Business and Economic Frontiers
Volume 1, Issue 1, Mei 2026
E-ISSN : xxx-xxxx

Digital-State Capacity, AI Governance, and SME Transformation: Comparative Business Systems Evidence from Singapore and Estonia

Julienn Moreau[1]

Julienn Moreau
Department of Management and Technology
École Polytechnique Fédérale de Lausanne
Email: julienn.moreau@epfl.ch

***Corresponding Author:** julienn.moreau@epfl.ch

Citation: Aziz (2026). Digital-State Capacity, AI Governance, and SME Transformation: Comparative Business Systems Evidence from Singapore and Estonia (Book Antiqua 14pt Bold). *Journal of Advanced Research and Studies in Law*, *10*(4), xx–xx. https://doi.org/0000-0000

Published: 21/05/2026

ABSTRACT

This article examines how digital-state capacity shapes AI governance, SME transformation, market trust, economic performance, and sustainable socio-economic development. Using a comparative institutional case study of Singapore and Estonia, the study argues that AI-enabled business transformation depends not only on firm-level technology adoption but also on the quality of digital public infrastructure, regulatory coordination, institutional trust, human-capital systems, and public-private implementation capacity. Singapore represents a strategic developmental digital economy in which the state actively coordinates AI governance, enterprise digitalization, cybersecurity, industrial upgrading, and global digital competitiveness. Estonia represents a digitally embedded institutional state in which secure identity, data interoperability, e-government, digital public services, and civic trust form the foundations of business efficiency and administrative resilience. The findings reveal that Singapore is stronger in strategic industrial scaling, AI commercialization, SME capability-building, and global digital economy positioning, while Estonia is stronger in interoperable public infrastructure, digital administrative legitimacy, and state-business transaction efficiency. However, both cases face implementation constraints: Singapore must prevent AI adoption from reinforcing firm-size inequality and compliance asymmetry, while Estonia must overcome SME digitalization gaps, connectivity constraints, and productivity convergence challenges. This article contributes to comparative business systems, digital economy governance, AI policy, and sustainable

development scholarship by developing theoretical propositions on digital-state capacity, trusted interoperability, adaptive AI governance, and inclusive business-system transformation.

Keywords: digital-state capacity; artificial intelligence; SME transformation; Singapore; Estonia; digital public infrastructure; AI governance; market trust; institutional transformation; sustainable development

INTRODUCTION

Digital transformation has become a central frontier of international business, economic governance, and sustainable development. Artificial intelligence, cloud computing, cybersecurity, digital identity, interoperable data systems, e-government platforms, and enterprise digitalization increasingly determine how firms compete, how states deliver services, how markets generate trust, and how societies manage productivity, inclusion, and resilience. Unlike earlier periods of information technology diffusion, the current phase of digital transformation is not confined to the adoption of software or automation inside firms. It involves the reorganization of institutional infrastructures through which businesses interact with governments, workers, customers, regulators, financial systems, and global markets. This article argues that the core determinant of successful AI-enabled business transformation is not technology availability alone but digital-state capacity: the ability of public institutions to coordinate infrastructure, regulation, skills, trust, cybersecurity, innovation, and enterprise adoption in ways that generate sustainable economic value.

The global context makes this issue theoretically and practically urgent. The OECD Digital Economy Outlook shows that the ICT sector has grown substantially faster than the wider economy across advanced economies, while AI adoption is reshaping production, services, knowledge work, and public administration (OECD, 2024). At the same time, the World Bank and UNCTAD emphasize that digital infrastructure can support productivity, inclusion, and service delivery only when accompanied by governance safeguards, data protection, cybersecurity, human capability, and environmental responsibility (UNCTAD, 2024; World Bank, 2025). Digitalization therefore presents a dual institutional problem. On the one hand, it can reduce transaction costs, expand market participation, improve government efficiency, and support innovation. On the other hand, it can increase surveillance risks, platform concentration, cyber vulnerability, algorithmic opacity, inequality between large and small firms, and environmental pressures from data centres and digital devices.

Singapore and Estonia provide analytically rich comparative cases because both are small, open, high-income digital economies that have used state capacity to overcome scale constraints. Yet their institutional pathways differ substantially. Singapore is a city-state with a strategic developmental governance model, strong public-sector coordination, a globally connected business environment, and deliberate positioning as a trusted digital and AI hub. Its digital economy accounted for 18.6% of GDP in 2024, up from 14.9% in 2019, while SME AI adoption more than tripled from 4.2% in 2023 to 14.5% in 2024; non-SME AI adoption reached 62.5% in 2024 (IMDA, 2025). These indicators show a rapidly expanding digital business system, but also reveal significant firm-size asymmetry in AI diffusion.

Estonia represents a different digital-state model. Its digital transformation is grounded in secure electronic identity, the X-Road data exchange architecture, online public services, digital signatures, e-residency, cybersecurity preparedness, and a long-standing institutional commitment to interoperability. Estonia's Digital Agenda 2030 seeks to advance the economy, state, and society through digital technology, with the stated aim of strengthening the country's digital society and ensuring high-quality digital experience for citizens and businesses (Ministry of Justice and Digital Affairs, 2025). The European Commission's 2025 Digital Decade country report identifies Estonia as a leader in digital public services and notes that it has already achieved full access to e-health records, while still lagging the EU average in connectivity and SME digitalization (European Commission, 2025a).

