UDC 005.21:004.8
JEL: M15; O32; L86
DOI: https://doi.org/10.32983/2222-4459-2026-8-497-510

SOVEREIGN AI MANAGEMENT: THE CASE OF «SIAIVO» AND UKRAINE'S NATIONAL DIGITAL GOVERNANCE MODEL

© 2026 **PROKOPENKO S. O.**

UDC 005.21:004.8
JEL: M15; O32; L86

Prokopenko S. O. Sovereign AI Management: The Case of «Siaivo» and Ukraine's National Digital Governance Model

The growing strategic importance of artificial intelligence has led many governments to pursue «sovereign AI» as a nationally developed and controlled AI infrastructure intended to reduce dependence on foreign technology providers. While the strategic management literature has examined sovereign AI extensively among major technological powers, comparatively little attention has been paid to how resource-constrained countries manage this trade-off under active security threats. This article addresses this gap by applying a strategic management framework to a case study of Ukraine's national large language model «SIAIVO», developed within the DIIA digital governance ecosystem. The aim of the study is to examine how a public-private national AI project, built under wartime resource constraints, manages the trade-off between strategic autonomy and governance risk. The research employs a qualitative single-case study design, combining analysis of official government communications, the draft National AI Development Strategy through 2030, and secondary media reporting, interpreted through a conceptual framework grounded in strategic management, risk management, and digital sovereignty literature. The analysis shows that the managerial structure of «SIAIVO» is hybrid rather than fully sovereign: State institutional ownership is combined with full private-sector financing by the telecommunications operator, a foreign foundational model architecture, and a still-incomplete domestic legal framework for the training-data rights. Three managerial tensions are identified: concentrated dependency on a single private partner, data governance lagging behind technical development, and undifferentiated oversight across administrative and defense applications of AI. Practical recommendations are proposed for structuring partnership agreements in case of unforeseen circumstances, coordinating data management with technical development, and implementing differentiated oversight of domains. The article concludes with implications for policymakers in other resource-constrained countries pursuing national AI capacity under comparable fiscal and security pressures.

Keywords: *sovereign AI; digital sovereignty; risk management; digital governance; Diia; «Siaivo».*

Bibl.: *47.*

Prokopenko Serhii O. *– PhD, Senior Lecturer, Faculty of Management and Marketing, Simon Kuznets Kharkiv National University of Economics (9a Nauky Ave., Kharkiv, 61165, Ukraine)*
E-mail: *prokopenko.serhii@gmail.com*
ORCID: *https://orcid.org/0000-0003-0718-4917*

УДК 005.21:004.8
JEL: M15; O32; L86

Прокопенко С. О. Стратегічне управління суверенним штучним інтелектом: кейс «Сяйво» та національної моделі цифрового врядування України

Зростаюче стратегічне значення штучного інтелекту спонукало багато урядів розвивати «суверенний ШІ» – національно розроблену та контрольовану інфраструктуру штучного інтелекту, покликану зменшити залежність від закордонних постачальників технологій. Хоча література зі стратегічного менеджменту широко досліджує суверенний ШІ на прикладі великих технологічних держав, порівняно мало уваги приділено тому, як держави з обмеженими ресурсами управляють цим компромісом в умовах активних загроз безпеці. Ця стаття усуває цю прогалину, застосовуючи рамку стратегічного менеджменту до кейс-стаді української національної великої мовної моделі «Сяйво», розробленої у межах екосистеми цифрового врядування «Дія». Мета дослідження – вивчити, як державно-приватний національний ШІ-проєкт, побудований в умовах воєнних ресурсних обмежень, управляє компромісом між стратегічною автономією та управлінським ризиком. У статті застосовано якісний однокейсовий дизайн дослідження, що поєднує аналіз офіційних урядових комунікацій, проєкту Національної стратегії розвитку штучного інтелекту до 2030 року та вторинних медіаджерел, інтерпретованих крізь концептуальну рамку, засновану на літературі зі стратегічного менеджменту, управління ризиками та цифрового суверенітету. Аналіз показує, що управлінська структура «Сяйва» є гібридною, а не повністю суверенною: державна інституційна власність поєднується з повним приватним фінансуванням з боку телекомунікаційного оператора, іноземною фундаментальною архітектурою моделі та досі незавершеною вітчизняною правовою рамкою щодо прав на навчальні дані. Виявлено три управлінські дисбаланси: концентровану залежність від єдиного приватного партнера, відставання управління даними від технічного розвитку, та розбалансований нагляд за адміністративними й оборонними застосуваннями ШІ. Запропоновано практичні рекомендації щодо структурування партнерських домовленостей на випадок непередбачених обставин, узгодження управління даними з технічним розвитком і впровадження диференційованого нагляду за доменами. Стаття завершується висновками для експертів з інших держав з обмеженими ресурсами, які розвивають національний потенціал у сфері штучного інтелекту за подібних фіскальних і безпекових умов.

Ключові слова: *суверенний штучний інтелект; цифровий суверенітет; управління ризиками; цифрове врядування; Дія; Сяйво.*

Бібл.: *47.*

Прокопенко Сергій Олександрович *– доктор філософії, старший викладач, факультет менеджменту і маркетингу, Харківський національний економічний університет імені Семена Кузнеця (просп. Науки, 9а, Харків, 61165, Україна)*
E-mail: *prokopenko.serhii@gmail.com*
ORCID: *https://orcid.org/0000-0003-0718-4917*

INTRODUCTION

Artificial intelligence has moved from a peripheral technology to a core strategic asset for national governments, reshaping how public administration, media systems, and economic policy are organized [1]. As states increasingly recognize the competitive and geopolitical value of AI capabilities, many have begun pursuing what is now commonly referred to as "sovereign AI": nationally developed and controlled algorithmic infrastructure designed to reduce dependence on a small number of dominant foreign technology providers. This strategic pivot reflects a broader pattern of technological competition between major powers, in which control over digital infrastructure has become a central instrument of state power and economic leverage [2].

From a management standpoint, the pursuit of sovereign AI can be understood as a form of risk diversification: by developing domestic AI capabilities, governments aim to insulate themselves from the vulnerabilities associated with reliance on external providers, including data extraction, loss of technological autonomy, and exposure to foreign regulatory or commercial interests [3]. At the same time, this strategy introduces a distinct set of internal risks. Nationally controlled AI systems, trained on domestically curated data and shaped by local institutional priorities, may reproduce and reinforce specific cultural, political, or organizational biases, effectively trading external dependency for the risk of internal governance [4; 5].

This paper argues that sovereign AI should be approached not merely as a technological or geopolitical project, but as a strategic management challenge requiring deliberate governance design. Effective management of sovereign AI initiatives requires balancing the pursuit of strategic autonomy with mechanisms that preserve accountability, adaptability, and resilience within national AI ecosystems. Without such mechanisms, sovereign AI risks becoming a source of concentrated organizational and reputational risk for the state rather than a stable strategic advantage [6].

To examine how this trade-off plays out in practice, the paper first looks at how major technological powers approach sovereign AI governance pursued by major technological powers, before turning to a case study of Ukraine's national digital infrastructure, centered on the DIIA platform and its national large language model, "SIAIVO". Ukraine offers a distinctive setting for this inquiry: a state pursuing digital and technological autonomy under resource constraints and active security threats, where the trade-off between strategic independence and governance risk is especially pronounced.

The remainder of the paper is structured as follows. Section 2 reviews the relevant literature on strategic management, risk governance, digital sovereignty, and public-sector marketing, situating the study within the broader academic debate and identifying the research gap it addresses. Section 3 outlines the qualitative single-case study methodology, including data sources and the three-dimensional analytical framework applied to the case. Section 4 provides a brief comparative overview of sovereign AI governance postures among major and middle powers, situating Ukraine among these approaches. Section 5 presents the case study proper, examining Diia's evolution into an AI infrastructure platform; the ownership and partnership structure of the "SIAIVO" national language model; its data governance arrangements; and the National AI Strategy through 2030, which formalizes these initiatives within a broader policy architecture. Section 6 discusses the governance implications arising from the case, including risks related to partnership dependency, data governance sequencing, undifferentiated oversight, and the underused potential of brand co-creation as a legitimation mechanism, and derives practical recommendations for policymakers and organizational leaders. Section 7 addresses the study's limitations and outlines directions for future research. Section 8 concludes with implications for other resource-constrained states pursuing sovereign AI strategies under comparable conditions.

