Digital Sovereignty Index [v. 1.1]:
An expert-coded country ranking of Digital Sovereignty

Abstract: This article proposes a theory-driven, public policy-oriented Digital Sovereignty Index (DSI) to measure the degree to which states exercise control over the technological systems upon which contemporary sovereignty increasingly depends. The framework operationalizes digital sovereignty through four analytical dimensions—Hardware, Software, Cognition, and Governance—comprising sixteen expert-coded subdimensions evaluated across 101 countries. After reviewing existing approaches to measuring digital sovereignty, the article presents the theoretical and methodological foundations of the DSI and applies it comparatively to identify distinct trajectories of technological development. The findings show that digital sovereignty is a multidimensional and progressive phenomenon, shaped by the interaction between Infrastructure Capacity and Actuation Capacity rather than by technological assets alone. The DSI provides a transparent and reproducible framework for comparative research and evidence-based public policy.

Keywords: Digital Sovereignty, Public Policy, Technological Governance, Comparative Indexes, International Political Economy.

RESEARCH LEAD

Isabela Wagnerovna **ROCHA-DASHICHEVA**

Institute of Political Science of the University of Brasília (IPOL UnB), BRICS+ Forum for Strategic Technologies (BRICS Tech Forum), GEPSI Data IREL UnB, rocha@bricstechforum.org.

RESEARCH COORDINATORS

Aleksandr Denisovich **DASHICHEV**

Russian Academy of Sciences (RAS), BRICS+ Forum for Strategic Technologies (BRICS Tech Forum), dashichev@bricstechforum.org.

Laura Beatriz **LUDOVICO**

Pontifical Catholic University of Minas Gerais (PUC-MG), BRICS+ Forum for Strategic Technologies (BRICS Tech Forum), GEPSI Data IREL UnB, ludovico@bricstechforum.org.

Felipe Camargo **PIAZZA**

Postgraduate candidate in Digital Law (ITS-Rio/UERJ), Bachelor of Laws (University of São Paulo - USP), Legal Advisor at the BRICS+ Forum for Strategic Technologies (BRICS Tech Forum), piazza@bricstechforum.org.

Ergon Cugler de Morae **SILVA**

Getúlio Vargas Foundation (FGV), Council for Sustainable Economic and Social Development (CDESS) of the Federative Republic of Brazil, contato@ergoncugler.com.

José Carlos **VAZ**

University of São Paulo (USP), Study Group on Technology and Innovation in Public Management,vaz@usp.br.

João Pedro Falcão de Oliveira **LUCENA**

Instituto de Educação Superior de Brasília (IESB), United Nations Development Programme (UNDP), GEPSI Data IREL UnB.

RESEARCH ASSISTANTS

Giovana **CARNEIRO**

Getulio Vargas Foundation, GEPSI Data IREL UnB.

Letícia **TEIXEIRA**

Federal University of Rio de Janeiro (UFRJ), BRICS+ Forum for Strategic Technologies.

Israel **ROCHA**

Federal University of Rio de Janeiro (UFRJ), Simulations and Scenarios Laboratory EGN, GEPSI Data IREL UnB.

Natália **MAGALHÃES**

Federal University of Santa Catarina (UFSC), BRICS+ Forum for Strategic Technologies.

João **CAMELLO**

University of Brasília (UnB), GEPSI Data IREL UnB.

Caio Ivo **SIMONI**

Research Group on Brazilian Foreign Policy (GEPEB) of the Unified Teaching Center of Brasília (CEUB), GEPSI Data IREL UnB.

Robson Cunha **RAEL**

Institute of International Relations of the University of Brasília (IREL UnB), Lab BRICS IREL UnB.

Iasmim Verônica Cardoso Alves de Souza e **SILVA**

Catholic University of Santos (UNISANTOS), GEPSI Data IREL UnB.

Claudio Andrés **TÉLLEZ-ZEPEDA**

Technological Institute of Aeronautics (ITA), GEPSI Data IREL UnB.

1 INTRODUCTION

Digital Sovereignty is, today, synonymous with Sovereignty as digital infrastructures shape the conditions under which sovereignty itself is exercised. Cloud computing, semiconductors, artificial intelligence, telecommunications networks, satellite systems, cybersecurity architectures, and platform ecosystems no longer operate merely as economic sectors or technical tools, but as strategic infrastructures through which states accumulate power, coordinate institutions, regulate populations, and project geopolitical influence. Under these conditions, technological dependency acquires consequences extending far beyond industrial competitiveness alone (Zuboff, 2019; Morozov, 2022; Hardt and Negri, 2001). Dependence on foreign-controlled infrastructures exposes states to asymmetrical vulnerabilities capable of affecting economic continuity (Srnicek, 2017; Couldry and Mejias, 2019), informational integrity, political autonomy, and national security itself (Rocha-Dashicheva, 2026).

At the same time, the contemporary technological order remains deeply unequal (Varoufakis, 2024; Morozov, 2022). A relatively small number of countries and corporations continue to dominate advanced semiconductor production, hyperscale cloud infrastructure, operating systems, standards-setting processes, artificial intelligence computation, and global digital platforms. Much of the Global South, meanwhile, experiences digital expansion through externally governed ecosystems, often integrating into global digital systems without proportional control over the infrastructures enabling them. As technological systems become increasingly central to governance, military coordination, communication, finance, and industrial production, the question of digital sovereignty emerges as one of the defining geopolitical questions of the twenty-first century.

The foregoing literature converges upon this diagnosis despite important theoretical disagreements. Whether interpreted through Empire (Hardt and Negri, 2001), platform capitalism (Srnicek, 2017), surveillance capitalism (Zuboff, 2019), data colonialism (Couldry and Mejias, 2019), techno-feudalism (Varoufakis, 2024), or broader critiques of digital capitalism (Morozov, 2022), these approaches share the recognition that technological power is increasingly exercised through infrastructures, software, institutions, and knowledge systems. And although these authors differ in their explanations of the political-economic logic underlying this transformation, they converge in identifying the growing strategic significance of technological capabilities and the asymmetries generated by their concentration.

If digital sovereignty has become a central condition of contemporary statehood, its insufficiency constitutes a public problem that demands responses from both governments and society. Producing systematic assessments and cross-national comparisons of countries' levels of digital sovereignty can support the formulation of national technological strategies and industrial policies. Such strategies require a high degree of public policy integration (Vaz, 2016), given the complexity and multidimensional character of technological sovereignty.

Understanding this complexity of digital sovereignty demands a significant analytical effort. Digital sovereignty is a construct that represents an abstract phenomenon, which requires a high degree of interpretation of reality, as it is necessary to identify variables capable of enabling analyses of its multiple dimensions. The use of synthetic indicators provides a useful instrument in this type of situation, as such indicators combine indicators related to specific aspects of reality that characterize the broader phenomenon under analysis, simultaneously producing analytical and synthetic resources for assessment and comparison. Without denying complexity, synthetic indicators simplify the understanding of complexity, facilitate the analysis and interpretation of results, and their communication and circulation in public debate (Maggino, 2017).

The construction of a Digital Sovereignty Index therefore serves three research-agenda objectives: (1) to identify and analyze the multiple dimensions of digital sovereignty in specific countries; (2) to enable synthetic assessments of the level of digital sovereignty; and (3) to enable cross-country comparisons that provide a comprehensive understanding of the global context of inequality among countries with respect to digital sovereignty.

The DSI presented in this paper seeks to translate these theoretical insights into an empirical framework capable of systematically measuring the material and institutional conditions through which digital sovereignty is exercised. It is a public-policy oriented, theory-driven and expert-coded measure of national capabilities and domains of control across critical technological layers, emphasizing geopolitical value capture rather than the mere presence or diffusion of specific technologies. The index evaluates countries across four analytical dimensions: Hardware, Software, Cognition, and Governance; each composed of four subdimensions assessed through a standardized 0-4 expert-coding framework based on publicly documented evidence - culminating in 16 expert-assessments per country. These assessments are then aggregated into synthetic measures of Infrastructure Capacity (normalized mean of Hardware and Software scores), Actuation Capacity (normalized mean of Cognition and Governance scores), and overall Digital Sovereignty (normalized mean of all 16 subdimensions), enabling transparent and comparable cross-national analysis.

This version [1.1] of the DSI evaluates 101 countries across these sixteen subdimensions, producing 1,616 expert-coded assessments supported by an archived repository of 1,265 unique source documents. The complete dataset is publicly available through the Harvard Dataverse (Rocha-Dashicheva et al., 2026b), ensuring full transparency, reproducibility, and independent verification of the methodology and results.

In the following sections, we first review the principal conceptual and methodological approaches to measuring digital sovereignty, identifying their respective contributions and limitations (Section 2). We then present the theoretical foundations, analytical architecture, and methodological procedures underlying the Digital Sovereignty Index (Section 3). Finally, we apply the DSI to a comparative analysis of 101 countries, examining the global distribution of digital sovereignty, the distinct developmental trajectories revealed by Infrastructure and Actuation Capacities, and the broader implications of the results for industrial policy, technological strategy, and contemporary geopolitical competition (Section 4). In the Conclusions and Final Considerations (Section 5), we discuss the principal methodological and empirical contributions of the DSI, its current limitations, and outline a broader research agenda for the continued refinement of digital sovereignty measurement and its application to comparative public policy and international political economy.

2 REVIEWING EXISTING INDEXES

In this section, we review the principal indices and conceptual frameworks developed to assess digital sovereignty, focusing on how each defines the construct, selects indicators, and translates it into measurable categories. Digital sovereignty is a construct rooted in interpretations of social reality, even though it is amenable to measurement and comparison via objective variables. The existence, thus, of multiple tools for measuring digital sovereignty allows for greater analytical diversity, as it offers a degree of flexibility in interpreting the phenomenon. To analyze these indices and conceptual frameworks, we adopt an analytical lens based on a sociotechnical perspective that considers the full range of factors and elements within technology usage chains. We examine the (2.1) Nextcloud Digital Sovereignty Index, the (2.2) European Digital Resilience Index, (2.3) Di Marco et al.'s conceptual framework, and the (2.4) Tricontinental BRICS Digital Sovereignty Index, before consolidating the comparison through the (2.5) policy-oriented ontology adopted by the DSI proposed in this study.

