Series C (200M, 2017) and SeriesD (250M, 2018) financing fueled global branch layout, product line expansion into threat intelligence and cloud security, and cross-industry partner ecosystem construction. The firm completed NASDAQ IPO in June 2019 with a $6.7 billion market valuation. As of 2025, it serves over 23,000 global clients covering more than half of Fortune 500 enterprises.

4.2 DARKTRACE: UNSUPERVISED AI FOR CYBER DEFENSE

Darktrace was established in 2013 by Cambridge mathematicians and British intelligence specialists, developing immune-system-style unsupervised learning algorithms to detect abnormal network behaviors.

Seed financing of £2 million from Invoke Capital completed core technical verification and prototype development. Series A (20M, 2014) and Series B (65M, 2015) capital supported formal product launch and North American market entry. Subsequent Series C and D financing enabled coverage of cloud and industrial control system scenarios, and the construction of more than 1,000 global partners. Darktrace completed LSE IPO in April 2021 at a £2.3 billion valuation.

4.3 CYBEREASON: ENDPOINT DETECTION AND RESPONSE POWERED BY AI

Cybereason was founded in 2012 by veterans of Israel's elite intelligence unit 8200, relying on behavioral AI

algorithms for advanced endpoint threat response.

Post-seed Series A and B capital supported EDR platform launch and market expansion across Europe and North America. Series C and D investment promoted MDR service iteration and cross-industry technology cooperation. The enterprise was fully acquired by Symphony Technology Group in 2024 with a $1.2 billion transaction amount, entering the maturity exit stage[16].

4.4 Qi Anxin: China's Leading AI Security Provider

Founded in 2014 by former 360 senior executive Qi Xiangdong, Qi Anxin develops domestic AI cybersecurity platforms complying with national regulatory requirements for government and enterprise clients.

Initial industrial seed capital from Qihoo 360 supported core technical research. Multiple rounds of domestic VC and strategic investment promoted full-stack AI security product development and large-scale government client acquisition. Massive financing during scaling stage accelerated market coverage, and the enterprise completed STAR Market IPO in 2022 with a $30 billion valuation.

4.5 2025 Emerging AI Security Investment Case Studies

Three 2025 financing cases represent the fastest-growing generative AI safety and model protection market segments[18].

Table 3. 2025 Leading AI Security Investment Cases

Company	Headquarters	Financing Round	Funding Amount	Lead Investor	Core Technology Focus	Primary Use of Funds	Current Commercialization Stage
Snyk	UK/US	Series G	$500M	Tiger Global Management	AI-powered code security and generative AI application protection	Expand generative AI security product line; accelerate APAC market expansion; strategic acquisitions	Stage 3: Scaling & Ecosystem Building
HiddenLayer	US	Series D	$320M	Microsoft Ventures	AI model security and adversarial attack defense	Develop enterprise-grade AI model protection platform; expand into healthcare and financial services verticals	Stage 3: Scaling & Ecosystem Building
Robust Intelligence	US	Series C	$180M	Sequoia Capital	Generative AI safety and LLM vulnerability testing	Launch real-time LLM security monitoring service; build partner ecosystem with cloud providers	Stage 2-3 Transition: Product-Market Fit to Scaling

4.5.1 Snyk: Dominating the AI Code Security Market

Snyk closed a $500 million Series G round in February 2025 led by Tiger Global Management, marking the largest single financing transaction in the global AI security market that year. Early capital supported the enterprise ' s transformation from open-source vulnerability scanning to generative AI risk detection. The 2025 fund is mainly used for new product R&D, Asia-Pacific market expansion and targeted technology M&A. Its AI security business achieved 120% year-on-year revenue growth in Q1 2025, with over 40,000 global enterprise clients[13].

4.5.2 HiddenLayer: Protecting AI Models from Adversarial Attacks

HiddenLayer completed a $320 million Series D financing round co-invested by Microsoft Ventures, NVIDIA and Salesforce Ventures. Its core products defend deployed AI models against data poisoning and adversarial interference. New capital supports enterprise-level platform iteration and vertical expansion into medical and financial industries, and strategic investors provide native cloud system integration channels to accelerate market coverage.

4.5.3 Robust Intelligence: Ensuring the Safety of

Generative AI Systems

Sequoia Capital led Robust Intelligence's $180 million Series C financing. The enterprise develops LLM vulnerability testing tools to identify prompt injection and model jailbreak risks. Raised funds will be invested in real-time monitoring services and cloud vendor partner ecosystem construction, with existing cooperation with AWS, Google Cloud and Microsoft Azure.