LITERATURE REVIEW

The concept of sovereign AI is closely related to a longer-standing debate on digital sovereignty, which emphasizes state and organizational autonomy over data governance, technological infrastructure, and platform control [7]. The most comprehensive recent treatment defines AI sovereignty as a spectrum of strategies for national agency over critical AI infrastructure, demonstrating that full-stack sovereignty is structurally infeasible for almost any state because the AI stack, spanning physical inputs, compute hardware, networks, digital infrastructure, data, models, applications, and the crosscutting enablers of talent and governance, is intrinsically transnational and characterized by concentrated choke points at nearly every layer [8].

This analysis categorizes states into four groups: broad stack leaders (the United States, China, the European Union), coordinated stack builders with strength across several layers (India, Japan, the United Kingdom), strategic layer specialists dependent on others for most inputs (Canada, Germany, Singapore, South Korea), and a residual category of

states only beginning AI deployment, whose position in the global AI ecosystem has been comparatively overlooked in the literature despite their growing share of the world's population [8]. Ukraine is not explicitly analyzed within this framework, but its combination of an advanced digital-government layer with minimal AI-stack capacity elsewhere positions it awkwardly across these categories, a tension explored further.

Rather than treating sovereignty as a binary condition, this literature converges on "managed interdependence" as the only structurally viable strategy: states are advised to map dependencies layer by layer, prioritize interventions where near-term policy tractability is highest, diversify suppliers, and embed interoperability rather than pursue closure [8]. A parallel formulation frames the same insight as a continuum balancing autonomy against interdependence across distinct sovereignty pillars – data, compute, models, and norms [9], while a two-pronged framework separates the *why* of sovereign AI (security, economic competitiveness, cultural autonomy) from the *how*, concluding that most observed national strategies are hybrid rather than fully sovereign and proposing "partial sovereignty" as the more accurate descriptive category [10]. Complementary industry analysis based on a global survey of governments and enterprises similarly finds that sovereign AI adoption is best understood as a multiyear organizational transformation constrained primarily by institutional readiness – workload tiering, budgets, and governance capacity rather than by technology availability, with successful ecosystems relying on identifiable partnership models between government, enterprise anchor tenants, and technology providers rather than on unilateral state build-out [11].

From an earlier strategic management perspective, this literature developed largely around the experience of major technological powers. Bradford's account of European regulatory influence illustrates how large jurisdictions can leverage market size and regulatory design to shape global technology standards, effectively exporting domestic governance models rather than depending on external ones [3]. Farrell and Newman similarly show how control over global economic and technological networks has become an instrument of state coercion, framing technological dependence itself as a strategic vulnerability that governments have strong incentives to reduce [2]. Within this earlier literature, sovereign AI was typically presented as a risk-mitigation strategy pursued by states with sufficient technological, financial, and institutional capacity to build independent infrastructure – an assumption that both the managed interdependence and partial sovereignty frameworks directly complicate once smaller and resource-constrained states are considered [8; 10].

A parallel stream of scholarship addresses the organizational and governance risks posed by the embedding of AI systems in decision-making processes. Research on algorithmic bias demonstrates that AI systems trained on culturally and institutionally situated data can reproduce and amplify existing social and organizational biases, regardless of the technical sophistication of the underlying models [5; 4]. From a risk governance standpoint, this body of work implies that reducing external technological dependence does not eliminate organizational risk; it relocates that risk inward, toward the domestic institutions responsible for designing, training, and overseeing nationally controlled systems [6]. This insight is central to the strategic management framing adopted in this paper: sovereign AI should be evaluated not only in terms of the external risks it mitigates but also in terms of the internal governance risks it creates, including data concentration, reduced oversight diversity, and dependence on a narrow set of domestic institutional actors.

Ukraine's digital governance and the Diia platform in the domestic literature

A substantial and growing body of domestic Ukrainian scholarship has examined the digitalization of public administration, with particular attention to the DIIA platform as its most visible institutional expression. Legal and administrative studies have analyzed the transformation of public service delivery through digital platforms such as DIIA and the Unified Social Register, focusing primarily on regulatory and institutional adaptation [12]. Related research has examined the digitalization of administrative services more broadly, identifying service-state formation as a defining feature of Ukraine's digital transformation trajectory [13]. Other studies have addressed the interaction between state and society under digitalization, noting that while platforms such as Diia have measurably improved access to administrative services, regional disparities in digital access persist [14].

International scholarship has increasingly engaged with Diia as an object of study in its own right, particularly in the context of full-scale war. Gustafsson et al. [15] examine how the DIIA platform and surrounding institutional arrangements have been adapted to sustain collaborative public service delivery during wartime disruption, applying an institutional analysis framework to explain how digital infrastructure enables adaptive governance under extreme crisis conditions [15]. Complementing this institutional perspective, Codreanu examines Diia specifically through

a cybersecurity lens, analyzing how Ukraine has maintained the platform's operational continuity amid a sustained campaign of cyberattacks and drawing comparative lessons from Estonia's earlier experience with state-directed cyberattacks [16].

These two bodies of literature address complementary but largely disconnected aspects of the problem examined in this paper. The strategic management and digital sovereignty literature has developed an increasingly refined conceptual vocabulary for analyzing sovereign AI as a trade-off between external dependence and internal governance risk, moving from earlier binary framings toward more nuanced concepts such as managed interdependence and partial sovereignty [8; 9; 10]. Yet even these more recent frameworks have been developed and empirically illustrated primarily with reference to major and middle powers possessing substantial fiscal, computational, and institutional capacity [8; 10]. Meanwhile, the domestic Ukrainian literature on Diia offers a detailed empirical account of institutional adaptation, legal transformation, and operational resilience under wartime conditions, but has engaged only marginally with the strategic management and risk governance concepts developed in the sovereign AI literature, and has not yet examined how these concepts apply once national platforms move beyond digital service delivery into the development of proprietary AI infrastructure.

This gap has become more consequential with Ukraine's recent movement from e-government toward sovereign AI proper. Beyond its established role as a digital service platform, Diia has become the institutional vehicle for Ukraine's first national large language model, "Siaivo," [17] developed by the Ministry of Digital Transformation in partnership with the private telecommunications operator Kyivstar [18], alongside a growing set of AI-enabled functions embedded directly into the platform [19]. This development positions Ukraine as a case that does not fit neatly within existing sovereign AI frameworks: it is neither a major power building a fully domestic AI stack, nor a smaller state passively adopting foreign models, but a resource-constrained state under active security threat that is simultaneously pursuing AI-driven public administration and forming strategic partnerships with domestic private capital and global technology providers.

This paper addresses that gap by extending the strategic management framework of sovereign AI governance to this distinctive case, using the Diia platform and Ukraine's emerging national AI ecosystem, centered on Siaivo, as an illustrative case through which to examine how the trade-off between strategic autonomy and governance risk plays out beyond the context of major technological powers.

METHODOLOGY

This study uses a qualitative single-case design, treating Ukraine's national digital infrastructure as an single exploratory case rather than a critical or representative one in the strict sense. The case is not meant to test a hypothesis against a best- or worst-case scenario. Instead, it shows how the vocabulary of sovereign AI governance, built largely around major and middle powers, holds up, and where it needs adjusting, when applied to a resource-constrained state building AI-enabled public administration under active security threat [47]. An exploratory single-case design suits this purpose: the phenomenon, a national LLM being integrated into an existing e-government platform during wartime, is recent enough that little systematic research exists on it. The aim here is not statistical generalization but generating propositions that later comparative work across other resource-constrained states can test more rigorously.

The empirical material comes from three sources. First, official communications from the Ministry of Digital Transformation covering the "Siaivo" LLM, the Diia.AI assistant, and the Agentic State initiative serve as primary evidence of the government's stated intentions and design choices. Second, Ukrainian and international media reporting fills in details on partnership structures, technical scope, and timelines that official statements leave out. Third, the literature reviewed in Section 2, particularly the managed interdependence and partial sovereignty frameworks [8; 9; 10], supplies the conceptual lens through which Ukraine's choices are read.