The academic and policy problem addressed in this study is that scholarship on AI and digital transformation often remains divided across disconnected literatures. Strategic management research focuses on firm-level dynamic capabilities, business model innovation, and organizational transformation (Teece, 2007; Warner & Wäger, 2019). Innovation studies examine national innovation systems, policy instruments, and digital technology diffusion (Edler & Fagerberg, 2017; Mazzucato, 2021). Institutional economics explains how rules, norms, and governance structures reduce uncertainty and shape incentives (North, 1990; Williamson, 1985). Comparative capitalism analyzes how different business systems organize finance, labour, skills, corporate governance, and inter-firm coordination (Hall & Soskice, 2001; Whitley, 1999). Digital government research examines public service modernization, administrative data systems, and citizen trust (Mergel et al., 2019; OECD, 2025a). However, existing scholarship has not sufficiently integrated these perspectives to explain how digital-state capacity shapes AI-enabled business transformation across firms, markets, and institutions.

The literature reveals several unresolved debates. While previous studies emphasize that AI can improve productivity through automation, prediction, and decision support, they often understate the institutional conditions needed for adoption, trust, and diffusion (Brynjolfsson et al., 2021; Filippucci et al., 2024). Other scholars argue that digital public infrastructure can improve state capacity and market inclusion, but less attention has been given to how these infrastructures affect SME competitiveness and business-system transformation (World Bank, 2025). Platform-economy research highlights network effects and digital market power, yet small digital states such as Singapore and Estonia show that public institutions can shape market architectures through standards, identity systems, cybersecurity frameworks, and trust infrastructures (Cusumano et al., 2019; Kenney & Zysman, 2020). Existing literature remains limited in explaining how AI governance, digital public services, enterprise digitalization, institutional trust, and sustainable competitiveness interact within comparative business systems.

The research gap is therefore sixfold. First, the theoretical gap concerns insufficient integration of business systems theory, digital-state capacity, AI governance, and sustainable development. Second, the empirical gap concerns limited comparative evidence on how small advanced economies translate digital policy into business transformation. Third, the comparative institutional gap concerns why Singapore and Estonia, despite both being digital leaders, generate different mechanisms of market trust, enterprise

upgrading, and state-business coordination. Fourth, the business implementation gap concerns how SMEs absorb AI and digital tools when they face constraints in finance, skills, cybersecurity, and managerial capacity. Fifth, the policy coordination gap concerns how governments align digital infrastructure, AI regulation, workforce development, cybersecurity, competition policy, and sustainability goals. Sixth, the economic sustainability gap concerns whether digital transformation improves broad-based socio-economic resilience or merely deepens technological asymmetries between frontier firms and lagging firms.

This article's novelty lies in conceptualizing digital-state capacity as a central institutional determinant of AI-enabled business transformation. It argues that digital transformation is neither a purely firm-driven nor purely technology-driven process. Rather, it is mediated by institutional infrastructures that shape how firms access data, verify identity, transact with the state, comply with regulation, adopt AI safely, protect themselves from cyber threats, and develop workforce capabilities. Singapore and Estonia are selected because they both demonstrate strong digital-state capacity, but through different institutional logics. Singapore uses strategic policy orchestration to scale enterprise adoption, AI governance, and global digital competitiveness. Estonia uses interoperable public infrastructure and digital administrative trust to reduce transaction costs and embed digital practices into everyday economic life.

The analytical framework of the article links institutional structures → digital-state capacity → AI and enterprise implementation → business-system performance → sustainable socio-economic development. Institutional structures shape the credibility, interoperability, and inclusiveness of digital systems. Digital-state capacity translates these structures into public infrastructure, regulatory frameworks, skills programs, and adoption incentives. AI and enterprise implementation determine whether firms convert digital tools into productivity, resilience, and innovation. Business-system performance emerges through competitiveness, SME upgrading, market trust, and public-private efficiency. Sustainable socio-economic development occurs only when digital transformation supports inclusion, security, human capability, environmental responsibility, and institutional legitimacy.

The research objective is to explain how Singapore and Estonia use different institutional architectures of digital-state capacity to govern AI-enabled business transformation, and what this comparison reveals about the conditions under which digital economies generate sustainable competitiveness and socio-economic development.

METHODOLOGY

This study employs a comparative institutional business systems methodology integrating digital economy analysis, AI governance analysis, and political economy interpretation. Singapore and Estonia are selected through a most-similar and most-different comparative logic. They are similar in being small, open, high-income, digitally advanced economies with strong public-sector modernization agendas and limited domestic market scale. They are different in institutional history, geographic location, regulatory embeddedness, business-system structure, public administration model, and regional economic context.

Singapore is analyzed as a strategic developmental digital economy characterized by centralized policy coordination, strong state-business alignment, global investment attraction, AI governance experimentation, and enterprise capability-building. Estonia is analyzed as a digitally embedded institutional state characterized by interoperable data exchange, secure electronic identity, digital public services, cybersecurity orientation, and administrative trust. This design allows the study to identify how different institutional architectures shape business implementation, market confidence, SME transformation, and sustainable economic outcomes.