In this section, we can indeed observe the maturation of digital sovereignty as an object of comparative measurement. The reviewed approaches evolve from single-proxy indicators (Nextcloud), to multiple observable proxies (EDRIX), to multidimensional conceptual frameworks (Di Marco et al.), and finally to comprehensive empirical operationalization (Tricontinental). Building upon these advances, the DSI proposed here seeks to align the ontology of digital sovereignty with analytically delimited indicators, a common scaling framework, and a policy-oriented methodology suitable for comparative analysis and public decision-making.

2.1 Nextcloud Digital Sovereignty Index

The Nextcloud Digital Sovereignty Index (DSI) constitutes one of the first explicit attempts to quantify digital sovereignty through an internationally comparable indicator. Developed by Nextcloud GmbH, the index estimates countries' levels of digital sovereignty by measuring the public deployment of approximately fifty self-hosted open-source collaboration applications, normalized by population (2025). Methodologically, the index operationalizes digital sovereignty through a single observable variable: the public deployment of approximately fifty self-hosted collaboration applications like Nextcloud, ownCloud, Seafile, Jitsi Meet, Matrix/Element, Rocket.Chat, Mattermost, OpenProject and others. Countries therefore receive higher scores according to the number of publicly visible deployments per capita, implicitly treating the diffusion of this specific class of software as a proxy for national digital sovereignty.

This operationalization constitutes a significant reduction of the concept by reducing Digital Sovereignty to the domestic adoption of a particular category of software, irrespective of the broader technological, industrial, institutional, or geopolitical conditions under which these applications operate. It effectively mistakes the uppermost layer of the technological stack for the stack itself. Collaboration software represents only the visible tip of a much deeper technological stack, ultimately dependent upon cloud infrastructure, data centers, operating systems, semiconductor and other technological supply chains, telecommunications networks, satellite systems, standards-setting processes, artificial intelligence capabilities, cognitive frameworks for technology adoption and the institutional capacity of states to regulate and strategically coordinate these technologies. A country may therefore host thousands of self-hosted applications while remaining almost entirely dependent upon foreign-controlled infrastructures across every underlying layer of the digital ecosystem.

Even within the framework proposed in this study, the phenomenon captured by the Nextcloud DSI corresponds only partially to a single subdimension of the DSI: S1 (State Operating Environment). The deployment of self-hosted collaboration software may provide limited evidence of the domestic use of alternative software ecosystems, but offers virtually no information regarding cloud infrastructure (S2), critical public digital systems (S3), interoperability and standards (S4), or any of the Hardware, Cognition, or Governance dimensions. Consequently, the index attempts to infer national digital sovereignty from a narrow empirical proxy that represents, at best, one limited component of one out of sixteen subdimensions.

Ultimately, the Nextcloud DSI does not measure digital sovereignty, but the diffusion of a particular software ecosystem, and its central limitation is that of validity. The methodology substitutes a complex, multidimensional phenomenon with a single observable variable, extrapolating from the deployment of self-hosted collaboration software to conclusions regarding national technological sovereignty. Such an inference is methodologically indefensible. The presence of collaboration applications provides no meaningful evidence regarding a state's capacity to produce semiconductors, operate cloud infrastructure, establish technical standards, regulate digital markets, develop artificial intelligence, or coordinate national technological strategy. Consequently, the indicator cannot support the conclusions it purports to draw as the operationalization fails to capture the phenomenon it claims to measure.

This limitation extends beyond methodological precision and carries significant implications for public policy because indicators shape priorities, influence resource allocation, and guide national technological strategies. An index that equates digital sovereignty with the deployment of self-hosted collaboration software risks directing policy attention toward the adoption of specific applications while neglecting the productive, infrastructural, cognitive, and institutional capabilities that ultimately determine sovereign technological capacity. By equating sovereignty with the domestic deployment of self-hosted software, the index risks encouraging governments to pursue technological independence at the application layer while remaining structurally dependent across the productive, infrastructural, cognitive, and institutional layers where sovereignty is ultimately exercised. The result is not merely conceptual confusion, but the risk of systematically misdirected public policy.

2.2 European Digital Resilience Index (EDRIX)

The European Digital Resilience Index (EDRIX) was developed to provide a quantitative assessment of what its authors describe as European digital sovereignty through a fully automated, data-driven methodology based exclusively on publicly available and reproducible data sources (EDRIX, 2026). Unlike expert-coded approaches, the index explicitly rejects subjective assessments and policy analysis, arguing instead that digital sovereignty should be measured through observable digital outcomes rather than stated governmental intentions. Since version 2.0, the index is generated quarterly through an automated pipeline without manual curation, relying exclusively on automatically refreshable public datasets.

Methodologically, EDRIX is structured around four analytical pillars comprising five raw metrics. The (1) Developer Ecosystem pillar measures the density of GitHub developers per capita using GitHub's Innovation Graph. (2) Grassroots Adoption combines two indicators derived from Cloudflare Radar: the share of Linux desktop users and the combined market share of Firefox and Opera browsers. (3) Private Sector Resilience evaluates the hosting infrastructure of the one thousand most-visited domains under each national top-level domain (TLD), assigning a sovereignty score according to the ownership of the hosting provider's autonomous system. Finally, (4) Public Sector Resilience applies the same hosting-sovereignty methodology to a small curated sample of official government websites, including the head of state, the national government portal, and the capital city's official website.

Each raw metric is normalized across the twenty-seven European Union member states using min-max normalization on a 0-10 scale. Where a pillar contains multiple metrics, these are averaged before being renormalized, and the final EDRIX score is obtained as the mean of the four pillar scores. Consequently, all scores are relative to the contemporary distribution of EU member states rather than to an absolute external benchmark, and are recalculated quarterly as the underlying data are refreshed.

While considerably more sophisticated than the Nextcloud DSI, the EDRIX nevertheless presents a fundamental problem of construct validity. The index indeed seeks to measure digital sovereignty, yet its empirical operationalization remains largely confined to observable indicators of digital resilience, software adoption, and hosting location. These variables work just as proxies that undoubtedly describe important characteristics of national digital ecosystems, but they do not, either individually or collectively, constitute digital sovereignty itself. Rather, they represent a limited subset of outcomes associated with broader technological development, leaving unmeasured the productive, institutional, industrial, cognitive, and geopolitical capacities through which states actually exercise sovereign control over digital technologies.

This conceptual mismatch becomes evident in the very architecture of the index. None of its five raw metrics directly evaluates a state's capacity to produce - or ensure the access to - semiconductors, develop telecommunications equipment, own hyperscale cloud infrastructure, manufacture critical hardware, establish technical standards, coordinate national innovation systems, formulate technological strategy, or regulate digital markets. Instead, sovereignty is inferred indirectly from indicators such as GitHub developer density, Linux desktop adoption, browser market shares, and the geographical location of hosting providers. Consequently, the operationalization substitutes manifestations of digital participation for the underlying capabilities that make technological sovereignty possible.

The (1) Developer Ecosystem pillar provides perhaps the clearest illustration of this problem. The number of GitHub developers per capita is treated as evidence of national digital sovereignty, **despite GitHub itself being a proprietary platform owned and governed by Microsoft**. Participation within a proprietary platform governed by a foreign corporation software ecosystem is therefore interpreted as evidence of sovereign technological capability, even though such activity says little about domestic control over software production, computational infrastructure, standards-setting, or strategic technological autonomy. The indicator measures participation in the global digital economy rather than sovereignty over it.

Similar conceptual difficulties arise within the (2) Grassroots Adoption pillar. The use of Linux desktop market share and the combined adoption of Firefox and Opera browsers assumes that preferences for particular software products constitute evidence of national digital sovereignty. Yet software adoption reflects choices made by individual users rather than the strategic capacities of states. Moreover, these technologies themselves remain embedded within complex transnational production networks: Firefox depends extensively on Google search revenues, Opera is owned by a Chinese consortium, and Linux distributions are developed through globally distributed communities and corporations. Their domestic adoption therefore provides, at most, indirect evidence of software preferences in some way less dependent on the big techs rather than sovereign technological capability.

The two (3 and 4) Resilience pillars introduce a similar conceptual leap by equating domestic hosting with digital sovereignty. While the geographical location of servers may contribute to resilience against certain operational risks, hosting location alone reveals little about ownership of the underlying cloud infrastructure, control over virtualization technologies, dependence upon foreign semiconductor supply chains, or the capacity to reproduce those infrastructures domestically. A government website hosted within national borders may still rely entirely upon foreign hardware, foreign cloud providers, foreign operating systems, and foreign software ecosystems. The operationalization therefore repeatedly conflates the physical location of digital services with sovereign control over the technological stack that sustains them.

The implications of this construct mismatch extend beyond methodological concerns and into the formulation of public policy - like Nextcloud's. Again, public indicators influence investment priorities, legislative agendas, industrial strategies, and national technology roadmaps. By presenting software adoption, platform participation, and hosting location as proxies for digital sovereignty, EDRIX risks directing policy attention toward optimizing observable digital outcomes rather than strengthening the structural capabilities upon which technological sovereignty ultimately depends. Governments encouraged by such indicators may prioritize increasing Linux adoption, promoting open-source software, expanding domestic hosting, or stimulating developer communities while leaving largely unaddressed the strategic challenges of semiconductor production, cloud ownership, telecommunications infrastructure, artificial intelligence, scientific capacity, standards-setting, and national technological coordination.