The analysis works through these materials along three dimensions drawn from the strategic management and risk governance literature: ownership and control (fully domestic, joint public-private, or externally dependent elements), institutional oversight mechanisms (data governance and risk management arrangements), and the pattern of external partnerships (their scope and strategic function).

The approach has clear limits, discussed further. A single document-based case cannot support statistical generalization, and leaning heavily on one ministry's public statements risks overlooking internal disagreements or unresolved problems the government has not yet disclosed. The case is better read as theory-extending than theory-testing: it shows how existing sovereign AI concepts apply and where they need to be stretched in a resource-constrained wartime context, not as a verdict on whether Ukraine's choices will ultimately succeed.

Sovereign AI Governance Postures Among Major and Middle Powers

Before turning to the Ukrainian case, it is useful to briefly situate it against the range of governance postures currently observed among states pursuing sovereign AI. These postures differ substantially in ownership structure, funding model, and the underlying strategic rationale.

The United States has followed a predominantly market-driven approach, in which sovereign capability emerges as a byproduct of competition among private developers rather than through direct state ownership of models or infrastructure. Government influence operates primarily through export controls on computer hardware and procurement policy rather than through a centrally directed national model [10]. China, by contrast, illustrates a state-directed posture, in which alignment between AI outputs and official policy objectives is treated as an explicit governance goal, and a small number of domestically developed models operate under close regulatory oversight of content and data flows [10].

The European Union presents a more fragmented and pluralistic picture than either of these two poles. Rather than a single EU-wide sovereign model, the past two years have seen a wave of nationally funded large-language-model initiatives across member states, each oriented toward linguistic and cultural sovereignty rather than pure technological competitiveness.

Germany has launched the Sovereign Open Source Foundation Models initiative, a 100-billion-parameter open-source model trained on domestic infrastructure [20]; Switzerland has developed Apertus, a multilingual model covering over 1,000 languages including Swiss German and Romansh, alongside the privately hosted Euria assistant [21]; France has backed Mistral AI as a national champion alongside the collaborative OpenEuroLLM initiative [22]; and comparable state-funded projects are underway in the Netherlands (GPT-NL) [23], Sweden (GPT-SW3) [24], Finland (LUMI-powered Finnish LLMs) [25], Spain (Alia) [26], Poland (PLLuM and Bielik AI) [30], Portugal (Amalia) [27], Greece (Meltemi) [28], Hungary (the PULI model family) [29], and Bulgaria (BgGPT) [47].

This pattern illustrates that even within a single regulatory bloc governed by a shared framework such as the EU AI Act, sovereign AI has been pursued as a decentralized, member-state-level strategy rather than a unified continental one, with individual governments funding models tailored to their own language, administrative, and cultural context.

Ukraine appears within this same regional wave, but under materially different conditions. Ukrainian national LLM effort, described as Gemma-based and oriented toward reflecting Ukrainian language and context, have a planned beta release in spring 2026 as part of a broader "AI Factory for sovereignty" initiative [31]. This runs in parallel to the domestically driven "Siaivo" project developed by the Ministry of Digital Transformation in partnership with Kyivstar [32].

The coexistence of these two tracks as internationally supported model-training initiative and a domestically financed public-private model developed under wartime conditions is itself indicative of the hybrid governance posture that distinguishes Ukraine from both the market-driven and state-directed postures described above, and from the comparatively well-resourced, peacetime national LLM projects observed elsewhere in Europe [33].

DIIA and Ukraine's National AI Ecosystem

Diia launched in 2020 as a mobile and web platform for digital ID documents and administrative services. Within a few years it became one of the most widely used e-government platforms in Europe, and by the mid-2020s had turned into the institutional base for Ukraine's emerging AI ecosystem. That shift matters strategically: instead of building AI capability as a separate project, Ukraine embedded it into a platform that already had users, data pipelines, and public trust. This section looks at ownership, oversight, and partnerships behind that strategy – the "Siaivo" language model, the Diia.AI assistant, and the Agentic State initiative.

In June 2025, the Ministry of Digital Transformation and Kyivstar, Ukraine's largest telecom operator, signed a memorandum to build the country's first national LLM [38]. The setup is an unusual public-private split: Kyivstar covers development, infrastructure, staffing, and financing in full, while the state keeps institutional ownership of the result [34]. In effect, the state sponsors and owns the outcome; a private company carries the financial and operational risk. Kyivstar's involvement follows an unusual selection process: the Ministry had initially expected a Western technology company or an international consortium to emerge as its partner, given the scale of expertise required, but Kyivstar was the party that responded to the government's open call [34]. The company's own estimate places the total cost of the first development phase at approximately $2 million – a modest figure relative to global AI industry spending, but one Kyivstar has committed to covering in full given the state's wartime budget constraints [34]. Beyond the stated goal of building in-house AI expertise, industry observers note that Kyivstar's participation coincides

with the company's broader push into Ukraine's technology market, including a partnership with SpaceX and preparation for a stock market listing, suggesting the project also serves as a reputational and strategic investment rather than a purely public-spirited contribution [34].

This choice reflects a broader resource constraint rather than a preference: Ukraine's AI center has indicated that the country currently lacks the computational capacity to train a model from scratch, making fine-tuning an existing open-weight architecture on Ukrainian data both the faster and the only realistic path [36]. Model size has been calibrated accordingly rather than pursuing frontier-scale parameter counts, the team has prioritized models in the 1–16 billion parameter range, a scale that can run on a single GPU or a small cluster and that industry practitioners argue can match or exceed larger models on specialized, localized tasks [36].

Development moved in stages rather than one large training run – a smaller model first, to test architecture and training choices before committing to something bigger [33]. The model runs on Google's open-weight Gemma, starting with Gemma 3 and later moving to the 31-billion-parameter Gemma 4 [34]. So even though the model trains on Ukrainian data for Ukrainian public services, its architecture comes from a foreign provider, making it a hybrid of domestic adaptation and foreign dependency rather than a fully indigenous system.

Data governance is where ambition and unresolved risk sit side by side. The training corpus draws on roughly 90 state institutions, media organizations, universities, and research bodies, including 10 terabytes of historical and scientific material from the State Archival Service, some of which still needs to be digitized from paper [35]. At the same time, the legal framework for data-usage rights and IP protection is still being worked out – Minister Oksana Ferchuk has named this one of the project's central unresolved problems [17]. This tracks with the pattern from Section 2: sovereignty over AI infrastructure doesn't remove governance risk, it just moves it inward, in this case into a domestic legal regime for data rights that isn't finished yet.

Quality and safety review falls to an expert committee of more than 70 people across four areas – scientific-technical, ethical-legal, cultural-historical, linguistic – checking Ukrainian-language accuracy, cultural and historical understanding, resistance to hallucination and bias, and disinformation risk, alongside benchmarking against other LLMs [17]. This is a real attempt to build in the kind of oversight Section 2 flags as a governance priority, though there's no way yet to judge how well it works, since the model hasn't launched.

The timeline itself says something about operational risk. First target: end of 2025. Revised to spring 2026 beta. That slipped to a closed beta in June 2026, by which point pre-training and fine-tuning were done and the model had moved into alignment [17]. Current estimate: a full test model by December 2026, public release in January 2027 [36]. Delays are telling– even a well-funded public-private partnership runs into real execution risk when building sovereign AI under wartime disruption, an unfinished data-rights framework, and dependence on one private partner for both delivery and money.

Once finished, Kyivstar is expected to hand the model to the state, which plans to release the base version open source along with the datasets, so outside developers and companies can fine-tune it [36]. The planned open-source release matters strategically: it pairs centralized, public-private development with a downstream commitment to openness rather than treating the model as closed IP which lines up with the "managed interdependence" idea from Section 2, where sovereignty comes from calibrated openness at different points in the stack, not from closing everything off.

On November 17, 2025, the Ministry of Digital Transformation announced a joint initiative with Nvidia aimed at building sovereign state AI capacity – infrastructure, talent, and government and defense applications with First Vice Prime Minister Mykhailo Fedorov framing the partnership as central to Ukraine's national AI strategy [37]. The initiative's first concrete deliverable is "Diia AI LLM," described as a sovereign large language model adapted to Ukrainian legislation and public-service needs, intended to underpin all AI services across the Diia ecosystem, including the already-launched AI assistant on the Diia portal, a forthcoming mobile-app assistant, and internal government tools [37].