The empirical basis consists of triangulated secondary data from official policy documents, international datasets, and peer-reviewed literature. The analysis draws on IMDA's Singapore Digital Economy Report, Singapore's National AI Strategy and Digital Enterprise Blueprint, Singapore's AI governance frameworks, Estonia's Digital Agenda 2030, European Commission Digital Decade reporting, OECD economic and digital government reports, World Bank and UNCTAD digital economy sources, WIPO innovation indicators, and academic research on institutions, dynamic capabilities, platform governance, digital government, SME digitalization, and sustainable transformation. The analytical method uses structured focused comparison, mechanism-based institutional interpretation, and cross-case mapping of variables including digital public infrastructure, AI governance, SME adoption, cybersecurity, innovation capacity, business environment, administrative trust, digital inclusion, and sustainability alignment. Reliability is strengthened by comparing multiple official and multilateral sources, distinguishing empirical evidence from analytical inference, and applying the same variables to both cases. No interview data are used, and no respondent quotations are fabricated. The main limitation is that the study does not estimate econometric treatment effects; its contribution is explanatory and theory-building, appropriate for identifying causal mechanisms and developing propositions for future empirical research.

Findings and Discussion

1. Digital-State Capacity and Institutional Architecture: Strategic Orchestration versus Embedded Interoperability

The first finding is that Singapore and Estonia demonstrate two distinct institutional models of digital-state capacity. Singapore's model is based on strategic orchestration. The state coordinates digital policy through national strategies, regulatory experimentation, enterprise capability programs, public-private partnerships, talent investments, and global digital positioning. Singapore's National AI Strategy 2.0, launched in 2023, emphasizes AI for the public good, national capability-building, and global competitiveness; the establishment of a National AI Council in 2026 further institutionalized high-level strategic direction for AI policy (Smart Nation Singapore, 2026). This reflects a governance model in which the state does not merely regulate technology markets but actively shapes the conditions under which firms, workers, researchers, and global investors adopt AI.

Estonia's model is based on embedded interoperability. Its digital-state capacity has developed through long-term investments in digital identity, secure data exchange, digital signatures, online services, and administrative integration. Estonia's Digital Agenda 2030 frames digital technology as a mechanism for advancing the economy, state, and society, while emphasizing universal access, digital government quality, and environmentally friendly digital practices (Ministry of Justice and Digital Affairs, 2025). Unlike Singapore's strategic scaling model, Estonia's core advantage lies in the routine institutionalization of digital interaction. Businesses, citizens, and public agencies operate within a governance environment where digital verification, data exchange, and public-service access are normalized.

The comparison reveals that digital-state capacity is not synonymous with technological sophistication. It is the institutional ability to make digital systems reliable, trusted, usable, and economically productive. Singapore's digital-state capacity operates through forward-looking policy coordination and targeted ecosystem development. Estonia's digital-state capacity operates through legal-technical infrastructure and administrative legitimacy. Both models reduce uncertainty, but they do so differently. Singapore reduces uncertainty by providing strategic direction, governance frameworks, adoption programs, and state-backed assurance. Estonia reduces uncertainty by embedding digital trust in public infrastructure, identity systems, and interoperable databases.

Institutional economics helps explain this divergence. North (1990) argues that institutions structure incentives by reducing uncertainty in exchange. In digital economies, uncertainty includes authentication risk, data misuse, cyber vulnerability, regulatory ambiguity, AI opacity, and interoperability failure. Singapore addresses these uncertainties through adaptive governance frameworks and public-private coordination. Estonia addresses them through a stable digital infrastructure that reduces transaction frictions between firms and the state. Williamson's (1985) transaction-cost theory is also relevant: digital public infrastructure reduces administrative and compliance costs, but the form of transaction-cost reduction differs. Singapore reduces costs by helping firms adopt digital and AI tools; Estonia reduces costs by making public administration digitally frictionless.

The business-system implications are substantial. In Singapore, firms benefit from a dense ecosystem of grants, frameworks, standards, sandboxes, public-private partnerships, and global digital networks. This environment is particularly advantageous for digitally ambitious firms seeking to scale regionally. However, firms with limited managerial capacity may struggle to navigate increasingly sophisticated digital and AI programs. In Estonia, businesses benefit from low administrative friction, digital company formation, e-services, and efficient state interaction. However, firms outside the advanced ICT sector may still lag in deep digital adoption, innovation investment, and international scale.

This finding extends comparative business systems theory. Hall and Soskice (2001) emphasize institutional complementarities in finance, labour, corporate governance, and coordination. The Singapore–Estonia comparison suggests that digital public infrastructure should be treated as a new institutional complementarity. It shapes how firms interact with regulators, access services, comply with obligations,

build trust, adopt AI, and participate in digital markets. Digital-state capacity is therefore not external to business systems; it is part of the institutional architecture of competitiveness.

2. AI Governance, Market Trust, and Responsible Innovation

The second finding is that AI governance functions as a market-trust infrastructure. Singapore has deliberately positioned itself as a trusted AI governance hub. Its Model AI Governance Framework, AI Verify testing toolkit, and 2024 Model AI Governance Framework for Generative AI attempt to translate broad ethical principles into practical organizational governance, testing, assurance, incident reporting, content provenance, security, and user literacy (IMDA & AI Verify Foundation, 2024). This approach reflects Singapore's preference for adaptive and pragmatic governance: rather than imposing rigid restrictions at the earliest stage, it develops frameworks, toolkits, sandboxes, and assurance mechanisms that encourage adoption while managing risks.