The consequence is the possibility of systematically misdirecting industrial and technological policy. States may improve their position within the index while making little substantive progress toward reducing structural technological dependence. In this sense, operationalization risks rewarding the visible manifestations of digital development while overlooking the productive, institutional, and geopolitical foundations upon which genuine technological sovereignty ultimately rests.

2.3 Di Marco (2025) Conceptual Framework for Digital Sovereignty

The Digital Sovereignty Index proposed by Di Marco (2025) adopts a considerably broader understanding of digital sovereignty than the previously discussed approaches. Developed within the Joint Research Centre (JRC) of the European Commission, the framework defines digital sovereignty as the capacity to exercise strategic autonomy in the digital domain while remaining open and connected to global networks. The framework organizes the concept into four interconnected dimensions: Digital Governance, Infrastructure, Software and Data, Digital Products and Markets, and People, seeking to capture the institutional, technological, economic, and societal conditions supporting the European Union's strategic autonomy in the digital domain.

Compared to the previously discussed approaches, Di Marco et al. (2025) represents a significant conceptual advance by explicitly recognizes the multidimensional character of the phenomenon, incorporating technological infrastructures, industrial capabilities, governance arrangements, market structures, and societal capacities into a unified analytical model instead of reducing Digital Sovereignty to a single technological indicator or a narrow set of observable digital outcomes It also correctly identifies the interdependence among these dimensions, arguing that digital sovereignty emerges from their interaction rather than from technological assets alone. In this respect, the framework converges with the central theoretical premise adopted by the DSI presented in this study: that digital sovereignty cannot be adequately understood through isolated technological indicators, but must instead be approached as a systemic property of national technological ecosystems.

Nevertheless, the principal limitation of the framework lies precisely where its stated objective ends. While it successfully establishes a broad conceptual architecture for understanding digital sovereignty, it does not operationalize that architecture into a transparent measurement framework. The report deliberately remains at the level of conceptual organization and policy discussion, providing neither measurable indicators nor explicit coding procedures, scoring criteria, aggregation rules, weighting schemes, or validation strategies capable of transforming its four dimensions into a reproducible comparative index. Consequently, although the framework offers a valuable heuristic for organizing the debate on digital sovereignty, it cannot itself serve as an empirical instrument for systematic cross-national comparison.

A second methodological difficulty concerns the analytical boundaries between the proposed dimensions. Although the framework distinguishes Digital Governance, Digital Infrastructures, Software and Data, Digital Products and Markets, and People as separate analytical layers, the empirical phenomena associated with these categories frequently overlap. Innovation, for example, simultaneously contributes to industrial capacity, human capital, infrastructure, and governance. Likewise, cybersecurity, interoperability, and digital skills influence several dimensions simultaneously. Without explicit operational rules delimiting where particular forms of evidence should be classified, the framework provides limited guidance for consistent empirical coding and comparative replication. This ambiguity becomes particularly relevant when multiple researchers seek to evaluate the same country or compare results across cases.

Therefore, unlike the DSI, the framework does not distinguish between conceptual interaction and analytical classification, leaving unresolved how overlapping empirical phenomena should be consistently operationalized.

2.4 Tricontinental Digital Sovereignty Index

Published in 2026, nearly concurrently with the present study, the Tricontinental BRICS Digital Sovereignty Index represents one of the first systematic attempts to operationalize digital sovereignty through a comprehensive comparative framework. Developed by the Tricontinental: Institute for Social Research, the index evaluates the BRICS countries across four dimensions: (1) Data Ownership, (2) Digital Infrastructure, (3) Cyberspace Governance, and (4) Digital Capability, and sixteen indicators, supported by an extensive AI-assisted research pipeline. Its methodology combines large-scale evidence collection with a multi-agent artificial intelligence system that retrieves, verifies, deduplicates, synthesizes, and scores documentary evidence, producing detailed country reports supported by hundreds of primary sources. This represents a significant methodological contribution to the emerging field of digital sovereignty measurement, demonstrating the potential of AI-assisted social science research to scale evidence collection while maintaining traceability, transparency and human review.

The nearly simultaneous publication of the Tricontinental Index and the Digital Sovereignty Index (DSI) presented in this study is itself noteworthy. Developed independently and from distinct institutional contexts, both frameworks converge on and reinforce the proposition that digital sovereignty is a multidimensional phenomenon that requires systematic empirical measurement. Although the two indices employ different theoretical vocabularies, they independently organize digital sovereignty into four broad analytical domains, suggesting an emerging consensus regarding the principal dimensions through which State’s digital sovereignty may be understood and assessed. This convergence strengthens, rather than diminishes, the contribution of each framework by providing independent validation that digital sovereignty has matured into a concept amenable to rigorous comparative operationalization.

At the same time, important conceptual distinctions remain. The DSI separates digital sovereignty into the interrelated dimensions of Hardware, Software, Cognition, and Governance, emphasizing the relationship between technological infrastructures, productive capabilities, knowledge systems, and institutional capacity as per Rocha-Dashicheva's (2026) and Vaz's (2016, 2026) work. The Tricontinental framework, by contrast, is structured around Data Ownership, Digital Infrastructure, Cyberspace Governance, and Digital Capability, placing comparatively greater emphasis on the governance of digital resources, data control, and AI-assisted evidence synthesis. Although these dimensions capture many of the same empirical phenomena addressed by the DSI, their analytical boundaries are less clearly delimited. Several indicators simultaneously reflect infrastructure, governance, capability, and data ownership, making it difficult to determine whether a particular piece of evidence belongs to one dimension or several. This conceptual overlap complicates both replication and the substantive interpretation of scores, since changes observed within one category may partly reflect phenomena that are also captured elsewhere in the framework.

A second methodological distinction concerns the role assigned to technological development levels. The Tricontinental framework incorporates categories that, in the DSI, are understood as the common scaling mechanism applied to every subdimension. Rather than treating stages of technological development as analytical dimensions in themselves, the DSI evaluates every Hardware, Software, Cognition, and Governance subdimension according to the same standardized progression from Use, Acquisition, Specification, Production, to Value Chain. This separation between analytical categories (what is being measured) and scaling criteria (the degree of technological control exercised within each category) provides greater conceptual clarity and substantially improves comparability across heterogeneous technological domains.

While the Tricontinental BRICS Digital Sovereignty Index demonstrates exceptional depth in country-level documentation, the DSI presented here offers distinct methodological advantages as a comparative research instrument. Our DSI's analytically delimited subdimensions reduce conceptual overlap during coding while still recognizing, through the principle of fungibility, that developments in one dimension may causally influence outcomes in another. Hardware may strengthen Governance; Governance may stimulate industrial development; Cognition may enhance Software capabilities. These interactions are treated as empirical relationships emerging from the analysis rather than as overlapping analytical categories. This distinction preserves coding consistency without sacrificing the multidimensional character of digital sovereignty itself.

This DSI also prioritizes a transparent and reproducible framework that can be consistently applied across a much broader set of countries. Its expert-coded methodology, publicly archived and versioned evidence repository, explicit scoring criteria, and theoretically coherent distinction between Hardware, Software, Cognition, and Governance provide a high degree of comparability and replicability suitable for longitudinal and cross-national research. Nevertheless, the two indices might be viewed as complementary rather than competing approaches. The Tricontinental Index excels in the depth of its 11 country-specific documentation, whereas the DSI's principal strengths lie in its broader comparative scope, expert-coded methodology, transparent evidence architecture, and theoretically grounded framework for comparative analysis.

2.5 The practical ontology of Digital Sovereignty for policy-making

Previously, we have made explicit the common recognition of diverse authors that technological power is now exercised through infrastructures, software, institutions, and knowledge systems. Empire (Hardt and Negri, 2001), platform capitalism (Srnicek, 2017), surveillance capitalism (Zuboff, 2019), data colonialism (Couldry and Mejias, 2019), techno-feudalism (Varoufakis, 2024), or critiques of digital capitalism (Morozov, 2022), they are all theoretical pointers towards a problem that warrants public policy solutions.

The convergence of these theoretical traditions around a common public policy problem provides the ontological foundation of the DSI. Digital sovereignty is understood neither as the mere possession of particular technologies nor as the domestic adoption of specific software solutions and instead refers to the capacity of states to exercise meaningful control over the technological systems upon which their political, economic, military, and social functions increasingly depend. From this perspective, the concentration of platforms described by Srnicek, the extraction and prediction of behaviour examined by Zuboff, the appropriation of data theorized by Couldry and Mejias, and the infrastructural forms of domination identified across the debates on Empire, techno-feudalism, and digital capitalism are different manifestations of the same underlying problem: control over the technological conditions through which state authority and social life are organized.

This ontological understanding also clarifies the principal distinction between the DSI proposed here and the existing measurement frameworks reviewed previously. Each of the existing approaches captures an important aspect of digital sovereignty, yet each operationalizes only a subset of the broader phenomenon identified by the literature. The Nextcloud DSI reduces sovereignty to the domestic diffusion of a particular class of software; EDRIX privileges observable digital outcomes associated with resilience and software adoption; Di Marco et al. (2025) successfully organize the concept into a multidimensional policy framework but deliberately stop short of proposing an operational methodology; and the Tricontinental BRICS Digital Sovereignty Index offers a sophisticated comparative architecture supported by extensive documentary evidence, while adopting analytical categories whose boundaries remain partially overlapping and whose developmental levels are incorporated into the analytical framework itself. These approaches therefore differ less in their recognition of the problem than in the way they translate it into measurable empirical categories.

The DSI is constructed from the opposite direction. Rather than beginning with available indicators or desirable policy outcomes, it begins with the latent construct itself: **the state's capacity to exercise technological control - and the measurement architecture is therefore derived from theory rather than from data availability.**. This construct is then decomposed into four analytically distinguished dimensions: Hardware, Software, Cognition, and Governance; which together exhaust the principal domains through which technological sovereignty is accumulated and exercised. This architecture maximizes transparency, reproducibility, and inter-coder consistency while preserving the multidimensional nature of the phenomenon under investigation.