The naming process added a layer of public legitimacy: in March 2026, Ukrainians submitted over 3,000 name proposals through Diia, ten finalists went to a public vote, and "Siaivo" ("radiance") won with 22,538 of more than 136,000 votes cast [38]. This is worth reading as more than a symbolic gesture – it's citizen co-creation applied to a national AI brand. Co-creation, in the marketing literature, means bringing end users into product design rather than treating them as passive recipients, and it builds engagement and perceived ownership around a brand [39]. In public-sector contexts specifically, co-creation has

been linked to greater trust and legitimacy, because it positions citizens as contributors rather than consumers of state technology [40]. Using Diia's existing civic infrastructure to crowdsource and vote on a strategic asset's name is a recognizably marketing move of participatory brand-building applied to something that could otherwise have looked like a closed, top-down project. None of the European sovereign LLM initiatives reviewed in Section 4 used anything comparable, which suggests this kind of co-creation may only be available to states that already have a high-trust civic platform like Diia to build on.

The National AI Strategy 2030: Institutionalizing the Governance Framework

In March 2026, the Ministry of Digital Transformation released a draft National AI Development Strategy through 2030 for public consultation, developed jointly with international partners, government bodies, business representatives, and the AI professional community [41]. The draft strategy provides the clearest official articulation of the governance logic underlying the case examined in this paper. Acting Minister of Digital Transformation Oleksandr Borniakov framed the strategy's central ambition as placing Ukraine among the top three countries globally for AI development in the public sector by 2030, with explicit application across defense, public administration, and education [41]. The strategy also explicitly reframes the strategic autonomy problem in terms directly consistent with the managed interdependence framework: it states that its objective is not full technological self-sufficiency, but strategic autonomy, defined as the capacity to deploy, adapt, and govern AI systems in accordance with national priorities and security requirements [41]. This formulation is a near-verbatim institutional counterpart to the "managed interdependence" and "partial sovereignty" concepts, suggesting that Ukrainian policymakers have independently converged on a governance logic consistent with the academic literature reviewed there [8; 9]

The strategy grounds this ambition in a candid assessment of current constraints. Ukraine ranks 41st globally on the Oxford Insights Government AI Readiness Index (2025), an improvement from 54th in 2024, and 62nd on the IMF AI Preparedness Index (2023); it simultaneously ranks 5th worldwide on the UN E-Government Online Services Index and 1st on the UN E-Participation Index (2024) [42]. This divergence of strong public-sector digital governance capacity alongside comparatively weak private-sector AI diffusion is itself diagnostic of the case examined in this paper: only 4.6 percent of Ukrainian enterprises reported using at least one AI function in 2025, a diffusion rate 20–30 percent behind EU and OECD averages, while domestic R&D spending stands at approximately 0.3 percent of GDP compared with 2.3 percent across the EU [41]. The defense sector is identified as the most operationally mature domain of AI application, reflecting battlefield deployment of AI-enabled systems for unmanned platforms, geospatial intelligence, cyber defense, and logistics since 2022 [41].

The draft strategy organizes implementation around four strategic goals, each mapping directly onto the governance dimensions examined in this case study. Strategic Goal 1 targets accelerated AI adoption, formalizing the "Agentic State" concept as the transformation of Diia into a platform on which AI agents independently identify the service a citizen needs, complete the associated forms, and automate routine analytical and reporting work currently performed by civil servants – with a target of 100 services accessible through an AI agent by 2030, up from a 2026 baseline of one [41; 42]. A defense-oriented component within this same priority calls for a unified platform coordinating battlefield data analytics and autonomous systems development, together with an AI-based decision-support tool for military command [41] – an application domain that carries governance stakes considerably higher than routine administrative automation. An education and workforce component positions the "Mriya" application as the primary AI-based learning tool for students, alongside a target of training 50,000 AI specialists domestically [41], while an economic component aims to quadruple the number of Ukrainian AI companies to 1,000, supported by a newly launched regulatory sandbox [41].

Strategic Goal 2 addresses the development and accessibility of foundational AI technologies, and it is here that the ownership structure examined earlier is given explicit policy grounding: the strategy commits to deploying a "Sovereign AI Factory," described as a hybrid governance arrangement in which sensitive workloads run on sovereign infrastructure while general-purpose tasks are integrated with scalable commercial cloud services, alongside a CloudBank-UA mechanism for pooling and allocating subsidized computing resources to SMEs, universities, and public bodies [41].

The accompanying Operational Plan for 2026–2028 distinguishes this civilian Sovereign AI Factory from a separate Defense AI Factory tasked with coordinating AI development between the state, the Armed Forces, and private industry for military applications, with a target completion date of December 2026 [42]. This distinction matters for interpreting public-facing

accounts of Ukraine's AI infrastructure, which have sometimes referred to a single undifferentiated "AI Factory": the strategy documents indicate two parallel, domain-differentiated sovereign infrastructure tracks as civilian and defense governed by different ministries and subject to different oversight requirements, rather than one unified initiative. Strategic Goal 2 also names the national large language model explicitly as a data-sovereignty instrument, tying it to a target of expanding the openly available Ukrainian-language text corpus from 60 billion tokens (2026 baseline) to 200 billion tokens by 2030, and to a specific 2026 deliverable requiring completion of "at least one competitive large language model optimized for the Ukrainian language" [41; 42] – a target that corresponds directly to Siaivo, confirming that the project is treated within the government's own planning documents as the operational vehicle for this strategic goal rather than a standalone technical initiative.

Strategic Goal 4 addresses governance proper. Here the strategy is explicit that AI oversight will not be built through new parallel institutions but through the expansion of Ukraine's existing digital-transformation governance architecture as the network of Chief Digital Transformation Officers (CDTOs) embedded across ministries combined with phased alignment to EU Regulation 2024/1689 (the EU AI Act), moving from voluntary soft-law instruments in 2026–2028 toward statutory enforcement under a planned Unified Digital Regulator from 2028 [41; 42].

Two features of the strategy are worth noting beyond its substantive content. First, it explicitly frames itself as a "signpost" subject to revision based on public and institutional feedback, with a formal consultation period and a defined feedback deadline – an unusually open and iterative approach to strategy formation for a national AI policy document, consistent with the participatory legitimation pattern already observed in the public naming of Siaivo [41; 42]. Second, and more consequentially for the analysis that follows, the strategy's priority domains span administrative automation, defense applications, and economic policy within a single governance architecture, without yet specifying differentiated oversight or risk-governance mechanisms appropriate to each domain – a gap taken up earlier given that the governance risks associated with an AI agent auto-filling an administrative form differ substantially from those associated with an AI-based decision-support tool for military command.

Read together with the ownership and data-governance findings earlier, the strategy confirms that Ukraine's sovereign AI posture is neither improvised nor merely reactive to individual project timelines, but is embedded in an explicit, multi-year policy architecture that names managed interdependence as its organizing principle, differentiates governance requirements by application domain, and sequences institutional and legal capacity-building to trail technological deployment rather than precede it. This a sequencing choice that carries its own governance risks, examined next.

Discussion: Governance Implications and Practical Recommendations

Sovereign AI governance in a resource-constrained, wartime context does not reduce to a single autonomy-versus-dependence trade-off, as much of the literature implicitly assumes. Three distinct tensions emerge from the Siaivo case instead.

Kyivstar's full financing and development role, against the state's institutional ownership, solves a real wartime budget constraint efficiently in the short term. But it concentrates delivery risk and negotiating leverage in a single private actor, with no parallel in-house capacity as a fallback the same concentration risk sovereign AI is meant to solve internationally, reproduced domestically. Gemma's foundational role adds a second layer of dependency beneath the first. Partnerships like this should be built with explicit contingencies from the start by phased IP transfer, documentation escrow, a parallel in-house team rather than informal trust.

Training proceeded ahead of the legal framework for data rights, a gap Minister Ferchuk herself has flagged. This is common in AI generally, but harder to fix here: reopening data-rights questions after training is difficult without reopening training itself. The Strategy's own phased approach as voluntary compliance now, enforcement from 2028 treats this as policy rather than urgency. Data governance should run in parallel with technical development, not behind it, with independent oversight rather than internal ministry review alone, especially given that much of the training corpus comes from state institutions themselves.