Estonia's AI governance is embedded in its broader digital-government architecture. The national AI strategy, known as the Kratt strategy, seeks to advance AI adoption in both the public and private sectors, strengthen skills and research, and develop an enabling legal environment (OECD.AI, 2025). Estonia's AI orientation is strongly linked to public-service modernization, including AI-enabled assistance and service simplification. Its governance challenge is less about becoming a global AI hub and more about integrating AI into an already highly digital state without weakening transparency, citizen trust, or cybersecurity.

The cross-case comparison shows that AI governance must be evaluated by its institutional function rather than by the existence of policy documents alone. Singapore's AI governance framework supports business confidence by giving firms practical guidance on responsible deployment. This matters because firms often hesitate to adopt AI when legal liability, data governance, explainability, and reputational risks are unclear. Estonia's AI governance supports public-sector modernization by embedding AI into a trusted digital government context. This matters because public-sector AI adoption can improve service quality, but only if citizens trust how data are used and decisions are made.

Theoretical linkage to platform governance and innovation policy is important. AI systems produce value through data, models, computation, organizational use, and market trust. If trust fails, adoption slows or becomes socially contested. If regulation is too rigid, innovation may be constrained. If governance is too weak, firms may deploy unsafe or discriminatory systems. Singapore attempts to solve this through practical assurance and voluntary-to-adaptive governance. Estonia attempts to solve this through digital institutional trust and public-sector integration. Both models show that responsible innovation is not merely a normative goal; it is a condition of market development.

The comparison also reveals different risks. Singapore's flexible AI governance can encourage experimentation, but voluntary frameworks may be insufficient if firms deploy high-risk systems without adequate accountability. Large firms may have the resources to implement AI assurance, while SMEs may lack compliance capability. Estonia's public-service AI integration can improve administrative efficiency,

but it depends heavily on cybersecurity, data quality, and legitimacy. A highly digital state may become vulnerable if citizens perceive automated public services as opaque or if cyber threats undermine confidence.

This finding contributes to AI governance scholarship by demonstrating that governance models must align with business systems. Singapore's governance is industry-facing, international, and adoption-oriented. Estonia's governance is state-infrastructure-facing, civic, and service-oriented. Both models differ from the European Union's more formal risk-based AI Act approach and from the United States' more decentralized market-led approach. The cases therefore show that small states can exercise digital governance influence by specializing in trust, interoperability, and policy agility.

For business strategy, firms should treat AI governance as a competitive capability. Firms that can document responsible AI use, protect data, audit models, train workers, and explain algorithmic decisions are more likely to gain customer and regulator trust. For public policy, AI governance should be designed as an enabling infrastructure for safe adoption rather than merely as a compliance burden. The policy challenge is to make responsible AI usable for SMEs, not only for large corporations with legal and technical teams.

3. SME Digitalization, Productivity, and Business-System Transformation

The third finding is that SME transformation is the decisive test of digital economy inclusiveness. Singapore's digital economy has expanded rapidly, but adoption gaps remain. IMDA reported that SMEs' AI adoption rate more than tripled in one year, reaching 14.5% in 2024, while non-SME AI adoption reached 62.5%. This gap indicates that Singapore's frontier digital performance coexists with significant differences in organizational capability by firm size (IMDA, 2025). The Digital Enterprise Blueprint addresses this challenge through four focus areas: helping firms become smarter through AI-enabled solutions, scale faster through integrated digital solutions, become safer through cyber resilience, and upskill workers for digital capabilities (MDDI, 2024).

The Singapore case shows how strategic policy attempts to turn digital transformation from an elite-firm phenomenon into a broader business-system process. IMDA expects 15,000 SMEs to benefit from AI-enabled solutions under the SMEs Go Digital programme, while digitally mature SMEs are targeted through GenAI initiatives and partnerships with technology companies (IMDA, 2024). This policy architecture recognizes that SMEs rarely adopt AI through spontaneous market forces alone. They need sector-specific solutions, financing support, trusted vendors, cybersecurity guidance, workforce training, and managerial confidence.

Estonia faces a different SME challenge. Its public sector is highly digital, and its ICT sector is internationally recognized, but the European Commission's 2025 Digital Decade country report notes that Estonia still lags the EU average in connectivity and the digitalization of SMEs (European Commission, 2025a). The OECD's 2024 Economic Survey similarly argues that Estonia's further convergence in living standards requires stronger productivity growth through digitalization, innovation, and skills across all firms, while traditional sectors need more effective digital upgrading (OECD, 2024a).

This contrast is analytically important. Singapore's challenge is diffusion from a globally competitive digital economy into SMEs that may lack AI readiness. Estonia's challenge is diffusion from a highly digital public administration and strong ICT ecosystem into the wider private economy. Both cases show that digital-state capacity does not automatically translate into economy-wide SME transformation. Public infrastructure creates enabling conditions, but SMEs need absorptive capacity. Absorptive capacity includes managerial awareness, digital skills, finance, organizational change, cybersecurity practices, and ability to integrate digital tools into business processes.

Dynamic capabilities theory helps explain this process. Teece (2007) argues that firms need sensing, seizing, and reconfiguring capabilities to adapt to technological change. In SMEs, these capabilities are often constrained by limited staff, cash flow, data quality, and technical expertise. Therefore, public policy can function as a capability accelerator. Singapore's sectoral digital plans and AI-enabled SME programs attempt to reduce the cost and uncertainty of adoption. Estonia's digital public infrastructure reduces administrative friction but may need stronger mechanisms to support firm-level technological deepening outside ICT-intensive sectors.