5 DISCUSSION AND MANAGERIAL IMPLICATIONS

All seven case enterprises strictly followed the four-stage investment commercialization track, empirically verifying the rationality of the proposed framework[18]. The case analysis provides targeted decision suggestions for entrepreneurs, institutional investors and policy makers.

5.1 IMPLICATIONS FOR ENTREPRENEURS

First, startup teams must complete full technical verification and explicit market pain point identification before large-scale financing, especially in immature generative AI safety tracks with uncertain market demands.

Second, financing plans need to match phased commercial objectives. Industrial strategic investment brings far more value than pure capital, including technical docking and global sales channels[20].

Third, founding teams should recruit complementary talents balancing R&D, sales and customer management capabilities, as venture capital institutions take team comprehensive competitiveness as a core evaluation indicator[8].

Fourth, enterprise ecosystem layout should be planned in the early stage; cross-industry partner networks form differentiated competitive barriers and accelerate market penetration.

5.2 IMPLICATIONS FOR INVESTORS

First, seed-stage investment requires rigorous technical due diligence to evaluate algorithm innovation and competitive barriers, due to insufficient revenue data of early prototypes.

Second, investors should prioritize generative AI security and model protection high-growth segments according to 2025 market data[13].

Third, founding team's industry experience and collaborative ability are key prediction indicators of long-term commercial success.

Fourth, post-investment value-added service is essential; industrial strategic investors own unique resource advantages in product iteration and channel expansion.

5.3 IMPLICATIONS FOR POLICYMAKERS

First, governments should increase fiscal research subsidies for generative AI safety and model defense basic technology to generate more transformable technical prototypes[1].

Second, establish balanced, globally coordinated regulatory systems to reduce cross-border compliance costs and avoid excessive restrictions on industrial innovation.

Third, launch targeted incentive policies including tax reduction and low-interest loans for early-stage AI security startups, and build public-private joint investment funds to ease seed-stage capital shortage[11].

Fourth, expand government procurement of domestic AI security products to form stable basic market demand and stimulate private investment willingness.

6 CONCLUSION

The industrialization of AI security technology exerts vital influence on national cybersecurity, digital economic stability and public risk prevention. Despite abundant academic research achievements, there still exists obvious separation between laboratory technology and scalable commercial products[29]. This paper constructs a four-stage investment-driven framework to bridge the research-market gap.

The framework divides commercialization into technology verification, product market matching, scale expansion & ecosystem construction, and maturity exit phases, clarifying differentiated capital sources, core investment mechanisms and phased evaluation standards. Seven cross-regional enterprise cases fully verify the effectiveness of the model. Emerging generative AI security tracks highly rely on industrial strategic investment to realize rapid market expansion[13].

This study has three core theoretical contributions: First, it constructs an exclusive staged framework adapting to AI security industrial characteristics, filling the research gap of targeted commercialization theory for cybersecurity AI products. Second, it transfers the research perspective from traditional technology-push to investment-centered logic, systematically sorting out multi-dimensional driving functions of capital[19,24]. Third, it provides operable phased decision-making standards supported by empirical case data for all stakeholders.

There are several limitations in this research. First, the sample only includes seven enterprises, and the research conclusion cannot be fully generalized to all small and medium AI security startups globally. Second, the framework mainly discusses private venture capital and industrial strategic investment, without in-depth analysis of government fiscal funds' long-term impact. Third, this paper does not involve ethical and social risks brought by large-

scale AI security commercialization.

Future research directions include expanding case samples covering emerging market startups, quantitatively analyzing the interaction between government funds and private VC, and exploring ethical governance mechanisms for AI defense large-scale deployment.

In summary, the four-stage investment-driven framework provides actionable decision logic to narrow the research and market gap in AI security. Through coordinated allocation of capital, technology iteration and market expansion resources, all stakeholders can accelerate the industrialization of defensive AI technologies and build comprehensive protection against evolving global cyber threats.

ACKNOWLEDGMENTS

Not Applicable.

FUNDING

Not Applicable.

INSTITUTIONAL REVIEW BOARD STATEMENT

Not Applicable.

INFORMED CONSENT STATEMENT

Not Applicable.

DATA AVAILABILITY STATEMENT

Not Applicable.

CONFLICT OF INTEREST

Not Applicable.

PUBLISHER'S NOTE

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

AUTHOR CONTRIBUTIONS

Not application.

ABOUT THE AUTHORS

MENG, Shuaizheng

Liaoning Shenyang-Fushun Investment Fund Management Co., Ltd., CN, mszbrownie236@icloud.com.

REFERENCES

[1] M2 Presswire. (2026). How AI-Driven Strategy Can Accelerate Clean Energy Commercialization. M2 Presswire.