The Strategy places administrative automation, economic development, and defense applications under one governance architecture – CDTOs now, a Unified Digital Regulator later, without differentiating oversight by domain. An AI agent filling out a form and an AI decision-support tool for military command carry very different risk profiles; one framework risks under-governing the high-stakes case while over-engineering the low-stakes one. Domain-differentiated oversight tiers should be built in early, not left to emerge once the Regulator's mandate is defined after 2028 – defense applications in particu-

lar need oversight independent of the civilian digital-transformation track.

Together, these tensions suggest Ukraine's sovereign AI approach is conceptually ahead of its institutions: managed interdependence and strategic autonomy are named in policy language, but the mechanisms to operationalize them are still being built. This isn't unique to Ukraine – the literature shows the same gap even among better-resourced powers. What's distinctive here is that Ukraine must close it under wartime constraints and a narrow window for iteration, which makes the three recommendations above conditions for the Strategy's 2030 goals, not optional refinements.

Limitations and Future Research

This study has several limitations worth noting. As a single-case, document-based design, it doesn't support statistical generalization – the findings are theoretically informed propositions about partnership dependency, data governance sequencing, and undifferentiated oversight, which future comparative work should test across other conflict-affected or fiscally constrained states.

The empirical material also leans heavily on official ministry communications and secondary media reporting, which likely understates internal disagreement or unresolved problems the government hasn't disclosed, and reflects the state's own framing rather than an independent assessment. Interviews with Kyivstar technical staff, civil society data-governance watchdogs, or independent AI policy analysts would balance this out.

The analysis is also necessarily prospective: Siaivo had not launched at the time of writing, so the evaluation of ownership, data governance, and oversight can't speak to actual performance or governance outcomes once deployed. A follow-up study after the planned January 2027 release could assess whether these mechanisms held up, and whether the three tensions identified in Section 6 were addressed or persisted.

Finally, this paper remains within strategic management and governance – it doesn't directly evaluate model performance, linguistic accuracy, or bias, though these matter given the expert committee's own focus on hallucination and disinformation risk [44]. And the comparative overview was deliberately brief, meant to situate Ukraine rather than survey sovereign AI governance comprehensively; applying this paper's three-dimensional framework systematically across more small and middle powers would help turn these single-case propositions into a comparative theory that holds up across more contexts.

CONCLUSION

This paper examined how a resource-constrained state under wartime conditions manages the trade-off between technological autonomy and governance risk in sovereign AI. Using Diia's national AI ecosystem Siaivo, Diia.AI, and the Agentic State initiative as an illustrative case, the analysis shows this trade-off is not the simple autonomy-versus-dependence binary common in the literature. Ukraine's approach is a hybrid: substantial domestic institutional ownership layered with dependencies on a single private partner, a foreign foundational model, and an incomplete domestic data-governance framework.

Three tensions identified here – partnership concentration, data governance lagging technical development, and undifferentiated oversight across administrative and defense applications. This extend the sovereign AI governance framework beyond the major and middle powers it was built around. These are structural consequences of pursuing sovereign AI under resource scarcity and active security threat, not incidental to Ukraine's circumstances, and likely to recur elsewhere under similar constraints.

The paper's central contribution is showing that Ukraine's own policy language – "strategic autonomy," a "Sovereign AI Factory" built on hybrid infrastructure anticipates the managed interdependence and partial sovereignty concepts developed independently in the international literature. But naming a governance principle isn't the same as building the institutions to operationalize it, and the recommendations offered here: explicit partnership contingencies, parallel rather than sequential data governance, and domain-differentiated oversight established early – are conditions for closing that gap, both for Ukraine and for other resource-constrained states starting similar initiatives.

For policymakers designing national AI strategies under fiscal constraint, security threat, or both, the lesson is that sovereign AI governance works better as an ongoing management discipline than a one-time strategic choice. ■

BIBLIOGRAPHY

1. Floridi L. Establishing the rules for building trustworthy AI. *Nature Machine Intelligence*. 2019. Vol. 1. No. 6. P. 1–2. DOI: https://doi.org/10.1038/s42256-019-0055-y
2. Farrell H., Newman A. L. Weaponized interdependence: how global economic networks shape state coercion. *International Security*. 2019. Vol. 44. No. 1. P. 42–79. URL: https://www.jstor.org/stable/26777882

3. Bradford A. The Brussels effect: how the European Union rules the world. Oxford : Oxford University Press, 2020. 424 p. DOI: https://doi.org/10.1093/oso/9780190088583.001.0001
4. Benjamin R. Race after technology: abolitionist tools for the new Jim code. Cambridge : Polity Press, 2019. 172 p. DOI: https://doi.org/10.23987/sts.102639
5. Noble S. U. Algorithms of oppression: how search engines reinforce racism. New York : New York University Press, 2018. 256 p. URL: https://www.researchgate.net/publication/327109256_Algorithms_of_Oppression_How_Search_Engines_Reinforce_Racism
6. Zuboff S. The age of surveillance capitalism: the fight for a human future at the new frontier of power. New York : PublicAffairs, 2019. 704 p. URL: https://we.riseup.net/assets/533560/Zuboff%2C+Shoshana.The+Age+of+Surveillance+Capitalism.2019.pdf
7. Aarab H. European digital sovereignty in the age of AI: regulation, infrastructure, and democratic legitimacy. *AI in Context of Digital Sovereignty*. Boca Raton : CRC Press, 2026. P. 333–355. DOI: https://doi.org/10.1201/9781003581581-14
8. Tanner B., Kerry C. F., Wyckoff A., Kyosovska N., Renda A., Tabassi E. Is AI sovereignty possible? Balancing autonomy and interdependence. Washington : Brookings Institution ; Brussels : CEPS, 2026. URL: https://www.brookings.edu/articles/is-ai-sovereignty-possible-balancing-autonomy-and-interdependence/
9. Singh S. K., Sengupta S. Sovereign AI: rethinking autonomy in the age of global interdependence. *arXiv*. 2025. DOI: https://doi.org/10.48550/arXiv.2511.15734
10. George J. Assessing sovereign AI: a two-pronged framework. Center for Security and Emerging Technology. Georgetown University, 2026. URL: https://cset.georgetown.edu/article/assessing-sovereign-ai-a-two-pronged-framework/
11. McKinsey & Company. The sovereign AI agenda: moving from ambition to reality. 2025. URL: https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/tech-forward/the-sovereign-ai-agenda-moving-from-ambition-to-reality
12. Медяник В. А. Цифровізація публічного управління в соціальній сфері: адміністративно-правовий вектор трансформації в Україні. *Аналітично-порівняльне правознавство*. 2025. DOI: https://doi.org/10.24144/2788-6018.2025.04.1.37
13. Бабик М. Цифровізація адміністративних послуг в Україні: проблеми та перспективи розвитку. *Науковий вісник Ужгородського національного університету. Серія : Право*. 2022. № 70. URL: https://r2.donnu.edu.ua/items/6f190bc9-09b5-44-d7-a78f-a6f65e217f38/full
14. Ремета М. Взаємодія держави та суспільства в умовах цифровізації: практичні аспекти. *Економіка та суспільство*. 2026. № 85. DOI: https://doi.org/10.32782/2524-0072/2026-85-111
15. Gustafsson M., Matveieva O., Wihlborg E., Borodin Y., Mamatova T., Kvitka S. Adaptive governance amidst the war: overcoming challenges and strengthening collaborative digital service provision in Ukraine. *Government Information Quarterly*. 2025. Vol. 42. No. 3. Art. 102056. DOI: https://doi.org/10.1016/j.giq.2025.102056
16. Codreanu C. Developing e-government under cyber threats and Russia's war: Ukraine's Diia platform. *Smart Cities International Conference (SCIC) Proceedings*. 2025. Vol. 12. P. 429–437. URL: https://scrd.eu/index.php/scic/article/view/709 (
17. Жахалов Ю. Повноцінна тестова модель «Сяйва» має з'явитися до кінця 2026 року. На якому етапі розробка української LLM. *DOU.ua*. 2026. URL: https://dou.ua/lenta/news/national-llm-when-launch/
18. Створення української LLM «Сяйво»: прогрес, виклики та нові терміни запуску. *Економічна правда*. 2026. URL: https://epravda.com.ua/tehnologiji/stvorennya-ukrajinskoji-llm-syayvo-progres-vikliki-ta-novi-termini-zapusku-822657/
19. Київстар та Мінцифра переходять до ключового етапу розробки національної LLM // УНІАН. 2026. URL: https://www.unian.ua/society/kijivstar-ta-mincifra-perehodyat-do-klyuchovogo-etapu-rozrobki-nacionalnoji-llm-13248705.html
20. Soofi: Germany to develop sovereign AI language model // Heise Online. 2025. URL: https://www.heise.de/en/news/Soofi-Germany-to-develop-sovereign-AI-language-model-11083336.html
21. Apertus: a fully open, transparent, multilingual language model : press release // ETH Zurich. 2025. URL: https://ethz.ch/en/news-and-events/eth-news/news/2025/09/press-release-apertus-a-fully-open-transparent-multilingual-language-model.html
22. Europe's AI sovereignty is under threat. Could Mistral be the answer? // Fortune. 2026. URL: https://fortune.com/2026/08/05/mistral-europe-ai-sovereignty-us-openai-anthropic-google-deepmind/
23. GPT-NL: secure & ethical AI to power Dutch society // Security Delta. URL: https://securitydelta.nl/news/overview/gpt-nl-secure-ethical-ai-to-power-dutch-society
24. AI Sweden contributes to the development of open LLMs for transparent AI in Europe // AI Sweden. URL: https://www.ai.se/en/news/ai-sweden-contributes-development-open-llms-transparent-ai-europe
25. University of Turku and SiloGen launch consortium to build the world's largest open LLM : press release // University of Turku. 2023. URL: https://www.utu.fi/en/news/press-release/university-of-turku-and-silogen-launch-consortium-to-build-the-worlds-