The productivity implications are significant. AI and digital tools can improve inventory management, customer engagement, compliance, accounting, logistics, cybersecurity, marketing, human resource management, and service delivery. However, productivity gains are not automatic. Firms must redesign workflows, train workers, integrate data, and change decision-making routines. If digital adoption remains superficial, it may produce subscription costs without productivity gains. If adoption is concentrated in large firms, it may widen productivity gaps and market concentration.

The development implications extend beyond small states. Many countries invest in digital government or AI strategies but fail to transform SMEs. Singapore and Estonia show that digital economy success must be evaluated by diffusion, not only by frontier performance. A country may have excellent digital public services or a vibrant start-up ecosystem while traditional firms remain digitally weak. Sustainable digital development requires moving from digital access to digital capability and from AI experimentation to productive transformation.

4. Cybersecurity, Institutional Trust, and Economic Resilience

The fourth finding is that cybersecurity and institutional trust are foundational to digital business systems. Singapore's digital economy strategy explicitly links AI adoption with cyber resilience. The Digital Enterprise Blueprint includes "Be Safer" as one of its four pillars, recognizing that enterprise digitalization increases exposure to scams, ransomware, data breaches, and operational disruption (MDDI, 2024). This is particularly important for SMEs, which often lack dedicated cybersecurity teams. If digital adoption increases risk faster than firms can manage it, trust in digital transformation may weaken.

Estonia's cybersecurity orientation is historically central to its digital-state model. Estonia's digital society is widely associated with resilience after cyberattacks in 2007, which strengthened its emphasis on

distributed systems, secure identity, data integrity, and cyber preparedness. OECD Government at a Glance 2025 reports that Estonia scored above the OECD average on the Digital Government Index, with particular strength in data-driven public-sector capability; the same country note reports that 83% of people were satisfied with administrative services used, above the OECD average of 66%, even though general trust in national government was 38%, slightly below the OECD average of 39% (OECD, 2025a). This distinction is important: satisfaction with digital services can be high even when broader political trust is moderate.

The comparison reveals that digital trust is multidimensional. It includes trust in technical systems, trust in institutions, trust in data use, trust in cybersecurity, trust in AI decisions, and trust in business practices. Singapore builds digital trust through regulatory assurance, public-private coordination, and governance frameworks. Estonia builds digital trust through long-term institutional familiarity with digital identity, transparency, data exchange, and public services. Both cases show that digital trust must be continuously maintained; it is not permanently secured by initial adoption.

This finding extends institutional resilience theory. Economic resilience is often defined as the ability to absorb shocks and recover from crises. In digital economies, resilience also means the ability to maintain critical data flows, authentication systems, payments, public services, and business operations during cyberattacks or system failures. Digital-state capacity therefore has a resilience dimension. If firms and citizens depend on digital systems, those systems become critical economic infrastructure.

For business systems, cybersecurity becomes a competitive factor. Firms with strong cybersecurity and data governance can participate more confidently in AI, digital trade, e-commerce, cross-border services, and cloud-based operations. Firms with weak cybersecurity may face reputational damage, regulatory penalties, and operational disruption. For SMEs, the problem is not lack of awareness alone but lack of resources and expertise. Public policy must therefore integrate cybersecurity into SME digitalization rather than treating it as a separate technical issue.

The sustainability dimension is also relevant. Digital resilience contributes to sustainable development by ensuring continuity of essential services, reducing administrative waste, enabling remote work and digital transactions, and supporting crisis management. However, digital systems also consume energy and generate environmental costs. UNCTAD warns that digitalization creates material and energy pressures through data centres, networks, devices, minerals, and e-waste (UNCTAD, 2024). Therefore, sustainable digital-state capacity must combine cybersecurity resilience with environmental responsibility.

Singapore and Estonia both recognize the importance of sustainability, but their approaches differ. Singapore's digital strategy is tied to its position as a global business hub and increasingly to responsible, resource-efficient AI. Estonia's Digital Agenda 2030 explicitly frames digitalization as climate and environmentally friendly, emphasizing that digital practices should conserve resources and support climate adaptation (Ministry of Justice and Digital Affairs, 2025). The comparison indicates that digital sustainability requires more than paperless government; it requires energy-efficient computing, responsible AI infrastructure, green procurement, device lifecycle management, and data minimization.

5. Innovation Ecosystems, Global Positioning, and Sustainable Competitiveness

The fifth finding is that Singapore and Estonia use digital-state capacity to compensate for small domestic market scale, but they do so through different global strategies. Singapore positions itself as a global and regional digital economy hub. It attracts multinational technology firms, supports AI research, develops governance frameworks, invests in talent, and provides a testbed for responsible AI and enterprise solutions. WIPO's Global Innovation Index 2025 ranked Singapore fifth globally and reported that Singapore had the highest number of indicators ranked first globally, including high-tech manufacturing, unicorn valuation, and GitHub commits (WIPO, 2025).

Estonia positions itself as a digital society model and governance exporter. Its e-government experience, e-residency system, X-Road architecture, and public-sector digital expertise have become part of its international identity. WIPO ranks Estonia 16th among 139 economies in the Global Innovation Index 2025, indicating strong innovation performance for a small economy (WIPO, 2025). Estonia's innovation ecosystem is therefore not based on market size but on institutional credibility, digital entrepreneurship, and administrative efficiency.