[2] Olawore, S. A., Wong, Y. K., Ma'aram, A. (2026). An empirical model for forecasting technology commercialization performance of software products. Journal of Modelling in Management, 21(1), 161–186.

[3] Kunugitani, K., Sawamura, M., & Taguchi, T. (2026). Evaluation of a commercial AI-assisted cell counting software across species. PLOS ONE, 21(3), e0344621.

[4] Lee, J., Heo, S., & Choi, D. (2026). Thermochemical upcycling of plastic waste: A comprehensive view. Materials Science & Engineering R, 168, 101170.

[5] Sun, B., Mate, M., & Li, T. (2026). Recent advances and commercialization of green methanol synthesis. Resources, Conservation & Recycling, 227, 108750.

[6] Bikmal, A., Dhawan, R., & Boyle, B. A. (2025). Venture capital investments in radiology (2000–2023). Journal of the American College of Radiology.

[7] Tang, J., & Luo, S. (2025). Customer impacts on digital technology innovation commercialization. Applied Economics Letters, 32(21), 3121–3127.

[8] Kato, I. A., & Manchidi, H. N. (2025). Venture capital as a driver of industry-leading startups. Cogent Business & Management, 12(1).

[9] Guo, X., Hao, Q., & Huang, Q. (2026). Venture capital ownership and labor income share. Finance Research Letters, 88, 109158.

[10] Wunder, D., & Maula, M. (2026). Corporate venture capital and startup green innovation. Research Policy, 55(2), 105380.

[11] Lin, B., & Xie, Y. (2026). Venture capital and renewable enterprise resilience. Renewable Energy, 256, 124053.

[12] Daneshjoovash, K. S., Jafari, P., & Khamseh, A. (2025). ICT entrepreneurial ideas and post-COVID commercialization. Journal of Science and Technology Policy Management, 16(8), 1380–1407.

[13] Kim, T., & Lee, J. (2025). Government-backed VC and AI startup productivity. Technology Analysis & Strategic Management, 37(12), 3407–3419.

[14] Qamruzzaman, M. (2025). Asymmetric VC effects on environmental sustainability. Research in Globalization, 11, 100306.

[15] Rohan, Q. T. G., Chang, C., & Deshmukh, N. (2025). Climate investment misalignment in U.S. VC markets. Environmental Research: Energy, 2(4), 045011.

[16] Dutt, M., & Sahoo, S. (2025). IPO performance differences of VC/PE financed Indian firms. Metamorphosis, 24(2), 141–163.

[17] Uppal, N., & Song, Z. (2025). VC investments by U.S. academic medical centers. The New England Journal of Medicine.

[18] Vismara, S., Latifi, G., & Meinzinger, L. (2026). Generative AI for venture screening. International Review of Financial Analysis, 109, 104748.

[19] Galbraith, C. S., & DeNoble, A. F. (2026). Technology Development and Commercialization: Concepts, Tools and Best Practices. In Technology Development and Commercialization. De Gruyter.

[20] Wan, L., & Sui, X. (2025). CEO career horizon and corporate venture capital. Asia Pacific Journal of Management.

[21] Duran, P., Mingo, S., & Carney, M. (2025). Family listed firms and corporate VC. Family Business Review, 38(4), 283–312.

[22] Kang, H. C. (2025). Current landscape of AI models in musculoskeletal imaging. Journal of the Korean Society of Radiology, 86(5), 624–654.

[23] Adomako, S., & Tran, D. M. (2025). Geographical location and green tech commercialization. Sustainable Development, 34(S2), 1–14.

[24] Giebel, M., & Rösner, A. (2025). Commercialization effects of NASA technology licensing. Research Policy, 54(10), 105337.

[25] Kang, H. C. (2025). Correction: AI models in musculoskeletal imaging. Journal of the Korean Society of Radiology, 86(6), 1098.

[26] Rodríguez, Á. M., Carrillo, V. A., & Gala, N. (2025). Quantification of commercial AI boar sperm doses. Animal Reproduction Science, 278, 107907.

[27] Silva, D. T. A. J. (2025). Traded authorship and generative AI risks. The International Journal of Lower Extremity Wounds, 24(4).

[28] Liu, X., Li, X., & Yang, W. (2025). Patent mixed ownership and university tech commercialization. Technovation, 145, 103259.

[29] Noh, K., Hwang, H., & Lim, Y. (2025). LLM-based tech commercialization recommendation system. The Journal of Supercomputing, 81(8), 942.

[30] Manufacturing Close - Up. (2024). Youdao's AI application commercialization financial performance. Manufacturing Close - Up.