A second distinguishing feature concerns the relationship between measurement and explanation. Existing frameworks frequently embed causal relationships directly within their analytical categories by combining productive capabilities, governance, technological outcomes, or developmental stages into overlapping dimensions. The DSI deliberately separates these two levels of analysis. Its dimensions constitute the object of measurement, whereas the principle of fungibility explains how developments in one dimension may influence another. Industrial capabilities may reinforce governance; governance may stimulate software development; cognitive capacity may enhance productive capabilities. These relationships are treated as empirical hypotheses to be observed through comparative analysis rather than as assumptions incorporated into the measurement architecture itself.

The same logic applies to technological development. Rather than treating stages of development as analytical dimensions, the DSI employs a common scaling mechanism applicable across every subdimension. The progression from Use to Acquisition, Specification, Production, and Value Chain measures the degree of technological control exercised by the state regardless of whether the object under evaluation concerns semiconductors, cloud computing, artificial intelligence, regulation, or scientific production. This distinction between what is measured and the degree to which it is controlled provides a common metric capable of comparing heterogeneous technological domains without sacrificing conceptual precision.

Consequently, the DSI seeks to bridge the gap between theory and public policy. The literature demonstrates why technological sovereignty matters; the existing indices demonstrate that it can be measured. The contribution of the DSI is therefore not simply the introduction of another digital sovereignty index, but the proposal of a coherent measurement architecture that aligns ontology, operationalization, coding, and comparative analysis. Existing approaches demonstrate that digital sovereignty can be measured but our DSI argues that how it is measured is equally consequential. By separating analytical domains from developmental stages and treating fungibility as an empirical relationship rather than an analytical category, the framework seeks to maximize construct validity, transparency, reproducibility, and policy relevance simultaneously.

3 METHOD

The method remains the same as version 1.0 of the DSI (Rocha-Dashicheva et al., 2026a), with the complete database now with 101 countries available at Harvard Dataverse (Rocha-Dashicheva et al., 2026b). Our approach is based on Rocha-Dashicheva's (2026) three levels of Technological Dominance, operationalized through (1) hardware, (2) software and (3) cognition with the addition of a fourth additional (4) governance level; and Vaz (2026) technological's autonomy verticality dimensions, operationalized through four levels of domain: (1) use, (2) acquisition, (3) specification, and (4) production as well as an additional fifth (5) value-chain domain. Our Digital Sovereignty Index (DSI) is therefore constructed as a multilevel measure that captures the degree to which they govern the material, infrastructural, cognitive and regulatory conditions under which technologies operate.

Underlying this framework is Rael's (2022) conception of the fungibility of power: the idea that power accumulated in one domain may be converted into leverage in another. Economic concentration may become regulatory authority; technological infrastructures may generate geopolitical influence; cognitive legitimacy may reinforce institutional dominance. Within the DSI, this means that hardware, software, cognition, and governance cannot be treated as fully isolated dimensions, but as interconnected layers through which power circulates, stabilizes, and reproduces itself across the technological system.

In this methodological section, we first present the analytical structure of the DSI (3.1), defining its four dimensions and introducing the distinction between Infrastructure Capacity and Actuation Capacity. We then describe the (3.2) standardized scaling framework, the (3.3) operationalization and aggregation procedures used to construct the index, the (3.4) role of artificial intelligence in evidence collection and preliminary coding under human supervision, and finally the (3.5) Data Accessibility Level

(DAL), which evaluates the transparency and verifiability of the evidentiary base supporting each country assessment.

3.1 Analytical Structure

The four dimensions do not emerge arbitrarily. Rather, they synthesize the principal layers through which contemporary literature understands technological power. Hardware captures material infrastructures and industrial production; Software reflects the digital architectures mediating their operation; Cognition concerns the production of strategic knowledge and technological paradigms; Governance encompasses the institutional capacity to regulate and direct technological development. Together, these dimensions operationalize the stacked architecture of technological dominance (Rocha-Dashicheva, 2026), while incorporating governance as an autonomous layer through which sovereignty is ultimately exercised.

1. **Hardware**: material infrastructures and industrial capacities (networks, data centers, satellites, defense and critical infra hardware, energy inputs).
2. **Software**: operating systems, cloud and middleware, critical applications, standards and protocols that mediate how hardware is used and interconnected.
3. **Cognition**: doctrines, expert communities, training pipelines, strategic imaginaries and epistemic infrastructures that shape how digital and defense technologies are understood and governed.
4. **Governance**: institutional, legal, and political architectures through which a state steers, constrains, **and arbitrates the other four levels**. It encompasses the laws, regulations, procurement rules, treaties, oversight mechanisms, budgetary decisions, and bureaucratic structures that decide who controls infrastructures and code, under which standards, with what accountability, and in whose strategic interest.

A distinction is useful when interpreting these four levels of Technological Dominance: Hardware and Software primarily capture a state's **Infrastructural Capacity**: the material and technical assets that constitute its digital base, from physical infrastructures to computational platforms and applications. Cognition and Governance, by contrast, capture its **Actuation Capacity**: the ability to mobilize, direct, coordinate, and strategically employ those infrastructures through knowledge production, institutional authority, and political decision-making.

A country may therefore possess substantial infrastructural capacity while lacking the cognitive or governance capabilities required to deploy it autonomously, just as a state with comparatively modest infrastructures may exercise considerable influence through regulatory authority or epistemic leadership - the latter, in fact, more common across countries, revealing that nations are *aware* of the importance of Digital Sovereignty, but lacking the industrial capacities. Therefore, Digital Sovereignty emerges as the interaction between the Infrastructural Capacity and Actuation Capacity, with the capacity of a country of transforming material capabilities into effective strategic power.

This distinction closely relates to the concept of the fungibility of power (Rael, 2022), where Hardware and Software constitute strategic resources and Cognition and Governance determine the extent to which those resources can be converted into political, economic, military, or normative influence. Infrastructures without actuation capacity remain underutilized or externally conditioned; actuation capacity without an adequate infrastructural base faces structural limits to its projection. Sovereignty is therefore achieved through the continuous conversion of capabilities across these domains, where material assets reinforce institutional authority and epistemic influence, while governance and cognition, in turn, maximize the strategic value extracted from technological infrastructures.

3.1.1 Infrastructural Capacity

Considering first the **Infrastructural Capacity** (Hardware and Software) we straightforwardly apply the five levels of domain to each level of technological dominance, as per Vaz (2026):

1. **Domain of use**: the State is able to operate the technology autonomously in its daily routines, but has little control over its choice or broader supply conditions.
2. **Domain of acquisition**: the State controls all variables related to the acquisition of the technological artefact: it has access to information, domestic expertise to negotiate, and no binding legal or contractual restrictions imposed by external actors that limit future control over its use (for example, restrictive technology-transfer clauses in military contracts).
3. **Domain of specification**: the State is capable of specifying how the artefact must be designed and used: it defines technical, security and interoperability requirements that guide procurement or internal development, and suppliers must adapt to these parameters.
4. **Domain of production**: the State (directly or via nationally controlled entities) controls all variables necessary to develop and reproduce the artefact or capability, including industrial base, human capital and critical knowledge.
5. **Domain of value-chain**: also understood as the commercial Return on Investment (ROI). The State (directly or through nationally controlled firms and funds) is capable of developing a market-viable artefact (which is either better or at least somewhat competitive relative to all the other available artefacts in the niche, nationally or globally) and then to capture economic value generated over its life cycle, including profits from exports, licensing, services, and integration into **national and global value chains**, such that technological autonomy translates into sustained fiscal, industrial, and innovation gains rather than being confined to operational control alone.

The Industrial Capacity is the most straightforward. It concerns the productive foundations of digital sovereignty, capturing the State's ability to sustain, reproduce, and expand its industrial and technological capabilities - even beyond borders. By combining the Hardware and Software dimensions, it measures the extent to which a country possesses the industrial, technological, and organizational conditions necessary to progressively reduce external dependence across the successive levels of technological dominance; from use and acquisition to specification, production, and participation in value. In this sense, Infrastructural Capacity reflects primarily the industrial dimension of digital sovereignty, assessing the productive capabilities that enable a state to reproduce and strengthen its domestic technological base over time.

This understanding follows a long tradition in political economy that associates industrial production with strategic autonomy. Yet, in the digital economy, productive capacity extends beyond manufacturing alone to include cloud infrastructures, software ecosystems, and computational architectures that increasingly function as critical infrastructures of economic and political power (Srnicek, 2017; Durand, 2024).

3.1.2 Actuation Capacity

A few particularities emerge when applying the framework to measure Actuation Capacity (Governance and Cognition levels), as these dimensions concern the state's ability to strategically mobilize, coordinate, and direct technological capabilities rather than merely reproduce them.

For Governance, the question goes beyond a State’s ***disposal*** of formal legislation or regulatory agencies, and into whether its institutional and legal system can effectively discipline, constrain, shape and regulate the transnational technological infrastructures operating within its territory, or offered to its citizens’ consumption. In practical terms, we ask whether a country adopting cloud, platform, cybersecurity, or AI solutions architected under foreign jurisdictions can impose the primacy of its own national order: requiring data localization, restricting international data transfers, enforcing auditability standards, demanding access to source code or operational transparency, and ensuring that such obligations have legal effect despite the foreign jurisdiction where the provider is headquartered.

This challenge acquires particular asymmetry in relation to the United States, for example, where most large digital providers remain headquartered. On one hand, foreign States settle for the extraterritorial reach of mechanisms such as the US CLOUD Act, alongside the structural dependence created by US digital platforms and infrastructures. On the other, the United States itself presents a distinct configuration: despite fragmented federal regulation, its institutional architecture, enforcement capacity, and geopolitical centrality allow it to exercise broad agenda-setting authority over the global digital environment, often through the combined influence of state agencies, technical standards bodies, and major private corporations.