The cross-case comparison indicates that small digital economies can achieve sustainable competitiveness through specialization in governance functions. Singapore specializes in strategic digital hub formation, enterprise scaling, AI governance, and regional connectivity. Estonia specializes in digital administrative architecture, identity infrastructure, cybersecurity credibility, and state-service innovation. Both strategies generate economic advantages that exceed domestic scale. However, both also depend on continuous upgrading. Singapore must remain attractive amid global AI competition and data-centre sustainability constraints. Estonia must prevent legacy digital systems from becoming outdated and must strengthen private-sector digitalization beyond its public-sector strengths.

This finding contributes to international business scholarship by showing that location advantage in the digital economy includes institutional trust and governance credibility. Traditional location advantage includes market size, labour cost, infrastructure, tax policy, and logistics. In AI-enabled digital economies, location advantage also includes data governance, AI assurance, digital public services, cybersecurity reputation, regulatory agility, and talent systems. Singapore and Estonia demonstrate that small states can compete by offering reliable institutional environments for digital business.

The comparison also has implications for sustainable socio-economic development. Digital competitiveness is sustainable only if it produces broad capabilities rather than narrow enclave growth. Singapore's challenge is ensuring that AI and digitalization benefit SMEs, workers, and domestic firms rather than primarily strengthening multinational and large-enterprise ecosystems. Estonia's challenge is ensuring that its digital public-sector strengths translate into productivity growth across traditional sectors, rural areas, and smaller firms. In both cases, human capital is decisive. Digital transformation requires not only engineers and AI specialists but also digitally fluent managers, workers, regulators, teachers, and citizens.

The policy implication is that digital-state capacity must be developmental rather than merely administrative. A state can deliver efficient online services without generating broad-based innovation. A state can promote AI adoption without ensuring responsible use. A state can attract technology firms without diffusing capabilities locally. Sustainable competitiveness therefore requires institutional mechanisms that link digital infrastructure to skills, SME upgrading, innovation finance, public procurement, cybersecurity, and environmental responsibility.

This finding also challenges technological determinism. AI does not independently produce competitiveness. Digital public services do not automatically generate productivity. Innovation rankings do not guarantee inclusive development. The causal mechanism runs through institutions: how governments coordinate, how firms absorb, how workers adapt, how markets trust, and how sustainability constraints are integrated. Singapore and Estonia show that digital transformation is most successful when institutional capacity turns technology into collective economic capability.

Table 1. Analytical Matrix of Comparative Business and Economic Development

Variable	Case 1: Singapore	Case 2: Estonia	Empirical Evidence	Analytical Interpretation
Institutional digital model	Strategic developmental digital economy based on state orchestration, public-private partnerships, AI governance, enterprise capability-building, and global hub positioning	Digitally embedded institutional state based on e-ID, X-Road, public-service interoperability, digital signatures, cybersecurity, and administrative trust	Singapore's digital economy reached 18.6% of GDP in 2024; Estonia is identified by the European Commission as a leader in digital public services	Singapore builds competitiveness through strategic scaling; Estonia builds competitiveness through trusted interoperability
AI governance architecture	Model AI Governance Framework, AI Verify, generative AI governance, enterprise adoption programs, and national AI	Kratt AI strategy, public-sector AI integration, digital government modernization, and EU regulatory embeddedness	Singapore has developed practical AI governance tools; Estonia's AI strategy promotes adoption in public and private	Singapore emphasizes responsible innovation for markets; Estonia emphasizes AI-enabled public-service modernization

	strategy		sectors	
SME digitalization	Strong policy support through Digital Enterprise Blueprint, SMEs Go Digital, AI-enabled solutions, cyber resilience, and workforce upskilling	Strong public digital infrastructure but SME digitalization and connectivity remain below EU averages	Singapore SME AI adoption reached 14.5% in 2024; Estonia lags the EU average in SME digitalization	Digital-state strength does not automatically translate into SME transformation
Business-system capability	Strong multinational linkages, regional digital hub role, technology partnerships, and enterprise transformation programs	Strong start-up culture, administrative efficiency, digital company formation, and public-private data exchange	WIPO ranks Singapore 5th and Estonia 16th in GII 2025	Both compensate for small market size through institutional specialization
Market trust mechanism	Trust generated through regulatory assurance, state credibility, cyber programs, AI governance, and policy coordination	Trust generated through digital identity, transparency, data exchange, e-services, and institutional familiarity	OECD reports high satisfaction with Estonian administrative services; Singapore develops AI assurance frameworks	Trust is an economic infrastructure for digital markets
Cybersecurity and resilience	Cyber resilience embedded into enterprise digitalization and SME support	Cybersecurity embedded into national digital identity and data exchange architecture	Singapore's Digital Enterprise Blueprint includes "Be Safer"; Estonia scores strongly in digital government	Digital economies require resilience as a condition of competitiveness

			indicators	
Innovation ecosystem	Global AI and digital hub with strong innovation inputs, high-tech manufacturing, and regional governance influence	Digital society exporter with strong governance innovation, e-residency, and ICT entrepreneurship	WIPO identifies Singapore as top five globally; Estonia ranks among leading innovation economies	Innovation advantage includes governance credibility, not only R&D spending
Sustainability orientation	Responsible AI, digital enterprise upgrading, cyber safety, and resource-efficient digital capability development	Digital Agenda 2030 links digital society to climate and environmentally friendly practices	UNCTAD warns digitalization has energy and material costs; Estonia's strategy explicitly links digitalization and environmental goals	Sustainable digital transformation requires green computing, inclusion, and responsible infrastructure
Developmental risk	AI adoption may reinforce gaps between large firms and SMEs; compliance capability may become unequal	Public-sector digital excellence may not fully diffuse into private-sector productivity; connectivity and SME gaps persist	Singapore shows large AI adoption gap between SMEs and non-SMEs; Estonia's Digital Decade report notes SME and connectivity weaknesses	Inclusion depends on capability diffusion, not only infrastructure quality