largest ALIA, Europe's first public, open and multilingual AI infrastructure.
26. LLM AMALIA shows Portugal's potential. *Portuguese Government*. 2026. URL: https://portugal.gov.pt/en/gc25/communication/news/llm-amalia-shows-portugals-potential
27. Voukoutis L. et al. Meltemi: the first open large language model for Greek. *arXiv*. 2024. URL: https://arxiv.org/html/2407.20743v1
28. PULI. *Hungarian Research Centre for Linguistics*. URL: https://puli.nytud.hu/
29. Sułkowski Ł., Ulatowska R. Entrepreneurial strategies for national LLMs: Bielik and PLLuM advancing Poland's digital sovereignty. *Entrepreneurial Business and Economics Review*. 2025. Vol. 13. № 4. P. 165–184. URL: https://eber.uek.krakow.pl/index.php/eber/article/view/3100
30. Мінцифра розвиватиме інфраструктуру для впровадження ШІ в державні сервіси – працюємо над AI Factory // Міністерство цифрової трансформації України. 2025. URL: https://thedigital.gov.ua/news/technologies/mintsifra-rozvivatime-infrastrukturu-dlya-vprovadzhennya-shi-v-derzhavni-servisi-pratsyuemo-nad-ai-factory
31. Ustyuzhantseva O. V. Architectural agency in the global AI infrastructure: the case of India. *Spatial Economics*. 2025. Vol. 21. No. 3. P. 102–141. DOI: https://dx.doi.org/10.14530/se.2025.3.102-141
32. Розробку національної LLM «Сяйво» планують завершити в листопаді цього року. *Економічна правда*. 2026. URL: https://epravda.com.ua/biznes/rozrobku-nacionalnoji-llm-syayvo-planuyut-zavershiti-v-listopadi-cogo-roku-822675/
33. Пилипів І. ШІ з українським акцентом: що створюють Мінцифра та «Київстар» і кому це потрібно. *Економічна правда*. 2025. URL: https://epravda.com.ua/tehnologiji/shi-z-ukrajinskim-akcentom-shcho-stvoryuyut-mincifra-ta-kijivstar-i-navishcho-ce-vsim-nam-808668/
34. Укрдержархів передав 10 терабайтів даних для навчання ШІ «Сяйво». *Міністерство цифрової трансформації України*. 2026. URL: https://thedigital.gov.ua/news/technologies/ukrderzarkhiv-peredav-10-terabaytiv-danykh-dlia-navchannia-shi-siayvo
35. Джугалик Д. Українці отримають доступ до національного ШІ «Сяйво» у січні 2027 року // Межа. 2026. URL: https://mezha.ua/news/ukrainian-llm-public-release-in-january-314081/
36. Мінцифри та Nvidia запускають спільну ініціативу у сфері ШІ // Forbes Ukraine. 2025. URL: https://forbes.ua/news/mintsifri-ta-nvidia-zapuskayut-spilnu-initsiativu-u-sferi-shi-shcho-tse-dast-ukraini-17112025-34157
37. Сяйво – українці обрали назву для національної LLM // Міністерство цифрової трансформації України. 2026. URL: https://thedigital.gov.ua/news/technologies/siayvo-ukrayintsi-obraly-nazvu-dlia-natsionalnoyi-llm
38. Prahalad C. K., Ramaswamy V. Co-creation experiences: the next practice in value creation. *Journal of Interactive Marketing*. 2004. Vol. 18. No. 3. P. 5–14. DOI: https://doi.org/10.1002/dir.20015
39. Voorberg W. H., Bekkers V. J. J. M., Tummers L. G. A systematic review of co-creation and co-production: embarking on the social innovation journey. *Public Management Review*. 2015. Vol. 17. No. 9. P. 1333–1357. DOI: https://doi.org/10.1080/14719037.2014.930505
40. Шлях розвитку ШІ до 2030 року: знайомтеся з проєктом Стратегії та давайте фідбек // Міністерство цифрової трансформації України. 2026. URL: https://thedigital.gov.ua/news/shtuchnyy-intelekt/shliakh-rozvytku-shi-do-2030-roku-znayomtesia-z-proyektom-stratehiyi-ta-davayte-fidbek
41. Операційний план заходів з реалізації у 2026–2028 роках Стратегії розвитку штучного інтелекту на період до 2030 року : проєкт / Міністерство цифрової трансформації України. 2026. URL: https://ai-files.thedigital.gov.ua/documents/Проєкт%20ОП%20Стратегія%20розвитку%20ШІ%202030.docx.pdf (
42. Das D., Tessono C., Ahmed S. I., Guha S. Bureaucratic silences: what the Canadian AI Register reveals, omits, and obscures. *arXiv*. 2026. DOI: https://doi.org/10.48550/arXiv.2604.15514
43. Mwaura J. Who owns the news? The political economy of AI journalism in Africa. In: Matsilele T., Tshuma L. A. (eds.). *Generative AI in African News Media: Opportunities and Challenges*. London : Routledge, 2026. Chapter 5. URL: https://www.taylorfrancis.com/books/edit/10.4324/9781003627524/generative-ai-african-news-media-trust-matsilele-lungile-tshuma
44. Kang S. The case for the development of an Asian regional AI framework – expanding the discussion on sovereign AI to a regional level // Geopolitical Risks and Geoeconomics in International Economic Law. Singapore : Springer, 2026. P. 315–337. DOI: https://doi.org/10.1007/978-981-95-6996-0_16
45. Gatrell C., Muzio D., Post C., Wickert C. Here, there and everywhere: on the responsible use of artificial intelligence (AI) in management research and the peer-review process. *Journal of Management Studies*. 2024. Vol. 61. № 3. P. 739–751. DOI: https://doi.org/10.1111/joms.13045
46. INSAIT creates leading Bulgarian-first LLM with Gemma 2 // Google DeepMind. URL: https://deepmind.google/models/gemma/gemmaverse/insait/
47. Siggelkow N. Persuasion with case studies. *Academy of Management Journal*. 2007. Vol. 50. № 1. P. 20–24. DOI: https://doi.org/10.5465/amj.2007.24160882

REFERENCES

Aarab H. (2026). European digital sovereignty in the age of AI: regulation, infrastructure, and democratic legitimacy. *AI in Context of Digital Sovereignty* (pp. 333–355). Boca Raton: CRC Press. https://doi.org/10.1201/9781003581581-14

AI Sweden. AI Sweden contributes to the development of open LLMs for transparent AI in Europe. https://www.ai.se/en/news/ai-sweden-contributes-development-open-llms-transparent-ai-europe