Within the Governance dimension, high scores therefore correspond to States capable of both enforcing domestic compliance across the digital production chain and projecting their regulatory model externally. This includes the ability to compel foreign corporations to structurally adapt products, contracts, and operational procedures to national requirements, as well as participation in international standard-setting and governance forums with sufficient authority to shape or influence, rather than merely import, the norms governing the global digital environment.

This distinction is particularly relevant because technological dependence may persist even where industrial capabilities are substantial. The USA itself presents a very interesting case as, regardless of its position as an unquestionable international digital superpower, they internally remain dependent on corporate power, having made little efforts to discipline the Big Tech as accountable to State regulation - thus compromising State Sovereignty to corporate interest. In this sense, States may manufacture advanced hardware or develop sophisticated software while continuing to rely upon foreign (in the case of the Global South), or corporate (in the special USA case) scientific paradigms, certification standards, policy models, and strategic doctrines. Such dependence influences procurement priorities, research agendas, security perceptions, and regulatory choices, reproducing external influence without requiring direct economic or political coercion.

Governance therefore concerns not merely the existence of legislation, but the effective capacity of the state to subordinate transnational digital infrastructures to domestic political authority. This distinction reflects the broader transformation identified by Hardt and Negri (2001), whereby sovereignty is increasingly exercised through standards, regulatory regimes, and infrastructural coordination rather than territorial command alone.

For Cognition, the logic of value capture differs from the material and regulatory domains because the strategic asset is knowledge itself. This domain addresses the State's capability of producing, retaining, and exporting the epistemic foundations that shape technological development both domestically and internationally. Cognitive sovereignty is ultimately expressed through the capacity to define how technologies are understood, evaluated, taught, and legitimized. And most important, if a country can produce its own cognition instead of adopting intellectual frameworks produced elsewhere.

Within the Cognition dimension, high scores therefore correspond to States capable of generating and sustaining autonomous epistemic ecosystems. This includes internationally competitive universities and research institutions, domestic production of scientific literature and technical standards, local professional training pipelines, influential think tanks and strategic communities, nationally developed technological doctrines, and the ability to shape global debates surrounding emerging technologies. Value capture occurs when this intellectual production becomes internationally adopted through education, scientific collaboration, technical assistance, consulting, standard-setting, or policy diffusion, allowing domestic knowledge to influence the technological trajectories of other States while simultaneously reinforcing the country's own innovation ecosystem and strategic autonomy.

Unlike production alone and the Industrial Capacity, cognitive value capture reflects the extent to which a State's ideas become reference points beyond its borders. Countries occupying the highest level are therefore producers of concepts, methodologies, technical norms, and strategic paradigms that other actors adopt, institutionalize, and reproduce. In this sense, cognition becomes a source of enduring geopolitical influence, as the export of ideas can shape technological development long after individual technologies themselves have evolved.

Therefore, for Actuation Capacity, the five levels of domain can be applied as:

1. **Domain of use**: the State is able to operate and administer technological systems through its existing institutions and human capital, but relies predominantly on externally developed legal frameworks, strategic doctrines, standards, or bodies of knowledge.
2. **Domain of acquisition**: the State controls the acquisition of institutional and cognitive capabilities: it can recruit, train, contract, and access the expertise, legal instruments, and organizational structures necessary to govern and strategically employ technology without being constrained by external actors.
3. **Domain of specification**: the State is capable of independently defining the legal, regulatory, technical, security, and strategic principles that guide technological development and deployment, requiring both domestic and foreign actors to adapt to its institutional and epistemic requirements.
4. **Domain of production**: the State autonomously develops and reproduces the institutional, legal, scientific, educational, and professional ecosystems necessary to sustain technological governance and strategic knowledge generation over time.
5. **Domain of value-chain**: the State is capable of transforming its governance models, regulatory frameworks, scientific production, strategic doctrines, educational systems, and institutional expertise into internationally adopted references, generating political, economic, and strategic returns through regulatory influence, policy diffusion, technical assistance, standard-setting, education, consulting, and participation in global governance networks. Such that institutional and epistemic autonomy translates into sustained geopolitical influence rather than remaining confined to domestic administrative capacity.

3.2 Qualitative scaling guidelines

For each layer × level we identify evidences that proxy the underlying power configuration, with three principles:

- **Layer coherence**: each evidence must be clearly anchored in hardware, software, cognition or governance, avoiding conceptual overlap as much as possible, even if we recognize the inherent fungibility of these levels.
- **Level discrimination**: evidences must allow us to distinguish use, acquisition, specification and production, rather than merely "more or less technology".
- **Sovereignty sensitivity**: evidences should reflect not only capacity, but who ultimately governs costs, lock-ins, standards and doctrines.

Operationally, evidences[1] are of two types. **Objective evidences** are based on administrative data, international statistics, budget and contract databases, legal texts and infrastructure maps (e.g., share of government workloads hosted on domestically controlled clouds). **Structured assessments** based on open-source information[2], in which direct measurement is impossible (e.g., degree of doctrinal dependence in cyber or defense strategy). In these cases, we rely on systematic analysis of publicly available materials such as media coverage, official communications, and other online content, using standardized coding rules to reduce subjectivity.

Evidences within each sub-dimensions (see Table 2) are normalized to a 0-4 scale corresponding to the levels of domain, where:

Table 1 - levels of domain scale

0	no effective domain (below use) or severe dependency
1	domain of use
2	domain of acquisition or specification, depending on the evidence
3	domain of production
4	domain of value-chain

Source: Authors.

For each country we define a small set of sub-dimensions inside each level. For each subdimensions:

[1] The complete evidences and rationale documentation database is available at https://dataverse.harvard.edu/dataverse/digital-sovereignty-index.

[2] Collection of laws, national strategies, procurement data, infrastructure statistics, academic and policy output, international datasets (ITU, UN, OECD, etc.) as well as publications.

Table 2 - Sub-dimensions of the Technological Dominance Levels

Hardware	H1	Connectivity and routing infrastructure
	H2	Data centers and cloud hardware
	H3	Critical components and manufacturing
	H4	Strategic space and satellite assets
Software	S1	State operating environments and productivity
	S2	Sovereign cloud and virtualization stack
	S3	Critical public-sector systems (taxation, social protection, elections, defense C2)
	S4	Interoperability and data standards
Cognition	C1	Formal strategies (cyber, AI, data, defense) and their authorship
	C2	Education and training ecosystems for digital/defense governance
	C3	Epistemic communities and think-tank production
	C4	Narrative autonomy in official discourse on technology and sovereignty
Governance	G1	Legal framework for data protection, cybersecurity, digital platforms and public procurement with explicit sovereignty clauses
	G2	Institutional architecture (existence, mandate and resources of digital-sovereignty, cybersecurity or data agencies; coordination between defense, foreign affairs and digital policy)
	G3	Regulatory capacity *vis-à-vis* of large national or foreign providers (track record of enforcement, ability to impose local-data, access to source code, or continuity obligations)
	G4	Participation and agenda-setting power in international standard-setting and Internet governance bodies.

Source: Authors.

We again map each evidence into 0-4 using the domain levels.

3.3 Operationalization and score aggregation into the DSI

Let us use the USA's chart, as a state-of-the-art country, as an example to describe the methodological pipeline. The scaling chart through the subdimensions, as per the analytical structure (3.1) and (3.2) scaling guidelines looks like this:

Table 3 - Measured sub-dimensions of the Technological Dominance Levels of the USA

UNITED STATES OF AMERICA			
LEVEL		**SCALE**	**RATIONALE**
Hardware	**H1**	4	The National Spectrum Strategy Implementation Plan identifies US leadership in wireless technologies. This commitment to fifth-generation networks, rural broadband, and fiber infrastructure places the US at a level of dominance in production and value capture.
	H2	4	The US is home to the world's leading cloud providers. GAO reports note that the cloud offers rapid

			access to shared resources and enables federal agencies to deliver services "*more quickly and at a lower cost*". The FedRAMP program and the OMB's Zero Trust guidelines demonstrate the capacity to specify, procure, and operate both on-premises and commercial infrastructures.
	H3	3	The Department of Commerce funded 40 chip manufacturing projects, planning to raise the share of advanced chip manufacturing from 0% in 2022 to 20% by 2030. However most PCMDPs (processed critical minerals and their derivative products) are not within US territory. The White House recognizes this as a strategic vulnerability, noting the US' continued dependence on foreign processing chains as a constraint on full technological autonomy.
	H4	4	The Space Force Commercial Strategy emphasizes that the force will integrate commercial and allied solutions into hybrid architectures to "increase resilience" and maintain an edge over competitors. These policies, combined with GPS networks and reusable launch programs, demonstrate full dominance of space production and commercial exploitation.
Software	**S1**	4	Memorandum M-22-09 stipulates a federal transition to a "*zero trust*" architecture and requires multi-factor authentication and encryption for all traffic. Such guidance shows that the government specifies and operates technological environments autonomously and in line with modern security practices.
	S2	4	The US sets requirements for public and private cloud through programs such as FedRAMP. The Zero Trust guidelines include strict criteria for cloud services as providers must adapt to federal parameters, indicating dominance in specification and production.
	S3	4	US tax, electoral, and defense systems are developed in-house and supported by domestic vendors. The GAO report on IRS modernization and the criteria in the FedRAMP Authorization Guide show that the state controls the design and operation of critical systems, ensuring redundancy and continuity.
	S4	4	NIST CSF 2.0 provides "*informative references*" that map requirements across different standards and help organizations achieve outcomes. This presence of NIST as a global standard-setter ensures that the US specifies and promotes interoperable standards, demonstrating full autonomy.
Cognition	**C1**	4	The state regularly publishes cybersecurity, AI, and defense strategies. The State Department's International Cyberspace Strategy emphasizes that a digital technology policy is "*foundational to US strategic, security, economic, and foreign policy interests*".
	C2	2	The initial implementation report of the National Cyber Workforce and Education Strategy acknowledges that demand for cybersecurity professionals exceeds the current training capacity and that it is necessary to expand the workforce. Although the government coordinates initiatives and collaborates with the private sector to reduce barriers, the talent shortage limits full autonomy.
	C3	4	Institutions such as Brookings and CEPS publish in-depth analyses on digital sovereignty and AI. The report "Is AI Sovereignty Possible?" defines AI sovereignty as a country's ability to make independent decisions about infrastructure, data, and models, setting out strategies and drivers for autonomy. The abundance of academic reports and debates illustrates a vibrant knowledge-production ecosystem.
	C4	3	Official US discourse emphasizes "digital solidarity" and a free, open, and secure order. However, the narrative privileges global leadership and alignment with partners rather than an explicit technological sovereignty agenda. There is partial autonomy, but the messaging highlights interdependence and shared norms.
Governance	**G1**	2	OMB memorandum M-24-04 provides FISMA guidance for 2024, requiring agencies to modernize systems, implement zero trust, and provide performance data in machine-readable format. Despite these directives and sectoral laws (for example, HIPAA, CCPA), the US still lacks a comprehensive federal data protection law, which limits full autonomy.
	G2	4	The institutional ecosystem includes the Office of Management and Budget (OMB), the National Cybersecurity Council, CISA, NIST, the FCC, the NTIA, the FTC, and the USSF. The State Department's Cyberspace Strategy stresses that the State Department will lead interagency coordination for digital diplomacy, while FISMA and EO 14028 set out clear roles for civilian and security agencies. This complexity indicates full coordination capacity.
	G3	2	The FTC's annual report highlights that the agency enforces antitrust laws to promote fair competition and protect consumers. The FTC and the Department of Justice have brought lawsuits