The table demonstrates that Singapore and Estonia represent two different pathways to digital competitiveness. Singapore's pathway is based on strategic orchestration: the state mobilizes institutions, enterprises, skills, governance tools, and global networks to accelerate AI adoption and digital economy growth. Estonia's pathway is based on embedded interoperability: the state creates trusted digital infrastructures that reduce administrative friction and make digital interaction normal across society. Both pathways generate advantages, but neither is complete. Singapore must convert strategic AI ambition into broad-based SME productivity and worker capability. Estonia must convert digital public-sector excellence

into wider private-sector innovation and productivity growth.

The table also clarifies the causal chain linking institutional structure to sustainable development. Institutional digital models shape digital-state capacity. Digital-state capacity shapes AI governance, SME adoption, and market trust. These mechanisms influence business-system capability, innovation performance, and economic resilience. Sustainable socio-economic development emerges only when digital transformation supports inclusion, cybersecurity, environmental responsibility, and broad capability diffusion. The comparison therefore confirms that digital transformation is not simply a technical process. It is an institutional process through which states and firms co-produce market confidence, productive capacity, and developmental outcomes.

Theoretical Propositions

Proposition 1: Digital-state capacity strengthens business competitiveness when it transforms public infrastructure into firm-level absorptive capability.

Singapore and Estonia show that digital public infrastructure creates enabling conditions, but business competitiveness depends on whether firms can absorb digital tools into production, management, compliance, and innovation. Public policy must therefore connect infrastructure with skills, finance, cybersecurity, and sector-specific adoption pathways.

Proposition 2: Trusted interoperability mediates the relationship between digital infrastructure and market participation.

Digital identity, secure data exchange, AI assurance, and public-service integration reduce uncertainty in market exchange. Estonia demonstrates the power of embedded interoperability in administrative efficiency, while Singapore demonstrates the power of assurance-based trust in AI-enabled business adoption.

Proposition 3: AI governance enhances innovation when it is adaptive, operational, and accessible to SMEs.

AI governance should not remain at the level of abstract principles. It must provide practical guidance on accountability, data governance, model testing, cybersecurity, human oversight, and user literacy. However, governance tools must be usable by SMEs; otherwise, responsible AI may become a capability available only to large firms.

Proposition 4: Digital transformation contributes to sustainable development only when productivity gains are distributed across firms, workers, and public services.

Digital economies can deepen inequality if frontier firms capture most benefits. Sustainable digital development requires SME upgrading, workforce reskilling, cyber resilience, inclusive service access, and environmentally responsible digital infrastructure.

Proposition 5: In small open economies, governance credibility is a source of international business advantage.

Singapore and Estonia show that small states can compensate for limited domestic market size by specializing in trusted governance, interoperability, digital public services, AI assurance, and innovation ecosystems. Institutional credibility becomes a location advantage in the global digital economy.

CONCLUSION

This article examined how Singapore and Estonia use different institutional architectures of digital-state capacity to govern AI-enabled business transformation and what this comparison reveals about the conditions under which digital economies generate sustainable competitiveness and socio-economic development. The direct answer to the research objective is that AI-enabled business transformation depends not merely on technological availability or firm-level adoption, but on the institutional capacity to create trusted, interoperable, secure, inclusive, and capability-enhancing digital systems.

The main analytical finding is that Singapore and Estonia are both digital leaders, but they represent different governance logics. Singapore's model is strategic and developmental. It uses national AI strategy, enterprise digitalization programs, AI governance frameworks, public-private partnerships, and global digital positioning to accelerate business transformation. Estonia's model is embedded and infrastructural. It uses secure digital identity, interoperable data exchange, e-government, digital signatures, and administrative trust to reduce transaction costs and strengthen state-business efficiency.

The theoretical contribution of the article is to integrate comparative business systems, institutional economics, AI governance, digital government, and sustainable development into a digital-state capacity framework. The article shows that digital public infrastructure is not merely an administrative tool; it is a business-system institution that shapes market trust, compliance costs, innovation capability, and firm competitiveness. It also shows that AI governance is not only a regulatory concern; it is a market-enabling mechanism that determines whether firms and citizens trust AI-enabled systems.

The empirical contribution lies in the structured comparison of two small but globally significant digital economies. Singapore demonstrates how strategic state coordination can scale AI adoption, enterprise digitalization, and innovation positioning. Estonia demonstrates how interoperable public infrastructure can institutionalize digital trust and administrative efficiency. Both cases also reveal limits. Singapore's AI adoption gap between SMEs and large firms indicates that digital economy success can coexist with firm-size inequality. Estonia's lag in SME digitalization and connectivity relative to EU averages indicates that public-sector digital excellence does not automatically produce economy-wide productivity transformation.