Babyk M. (2022). Tsyfrovizatsiia administratyvnykh posluh v Ukraini: problemy ta perspektyvy rozvytku [Digitalization of administrative services in Ukraine: problems and development prospects]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo*, *70*. https://r2.donnu.edu.ua/items/6f190bc9-09b5-44d7-a78f-a6f65e217f38/full

Benjamin R. (2019). *Race after technology: abolitionist tools for the new Jim code*. Cambridge: Polity Press. https://doi.org/10.23987/sts.102639

Bradford A. (2020). *The Brussels effect: how the European Union rules the world*. Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

Codreanu C. (2025). Developing e-government under cyber threats and Russia's war: Ukraine's Diia platform. *Smart Cities International Conference (SCIC) Proceedings* (pp. 429–437). https://scrd.eu/index.php/scic/article/view/709

Das D., Tessono C., Ahmed S. I. & Guha S. (2026). Bureaucratic silences: what the Canadian AI Register reveals, omits, and obscures. *arXiv*. https://doi.org/10.48550/arXiv.2604.15514

Dzhuhalyk D. (2026). Ukraintsi otrymaiut dostup do natsionalnoho ShI «Siaivo» u sichni 2027 roku [Ukrainians will get access to the national AI "Syayvo" in January 2027]. *Mezha*. https://mezha.ua/news/ukrainian-llm-public-release-in-january-314081/

Ekonomichna pravda. (2026). Stvorennia ukrainskoi LLM «Siaivo»: prohres, vyklyky ta novi terminy zapusku [Creation of the Ukrainian LLM "Syayvo": progress, challenges, and new launch deadlines]. https://epravda.com.ua/tehnologiji/stvorennya-ukrajinskoji-llm-syayvo-progres-vikliki-ta-novi-termini-zapusku-822657/

Ekonomichna pravda. (2026). Rozrobku natsionalnoi LLM «Siaivo» planuiut zavershyty v lystopadi tsoho roku [Development of the national LLM "Syayvo" is planned to be completed in November of this year]. https://epravda.com.ua/biznes/rozrobku-nacionalnoji-llm-syayvo-planuyut-zavershiti-v-listopadi-cogo-roku-822675/

ETH Zurich. (2025). Apertus: a fully open, transparent, multilingual language model: press release. https://ethz.ch/en/news-and-events/eth-news/news/2025/09/press-release-apertus-a-fully-open-transparent-multilingual-language-model.html

Farrell H. & Newman A. L. (2019). Weaponized interdependence: how global economic networks shape state coercion. *International Security*, *1*(44), 42–79. https://www.jstor.org/stable/26777882

Floridi L. (2019). Establishing the rules for building trustworthy AI. *Nature Machine Intelligence*, *6*(1), 1–2. https://doi.org/10.1038/s42256-019-0055-y

Forbes Ukraine. (2025). Mintsyfry ta Nvidia zapuskaiut spilnu initsiatyvu u sferi ShI [Ministry of Digital Transformation and Nvidia launch joint initiative in the field of AI]. https://forbes.ua/news/mintsifrita-nvidia-zapuskayut-spilnu-initsiativu-u-sferi-shishcho-tse-dast-ukraini-17112025-34157

Fortune. (2026). Europe's AI sovereignty is under threat. Could Mistral be the answer?. https://fortune.com/2026/08/05/mistral-europe-ai-sovereignty-us-openai-anthropic-google-deepmind/

Gatrell C., Muzio D., Post C. & Wickert C. (2024). Here, there and everywhere: on the responsible use of artificial intelligence (AI) in management research and the peer-review process. *Journal of Management Studies*, *3*(61), 739–751. https://doi.org/10.1111/joms.13045

George J. (2026). Assessing sovereign AI: a two-pronged framework. *Georgetown University*. https://cset.georgetown.edu/article/assessing-sovereign-ai-a-two-pronged-framework/

Google DeepMind. INSAIT creates leading Bulgarian-first LLM with Gemma 2. https://deepmind.google/models/gemma/gemmaverse/insait/

Gustafsson M., Matveieva O., Wihlborg E., Borodin Y., Mamatova T. & Kvitka S. (2025). Adaptive governance amidst the war: overcoming challenges and strengthening collaborative digital service provision in Ukraine. *Government Information Quarterly*, *3*(42), Art. 102056. https://doi.org/10.1016/j.giq.2025.102056

Heise Online. (2025). Soofi: Germany to develop sovereign AI language model. https://www.heise.de/en/news/Soofi-Germany-to-develop-sovereign-AI-language-model-11083336.html

Hungarian Research Centre for Linguistics. PULI. https://puli.nytud.hu/

Kang S. (2026). The case for the development of an Asian regional AI framework — expanding the discussion on sovereign AI to a regional level. *Geopolitical Risks and Geoeconomics in International Economic Law* (pp. 315–337). Singapore: Springer. https://doi.org/10.1007/978-981-95-6996-0_16

McKinsey & Company. (2025). The sovereign AI agenda: moving from ambition to reality. https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/tech-forward/the-sovereign-ai-agenda-moving-from-ambition-to-reality

Medianyk V. A. (2025). Tsyfrovizatsiia publichnoho upravlinnia v sotsialnii sferi: administratyvno-pravovyi vektor transformatsii v Ukraini [Digitalization of public administration in the social sphere: administrative and legal vector of transformation in Ukraine].

Analitychno-porivnialne pravoznavstvo. https://doi.org/10.24144/2788-6018.2025.04.1.37

Ministerstvo tsyfrovoi transformatsii Ukrainy. (2025). Mintsyfra rozvyvatyme infrastrukturu dlia vprovadzhennia ShI v derzhavni servisy — pratsiuiemo nad AI Factory [The Ministry of Digital Transformation will develop infrastructure for the implementation of AI in public services — working on AI Factory]. https://thedigital.gov.ua/news/technologies/mintsifra-rozvivatime-infrastrukturu-dlya-vprovadzhennya-shi-v-derzhavni-servisi-pratsyuemo-nad-ai-factory

Ministerstvo tsyfrovoi transformatsii Ukrainy. (2026). Ukrderzharkhiv peredav 10 terabaitiv danykh dlia navchannia ShI «Siaivo» [Ukrderzharkhiv transferred 10 terabytes of data for training the "Syayvo" AI]. https://thedigital.gov.ua/news/technologies/ukrderzarkhiv-peredav-10-terabaytiv-danykh-dlia-navchannia-shi-siayvo

Ministerstvo tsyfrovoi transformatsii Ukrainy. (2026). Siaivo – ukraintsi obraly nazvu dlia natsionalnoi LLM [Syayvo – Ukrainians chose the name for the national LLM]. https://thedigital.gov.ua/news/technologies/siayvo-ukrayintsi-obraly-nazvu-dlia-natsionalnoyi-llm

Ministerstvo tsyfrovoi transformatsii Ukrainy. (2026). Shliakh rozvytku ShI do 2030 roku: znaiomtesia z proiektom Stratehii ta davaite fidbek [Path of AI development until 2030: get acquainted with the Strategy project and give feedback]. https://thedigital.gov.ua/news/shtuchnyy-intelekt/shliakh-rozvytku-shi-do-2030-roku-znayomtesia-z-proyektom-stratehiyi-ta-davayte-fidbek

Ministerstvo tsyfrovoi transformatsii Ukrainy. (2026). Operatsiinyi plan zakhodiv z realizatsii u 2026–2028 rokakh Stratehii rozvytku shtuchnoho intelektu na period do 2030 roku: proiekt [Operational action plan for the implementation in 2026–2028 of the Artificial Intelligence Development Strategy for the period up to 2030: project]. https://ai-files.thedigital.gov.ua/documents/Proiekt%20OP%20Stratehiia%20rozvytku%20ShI%202030.docx.pdf

Mwaura J. (2026). Who owns the news? The political economy of AI journalism in Africa. *Generative AI in African News Media: Opportunities and Challenges* (pp. 5). London: Routledge. https://www.taylorfrancis.com/books/edit/10.4324/9781003627524/generative-ai-african-news-media-trust-matsilele-lungile-tshuma

Noble S. U. (2018). *Algorithms of oppression: how search engines reinforce racism*. New York: New York University Press. https://www.researchgate.net/publication/327109256_Algorithms_of_Oppression_How_Search_Engines_Reinforce_Racism