		against technology companies, but these efforts face prolonged litigation and legislative pushback. The capacity exists, but value capture and the imposition of data requirements (for example, localization, access to source code) remain limited.
G4	4	The State Department's Cyberspace Strategy states that the US will actively participate in international and multistakeholder bodies "*where obligations, norms, standards, and principles that affect cyberspace and technology are developed*". The commitment to leadership in forums such as the ITU, ISO, and AI forums, together with NIST's role in setting standards, demonstrates clear dominance.

Source: Authors.

For each level, we first compute a simple arithmetic mean of the four sub-dimensions (H1-H4, S1-S4, C1-C4, G1-G4), which yields a level score on the original 0-4 domain scale. Formally, for level $L \in H,\ S,\ C,\ G$, we have:

$$L_{0-4} = \frac{1}{4}\Sigma_{i=1}^{4} L_i$$

where L_i is the score of sub-dimension i in level L (for example, $H_1 - H_4$ for Hardware). We then linearly rescale each level score to a 0-100 range (normalization) using:

$$L_{0-100} = \frac{L_{0-4}}{4} \times 100$$

to create a range where 0 represents complete dependency (below use) and 100 full domain of production and value-chain in the layer. The DSI (Digital Sovereignty Index) for each country is, finally, obtained as the simple average of the four normalized level scores:

$$DGI_{0-100} = \frac{H_{0-100} + S_{0-100} + C_{0-100} + G_{0-100}}{4}$$

The aggregate table for the US and its scores will be:

Table 4 - Aggregate domain scales of USA

	Hardware	Software	Cognition	Governance
Level mean	3,75	4	3.25	3
Normalized level mean	93,75	100	81.25	75
Normalized DSI score				**87,5**

Source: Authors.

Finally, and should two or more countries obtain the same final DSI score, rankings are determined through a hierarchical tie-breaking procedure designed to preserve the analytical priorities of the framework. Countries are first compared according to their (3.5) Data Accessibility Level (DAL), reflecting the transparency, completeness, and verifiability of the underlying evidence. If the tie persists, comparison proceeds sequentially through the normalized scores of Hardware (H), Software (S), Governance (G), and Cognition (C). The complete order is therefore: DSI score → DAL level → Hardware → Software → Governance → Cognition. This procedure ensures that countries with identical aggregate scores are ranked consistently while preserving the methodological integrity and reproducibility of the index.

3.4 AI use

To scale this research, we have employed AI in the process of evidence collection and initial scaling, abiding by the human-centric approach as outlined by David Resnik and Mohammad Hosseini (2024) and the University of the State of Santa Catarina (UDESC)'s (Silva and Dornelles, 2025). With varied research agents[3], we used the following prompt with an attachment of this article's research design (section 2 all the way to 2.3):

> You are assisting with a comparative research project using a provided research design.
>
> Step 1 – Understand the research design
> Carefully read the attached .txt file containing the research design and methodology.
> Extract and list all:
> Dimensions
> Subdimensions (subdomains)
> The 0–4 scoring scale and the criteria associated with each score.
> Confirm that you have understood the structure and the scoring scale before proceeding.
>
> Step 2 – Collect evidence for [COUNTRY] by subdimension
> For each subdimension in the research design, identify and list at least four high-quality, citable sources that provide evidence for the [COUNTRY] case.
> Prefer official and credible materials (e.g., government reports, reputable think tanks, academic articles, international organizations, major news outlets with analytic reports).
> For each source, provide:
> Author(s) or institution
> Year of publication
> Full title
> Type of source (e.g., government report, academic paper, policy brief, news analysis)
> Short note (1–2 sentences) explaining what aspect of the subdimension it supports.
> Only include sources that:
> Are accessible online (public or via stable repositories), and
> Are suitable to be downloaded/printed and independently verified.
>
> Step 3 – Create an Excel-ready evidence list
> Create a table that can be exported to Excel with the following columns:
> Country | Subdimension | Year | Author | Title | Filename | evidence_url
> Populate one row per source. Use the following rules:
> Country: use [COUNTRY].
> Subdimension: use the exact subdimension name from the research design.
> Year: year of publication (numeric).
> Author: main author(s) or institution (in SMALL CAPS for institutions if possible).
> Title: full title of the document/report/article.
> Filename: create a suggested filename in the following format:
> COUNTRY. [SUBDIMENSION CODE]. YEAR. AUTHOR, Name/SOURCE

[3] AI models used included: GPT-5.4, Gemini 3.1 and 2.5 series, Deepseek-V4 series, Claude Opus 4.6 and 4.7.

Examples:
SOUTH AFRICA. G2. 2025. SITA. Annual Report
INDIA. H3. 2025. NANDI, Anukekha. India's Semiconductor Ambitions and Global Competitiveness
Use the appropriate subdimension code from the research design and adapt the author/source and title accordingly.
evidence_url: direct URL where the document can be accessed or downloaded.
Present this table in a clean, copy-and-paste-friendly format (e.g., markdown table or CSV-style text).

Step 4 – Score each subdimension (0–4) and justify the scores
Using the methodology and scale described in the attached research design:
Assign a score from 0 to 4 to each subdimension for [COUNTRY].
For each subdimension, provide:
The chosen Score (0–4).
A concise Rationale (3–6 sentences) that explicitly links the score to:
The criteria in the methodology, and
Specific evidence from the collected sources.
At least one Reference (from Step 2/3) that supports the rationale.
Present your scoring in a separate table with the following columns:
LEVEL | Subdimension | Score | Rationale | Reference
Where:
LEVEL: main dimension or theme (as defined in the research design) that the subdimension belongs to.
Subdimension: exact name from the research design.
Score: integer from 0 to 4 according to the methodology.
Rationale: short textual justification citing key facts and pointing to source(s).
Reference: in-text citation(s) or brief reference to the source(s) used (e.g., World Bank 2023; Ministry of Finance 2022).
If any subdimension lacks sufficient evidence to score confidently, explicitly state this in the rationale and assign the most appropriate score based on the available information, noting the uncertainty.

The researchers then parse through each AI-generated output individually, reviewing every subdimension classification against the sourced evidence. This is because we are expected to interrogate the rationale provided by the AI, verify that the cited documents substantiate the attributed score, and correct any misclassification that results from the machine's known limitations, including the conflation of nominal capability with effective control, the misreading of policy announcements as implemented realities, or the attribution of scores based on sources that are geographically or temporally misaligned with the country case under examination - as well as biases built into model training.

Therefore, **AI usage in this research has the primary function of organizing and pre-processing an otherwise unmanageable volume of documents, often in various languages**, surfacing relevant materials, and structuring preliminary interpretations so that researchers may move through large bodies of evidence with greater speed and coherence. The burden of interpretation remains human while the machine serves as an instrument of scale.

Finally, the research coordinators conduct a cross-country review of all finalized rankings, examining the complete matrix of domains and subdomains and their attributed values simultaneously across all country cases. This final layer of oversight is designed to ensure internal consistency and comparative validity. Then, we re-evaluate borderline cases, flag systematic scoring drift across a research team, and adjust values where the cross-national comparison reveals implicit inconsistencies that individual case reviews could not detect. Only after this coordinators' review are the rankings considered finalized and suitable for the analytical and interpretive stages that follow.

3.5 Data Accessibility

In the previous subsection, we have outlined the use of AI for gathering evidences. What follows now is to sift through what has been collected and judge how firmly it stands. Each document, each report, each fragment of law or statistic must be weighed for its accessibility, its origin, and the degree to which it allows independent verification. Our concern here is less with what is claimed, and more with how that claim may be reached, traced, and confirmed across sources. In this sense, accessibility becomes a proxy for epistemic solidity: the clearer the path to the data, the stronger the ground upon which the classification rests.

Thus, for every subdimension outlined in the analytical structure, the collected evidences are systematically assessed by the research coordinators and assigned to one of four Data Accessibility levels: A, B, C, or D. These levels assess the conditions under which such capacity may be observed, reconstructed, and validated by the researcher, indicating also where further research is needed as we move beyond version 1.0 of our DSI.