The business implications are clear. Firms must treat digital governance, cybersecurity, AI assurance, and data capability as strategic resources. SMEs should not approach AI as a single technology

purchase but as an organizational transformation involving skills, workflow redesign, data quality, and risk management. Large firms should recognize that responsible AI and cyber resilience are increasingly central to market credibility.

The policy implications are equally significant. Governments should design digital transformation policy as an integrated system linking infrastructure, AI governance, SME support, workforce development, cybersecurity, innovation finance, and sustainability. Singapore should continue broadening AI adoption while reducing capability gaps between large firms and SMEs. Estonia should strengthen private-sector digital upgrading and connectivity while maintaining its advantages in trusted public infrastructure. Both countries should ensure that digital growth is environmentally responsible and socially inclusive.

The sustainability implications are central. Digital economies are sustainable only when they improve productivity without intensifying exclusion, cyber vulnerability, or environmental harm. Responsible AI, energy-efficient computing, cyber resilience, inclusive digital skills, and accessible public services must therefore become core components of digital economic strategy. Digital transformation should be judged not only by GDP contribution, innovation rankings, or adoption rates, but by its ability to produce resilient, trusted, inclusive, and environmentally responsible development.

This study has limitations. It relies on secondary data and comparative institutional interpretation rather than firm-level interviews or econometric estimation. Future research should test the propositions using firm-level digital adoption data, SME productivity surveys, AI governance compliance studies, cybersecurity incident analysis, and comparative research involving additional small digital states such as Finland, Denmark, Israel, New Zealand, and the United Arab Emirates. Further research should also examine how digital-state capacity affects cross-border digital trade, platform regulation, AI safety markets, public procurement, and green digital infrastructure.

The broader conclusion is that the next frontier of business and economic development is not simply digitalization, but institutionally governed digital transformation. Singapore and Estonia show that the most successful digital economies are not those that merely adopt advanced technologies. They are those that build trusted institutions capable of turning technology into collective economic capability, market confidence, and sustainable socio-economic development.

REFERENCES

Acemoglu, D., & Restrepo, P. (2020). Robots and jobs: Evidence from US labor markets. Journal of Political Economy, 128(6), 2188–2244.

Brynjolfsson, E., Rock, D., & Syverson, C. (2021). The productivity J-curve: How intangibles complement general purpose technologies. American Economic Journal: Macroeconomics, 13(1), 333–372.

Cusumano, M. A., Gawer, A., & Yoffie, D. B. (2019). The business of platforms: Strategy in the age of digital competition, innovation, and power. Harper Business.

Edler, J., & Fagerberg, J. (2017). Innovation policy: What, why, and how. Oxford Review of Economic Policy, 33(1), 2–23.

European Commission. (2025a). Estonia 2025 Digital Decade Country Report. European Commission.

Filippucci, F., Gal, P., Jona-Lasinio, C., Leandro, A., & Nicoletti, G. (2024). The impact of artificial intelligence on productivity, distribution and growth. OECD Publishing.

Hall, P. A., & Soskice, D. (2001). Varieties of capitalism: The institutional foundations of comparative advantage. Oxford University Press.

IMDA. (2024). Singapore unveils new Digital Enterprise Blueprint. Infocomm Media Development Authority.

IMDA. (2025). Singapore Digital Economy Report 2025. Infocomm Media Development Authority.

IMDA & AI Verify Foundation. (2024). Model AI Governance Framework for Generative AI. Infocomm Media Development Authority.

Kenney, M., & Zysman, J. (2020). The platform economy: Restructuring the space of capitalist accumulation. Cambridge Journal of Regions, Economy and Society, 13(1), 55–76.

Mazzucato, M. (2021). Mission economy: A moonshot guide to changing capitalism. Allen Lane.

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. Government Information Quarterly, 36(4), 101385.

Ministry of Digital Development and Information. (2024). Digital Enterprise Blueprint. Government of Singapore.

Ministry of Justice and Digital Affairs. (2025). Digital Agenda 2030. Government of Estonia.

North, D. C. (1990). Institutions, institutional change and economic performance. Cambridge University Press.

OECD. (2024a). OECD Economic Surveys: Estonia 2024. OECD Publishing.

OECD. (2024b). OECD Digital Economy Outlook 2024, Volume 1: Embracing the technology frontier. OECD Publishing.

OECD. (2025a). Government at a Glance 2025. OECD Publishing.

OECD. (2025b). Digital government index: Government at a Glance 2025. OECD Publishing.

OECD.AI. (2025). National AI policy initiatives: Estonia. OECD AI Policy Observatory.

Schot, J., & Steinmueller, W. E. (2018). Three frames for innovation policy: R&D, systems of innovation, and transformative change. Research Policy, 47(9), 1554–1567.

Smart Nation Singapore. (2026). National AI Strategy. Government of Singapore.

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of enterprise performance. Strategic Management Journal, 28(13), 1319–1350.

UNCTAD. (2024). Digital Economy Report 2024: Shaping an environmentally sustainable and inclusive digital future. United Nations Trade and Development.

Warner, K. S. R., & Wäger, M. (2019). Building dynamic capabilities for digital transformation. Long Range Planning, 52(3), 326–349.

Whitley, R. (1999). Divergent capitalisms: The social structuring and change of business systems. Oxford University Press.

Williamson, O. E. (1985). The economic institutions of capitalism. Free Press.

WIPO. (2025). Global Innovation Index 2025. World Intellectual Property Organization.

World Bank. (2025). Digital public infrastructure and development: A World Bank Group approach. World Bank.