Portuguese Government. (2026). LLM AMALIA shows Portugal's potential. https://portugal.gov.pt/en/gc25/communication/news/llm-amalia-shows-portugals-potential

Prahalad C. K. & Ramaswamy V. (2004). Co-creation experiences: the next practice in value creation. *Journal of Interactive Marketing*, *3*(18), 5–14. https://doi.org/10.1002/dir.20015

Pylypiv I. (2025). ShI z ukrainskym aktsentom: shcho stvoriuiut Mintsyfra ta «Kyivstar» i komu tse potribno [AI with a Ukrainian accent: what the Ministry of Digital Transformation and Kyivstar are creating and who needs it]. *Ekonomichna pravda*. https://epravda.com.ua/tehnologiji/shi-z-ukrajinskim-akcentom-shcho-stvoryuyut-mincifra-ta-kijivstar-i-navishcho-ce-vsim-nam-808668/

Remeta M. (2026). Vzaiemodiia derzhavy ta suspilstva v umovakh tsyfrovizatsii: praktychni aspekty [Interaction of the state and society in conditions of digitalization: practical aspects]. *Ekonomika ta suspilstvo*, *85*. https://doi.org/10.32782/2524-0072/2026-85-111

Security Delta. GPT-NL: secure & ethical AI to power Dutch society. https://securitydelta.nl/news/overview/gpt-nl-secure-ethical-ai-to-power-dutch-society

Siggelkow N. (2007). Persuasion with case studies. *Academy of Management Journal*, *1*(50), 20–24. https://doi.org/10.5465/amj.2007.24160882

Singh S. K. & Sengupta S. (2025). Sovereign AI: rethinking autonomy in the age of global interdependence. *arXiv*. https://doi.org/10.48550/arXiv.2511.15734

Sułkowski Ł. & Ulatowska R. (2025). Entrepreneurial strategies for national LLMs: Bielik and PLLuM advancing Poland's digital sovereignty. *Entrepreneurial Business and Economics Review*, *4*(13), 165–184. https://eber.uek.krakow.pl/index.php/eber/article/view/3100

Tanner B., Kerry C. F., Wyckoff A., Kyosovska N., Renda A. & Tabassi E. (2026). Is AI sovereignty possible? Balancing autonomy and interdependence. *Washington: Brookings Institution ; Brussels: CEPS*. https://www.brookings.edu/articles/is-ai-sovereignty-possible-balancing-autonomy-and-interdependence/

UNIAN. (2026). Kyivstar ta Mintsyfra perekhodiat do kliuchovoho etapu rozrobky natsionalnoi LLM [Kyivstar and the Ministry of Digital Transformation move to the key stage of developing the national LLM]. https://www.unian.ua/society/kijivstar-ta-mincifra-perehodyat-do-klyuchovogo-etapu-rozrobki-nacionalnoji-llm-13248705.html

University of Turku. (2023). University of Turku and SiloGen launch consortium to build the world's largest open LLM: press release. https://www.utu.fi/en/news/press-release/university-of-turku-and-silogen-launch-consortium-to-build-the-worlds-largest

Ustyuzhantseva O. V. (2025). Architectural agency in the global AI infrastructure: the case of India. *Spatial Economics*, *3*(21), 102–141. https://dx.doi.org/10.14530/se.2025.3.102-141

Voorberg W. H., Bekkers V. J. J. M. & Tummers L. G. (2015). A systematic review of co-creation and co-produc-

tion: embarking on the social innovation journey. *Public Management Review*, *9*(17), 1333–1357. https://doi.org/10.1080/14719037.2014.930505

Voukoutis L. & et al. (2024). Meltemi: the first open large language model for Greek. *arXiv*. https://arxiv.org/html/2407.20743v1

Zhakhalov Yu. (2026). Povnotsinna testova model «Siaiva» maie ziavytysia do kintsia 2026 roku. Na yakomu etapi rozrobka ukrainskoi LLM [A full-fledged test model of "Syayvo" is expected by the end of 2026. At what stage is the development of the Ukrainian LLM]. *DOU.ua*. https://dou.ua/lenta/news/national-llm-when-launch/

Zuboff S. (2019). *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: PublicAffairs. https://we.riseup.net/assets/533560/Zuboff%2C+Shoshana.The+Age+of+Surveillance+Capitalism.2019.pdf

This research received no external funding.
The author declares no conflict of interest.
The author solely performed the conceptualization, methodology, source analysis, original draft writing, and editing of this article.
In preparing this manuscript, the author used the generative AI tool Claude (Anthropic) to assist with drafting portions of text, structuring sections, formatting citations, and searching for relevant sources. All sources used were verified by the author for accuracy, and the final content, analytical conclusions, and interpretations belong to the author. The AI tool is not a co-author of this article, in accordance with the journal's requirements. This paper's approach to transparent AI disclosure follows the recommendations outlined in [46].

Стаття надійшла до редакції / Received: 23.07.2026
Статтю прийнято до публікації / Accepted: 10.08.2026
Оприлюднено / Published: 08.10.2026

УДК 005.5:004.78(477)
JEL: L86; M10; M15; O33
DOI: https://doi.org/10.32983/2222-4459-2026-8-510-518

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ СТРАТЕГІЙ УПРАВЛІННЯ БІЗНЕС-ПРОЦЕСАМИ В ІТ-КОМПАНІЯХ УКРАЇНИ

© 2026 **БАБЕНКО Д. І.**

УДК 005.5:004.78(477)
JEL: L86; M10; M15; O33

Бабенко Д. І. Сучасні тенденції розвитку стратегій управління бізнес-процесами в ІТ-компаніях України

У статті здійснено аналіз і систематизацію наявних стратегій управління бізнес-процесами (Business Process Management, BPM), які застосовуються ІТ-компаніями України в умовах цифрової трансформації та підвищеної турбулентності зовнішнього середовища. Обґрунтовано, що специфіка вітчизняного ІТ-сектора – висока частка нематеріальних активів, розподілений і релокований характер команд, посилені вимоги до кібербезпеки та необхідність забезпечення процесної резильєнтності в умовах воєнного стану – зумовлює потребу в диференційованому підході до вибору стратегії BPM залежно від бізнес-моделі компанії (сервісної, продуктової чи гібридної) та рівня зрілості її процесів. За результатами узагальнення вітчизняного та зарубіжного досвіду виокремлено й систематизовано п'ять основних стратегій управління бізнес-процесами: класичну регламентовану, Agile-орієнтовану, ощадливу (Lean-оптимізаційну), дата-орієнтовану (Data-Driven/Process Mining) та гібридну, які наведено в порівняльній таблиці за критеріями сутності, переваг, обмежень і прикладів застосування. Розроблено логічну матрицю вибору стратегії управління бізнес-процесами ІТ-компанії залежно від рівня динамічності зовнішнього середовища та ступеня необхідної стандартизації внутрішніх процесів. Установлено, що більшість українських ІТ-компаній використовують не одну «чисту» стратегію, а поєднання елементів Agile-методологій з окремими регламентувальними механізмами класичного BPM, що відповідає концепції організаційної дворукості (ambidexterity). Виявлено тенденцію до поступового переходу від суб'єктивно-експертних методів оцінювання процесів до об'єктивних, заснованих на даних інструментів (Process Mining, BI-аналітика), що зумовлено потребою підвищення процесної резильєнтності в умовах релокації бізнесу та порушень інфраструктури. Результати дослідження можуть бути використані менеджментом ІТ-компаній для обґрунтованого вибору та коригування стратегії управління бізнес-процесами відповідно до специфіки бізнес-моделі та зовнішніх викликів.

Ключові слова: *бізнес-процеси; управління бізнес-процесами; ІТ-компанії; ІТ-сектор України; стратегії управління; цифрова трансформація; автоматизація бізнес-процесів; оптимізація бізнес-процесів; інноваційні технології; ефективність управління.*

Рис.: *1.* ***Табл.:*** *1.* ***Бібл.:*** *15.*

Бабенко Дмитро Ігорьович *– аспірант кафедри менеджменту і публічного адміністрування, Харківський національний університет міського господарства ім. О. М. Бекетова (вул. Чорноглазівська, 17, Харків, 61002, Україна)*
E-mail: *dmytro.babenko2@kname.edu.ua*
ORCID: *https://orcid.org/0009-0005-7749-6387*