Table 4 - Data Accessibility Level (DAL)

Level	Meaning	Rationale
A	Excellent Accessibility	Data is directly available from primary sources, including official national institutions (ministries, regulatory agencies, statistical bodies) and well-established international organizations (e.g., OECD, UN, WIPO). Documentation is consistent, up-to-date, and sufficiently detailed across domains. Cross-verification is straightforward, requiring limited reliance on interpretive or secondary material
B	Moderate Accessibility	Data is available through a combination of official sources and recognized international datasets, though coverage may be uneven across some dimensions. Gaps are present but manageable. Research remains feasible with moderate triangulation, occasionally requiring supplementation from analytical reports or secondary literature.
C	Limited Accessibility	Data availability is constrained, outdated or inconsistent. Official sources are partial, outdated, or difficult to access, and coverage across domains is uneven. Research may depend significantly on secondary materials such as think tank reports, policy briefs, and international financial or technical organizations. Triangulation requires careful validation due to variability in quality and scope.
D	Minimal Accessibility	There is little to no reliable primary data available from national institutions. Coverage in international datasets is sparse, outdated or absent. Research may rely almost entirely on external and indirect sources, often fragmented or inferential in nature, with limited capacity for robust verification.

Source: Authors.

This assessment allows us to move forward with greater precision by treating the DSI as a living instrument that sharpens as the evidentiary base deepens. Classifying Data Accessibility allows us to assess where the DSI stands on firmer ground and where it still rests on inference. As stronger evidences emerge, whether through newly released administrative data, updated institutional reports, or expanded international coverage, subdimensions may be revisited, reclassified, and, where necessary, rescored.

In this way, the DSI is not conceived as a closed measurement, but as an iterative process of refinement. This pilot version captures the observable contours of technological dominance under existing informational constraints while subsequent iterations incorporate more robust, direct, and granular sources, gradually reducing reliance on secondary interpretation. This process also entails an active effort to access materials that do not readily circulate in open repositories. Where gaps persist, research teams may formally request internal or restricted documents from public institutions, regulatory agencies, or relevant stakeholders, particularly in cases where national practices are known to exist but remain under-documented. Such requests form part of its extension, pushing the boundary between observable and obscured domains of governance and capacity.

In this version (1.1), we indeed comprehended the difficulty of accessing reliable and comparable data across national contexts. In many cases, the problem did not lie solely in the absence of information, but in its fragmentation across institutions, the opacity of administrative procedures, or the disjunction between official discourse and operational reality. Countries frequently announce strategies, partnerships, or regulatory ambitions that suggest high levels of technological autonomy, while the material conditions required to sustain such autonomy remain partially obscured, inconsistently documented, or altogether unverifiable. This asymmetry between declared capacity and observable capacity became one of the central methodological challenges of the project.

The difficulty intensified when attempting to compare states operating under radically different informational cultures. Highly digitized countries may produce abundant documentation while revealing little about strategic dependencies hidden within supply chains, proprietary infrastructures, or foreign-controlled layers of computation. Conversely, states with limited statistical transparency may still possess meaningful sovereign capacities that remain poorly represented in international datasets. In this sense, informational abundance does not necessarily translate into epistemic clarity, just as informational scarcity does not automatically indicate technological weakness. The challenge, therefore, was not merely to collect data (though we cannot understate the difficulty of collecting specific national data), but to interpret the conditions under which data itself becomes visible, legible, and politically available.

As a result, Data Accessibility operates both as a diagnostic and as a guide by signaling where the current measurement is most reliable, and where further empirical work must be directed. The DSI, in turn, evolves with each version as each new layer of evidence tightens the correspondence between measured scores and the underlying structures they seek to represent.

4 DIGITAL SOVEREIGNTY INDEX

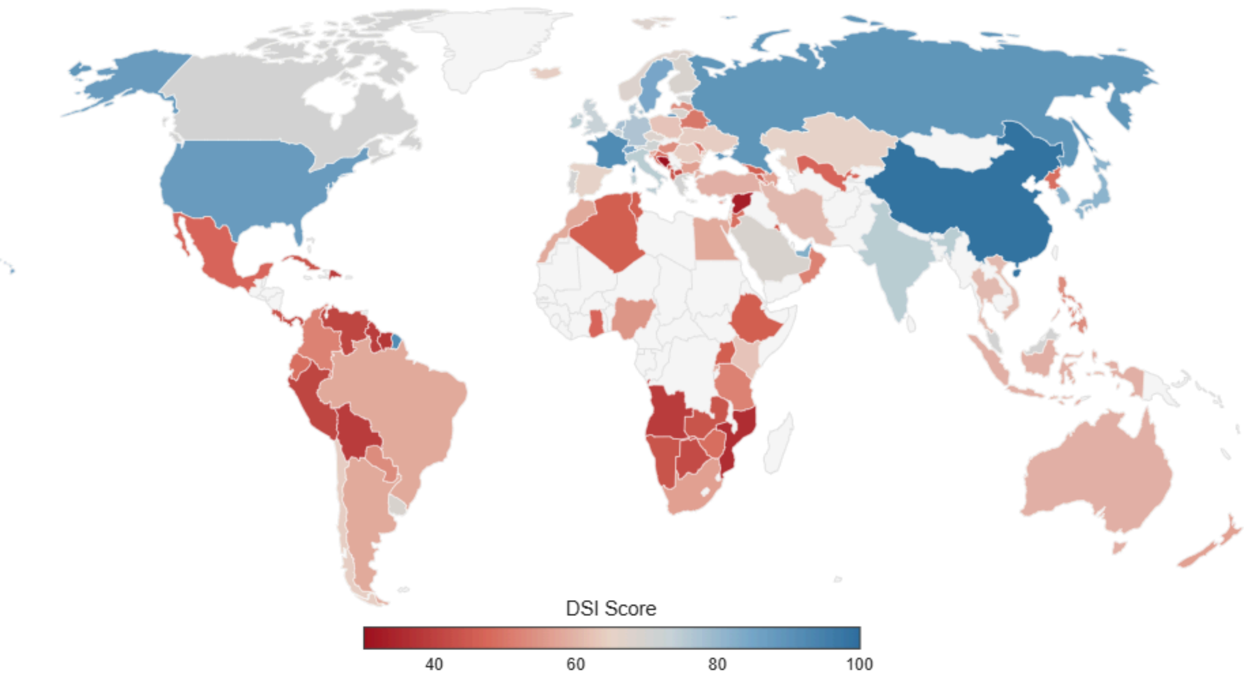
The official ranking with all 101 countries and 1616 expert-coded assessments, as well as its 1265 sourced evidences is available at Harvard Dataverse (Rocha-Dashicheva, et al., 2026) for full transparency, replication, and independent verification of the DSI methodology and results.

In this section, we present the empirical application of the index. We (4.1) examine the global distribution of digital sovereignty through the DSI heat map and discuss the geographical patterns that emerge from the overall index. We then (4.2) decompose the DSI into its two synthetic capacities (Infrastructure Capacity and Actuation Capacity) to investigate the different developmental trajectories through which states accumulate digital sovereignty, comparing the distinct patterns observed across the Global North and the Global South.

4.1 The DSI as a map

Though a North × South bipolar division between technologically sovereign and technologically dependent States was somewhat expected, the DSI heat map instead displays a gradient of technological capability. Countries occupy intermediate positions across the distribution, suggesting that digital sovereignty is accumulated progressively, supporting conceptualization of digital sovereignty as a multidimensional process.

Figure 1 - DSI heat map.



Source: Authors. Visualization available at BRICS Tech Forum DSI page[4].

Beyond revealing a global gradient of digital sovereignty, the heat map also demonstrates a strong degree of geographical clustering. High DSI scores remain concentrated in regions historically associated with industrialization, scientific accumulation, and technological leadership, particularly Europe, North America, and parts of East Asia. Conversely, lower scores predominate across much of Sub-Saharan Africa and Latin America, while intermediary levels are observed throughout the Middle East and emerging economies. This spatial coherence suggests that digital sovereignty remains closely associated with long-term patterns of economic development, industrial capacity, and institutional consolidation rather than isolated technological achievements.

Nevertheless, geographical distribution alone cannot explain how countries achieve similar levels of digital sovereignty. States with comparable DSI scores frequently combine very different configurations of industrial capabilities, software ecosystems, governance structures, and knowledge systems. Likewise, countries occupying similar geographical regions may rely upon distinct developmental trajectories to reach comparable outcomes. The aggregate DSI therefore conceals important differences in the composition of national capabilities.

To uncover these distinct pathways, the DSI is decomposed into its two synthetic capacities, as previously described. Infrastructure Capacity captures the productive foundations of digital sovereignty through the Hardware and Software dimensions, while Actuation Capacity measures the state's ability to strategically mobilize these productive capabilities through the Cognition and Governance dimensions. Examining both capacities simultaneously makes it possible to distinguish countries that achieve similar

[4] Available at: https://www.bricstechforum.org/dsi-ranking.

overall DSI scores through fundamentally different combinations of industrial and institutional development.

4.2 Industrial and Actuation Capacities

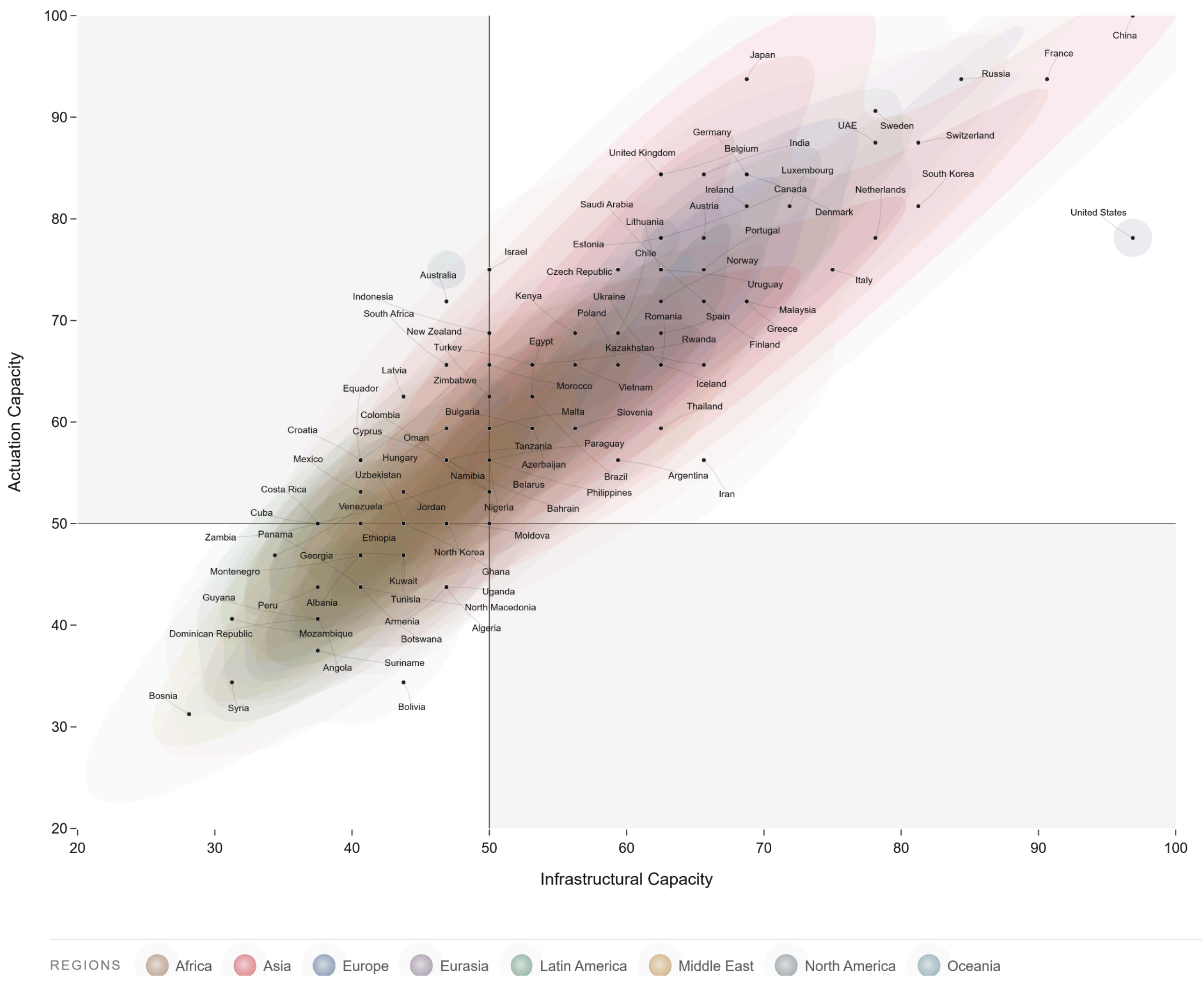
To visualize how developed countries are in terms of Digital Sovereignty, we organize them across two synthetic axes that capture distinct but interconnected dimensions of technological power. The horizontal (X) axis, **Infrastructural Capacity**, represents the average between the Hardware (H_{0-100}) and Software (S_{0-100}) levels, measuring the material and industrial foundations of technological autonomy. The vertical (Y) axis, **Actuation Capacity**, represents the average between Cognitive (C_{0-100}) and Governance (G_{0-100}), capturing the ability of states to regulate, coordinate and shape digital environments through governance architectures, informational influence, data regulation and institutional control. These axes position countries according to the balance between material technological capacity and the political-cognitive ability to govern technological systems, allowing the identification of differentiated trajectories of sovereignty within the emerging multipolar digital order.

The axes are operationalized through the following formulas:

$$X = \frac{H_{0-100} + S_{0-100}}{2} \text{ and } Y = \frac{C_{0-100} + G_{0-100}}{2}$$

The plotted countries are shown in the following chart:

Chart 1 - Infrastructural × Actuation Capacity



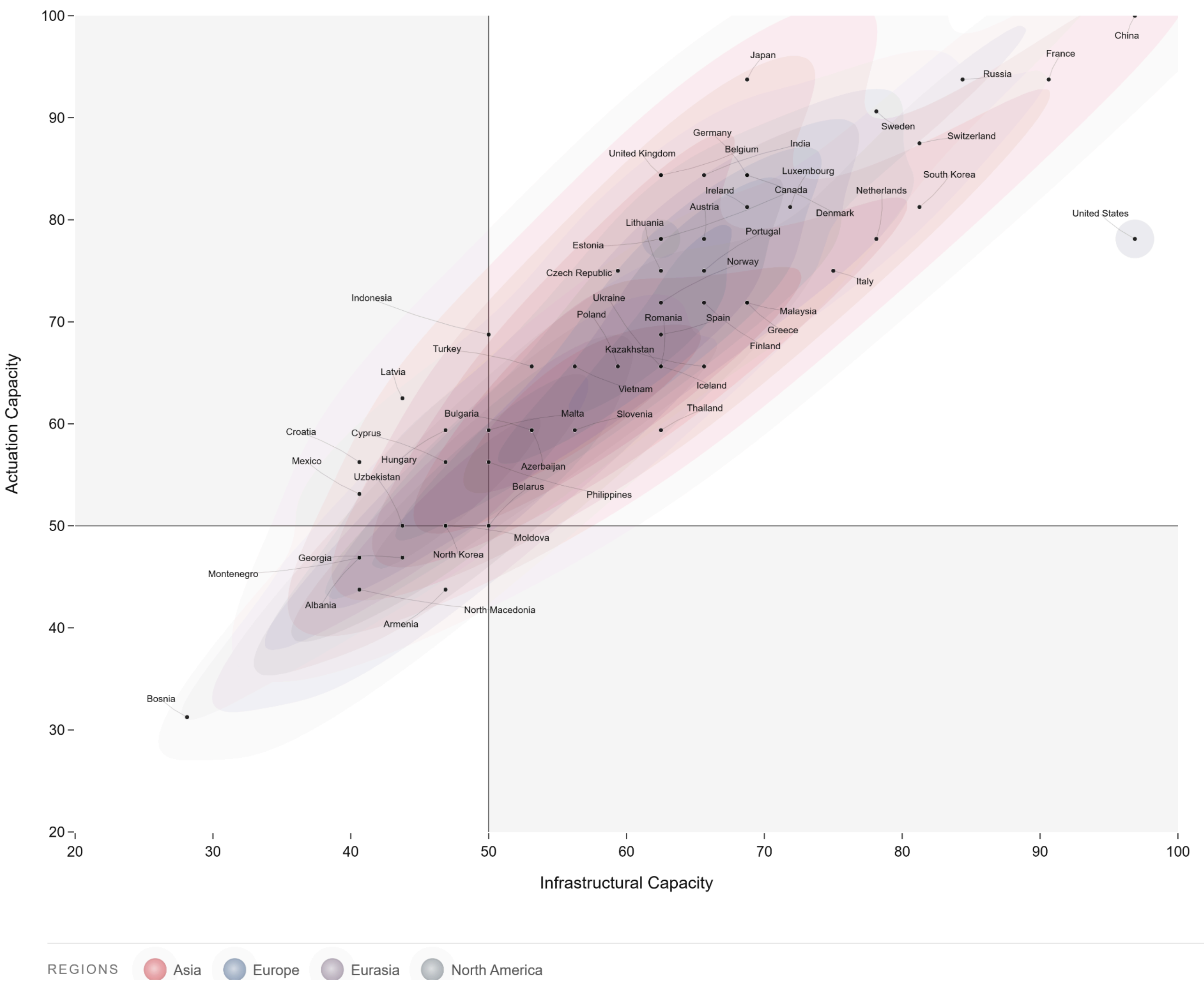
Source: Authors. Visualization available at BRICS Tech Forum DSI page[5].

4.2.1 The Global North. the top 5 and the three paradigms of Digital Sovereignty

The distribution of countries across the graph reveals that structural technological power remains heavily concentrated in the Global North, as seen before in **Figure 1**. For example, if we select only the regions of Asia, Europe and North America, the great majority of countries are located at the upper-right quadrant of the graph:

[5] Available at: https://www.bricstechforum.org/dsi-capacity.

Chart 2 - Infrastructural × Actuation Capacity - Asia, Europe, Eurasia and North America.



Source: Authors. Visualization available at BRICS Tech Forum DSI page[6].

This is where both infrastructural capacity and actuation capacity converge at high levels. Expectedly populated predominantly by states historically integrated into the industrial, scientific, and financial core of the international system, countries such as France (Infrastructural: 90.63; Actuation: 93.75), Switzerland (Infrastructural: 81.25; Actuation: 87.50), Sweden (Infrastructural: 78.13; Actuation: 90.63), Japan (Infrastructural: 68.75; Actuation: 93.75), Germany (Infrastructural: 68.75; Actuation: 84.38), South Korea (Infrastructural: 81.25; Actuation: 81.25), and the United States (Infrastructural: 96.88; Actuation: 78.13). combine advanced telecommunications infrastructure, domestic industrial ecosystems, high-end research capacity, institutional continuity, and regulatory sophistication. **Their position reflects the cumulative historical consolidation of scientific institutions, industrial capital, educational systems, military innovation, and bureaucratic coordination accumulated over decades, and in some cases centuries**. Technological sovereignty thus appears as an extension of long-term structural power.

[6] Available at: https://www.bricstechforum.org/dsi-capacity.

The top five countries are China (Infrastructure: 96.88; Actuation: 100.00), France (Infrastructure: 90.63; Actuation: 93.75), Russia (Infrastructure: 84.38; Actuation: 93.75), the United States (Infrastructure: 96.88; Actuation: 78.13), and Switzerland (Infrastructure: 81.25; Actuation: 87.50). See **Table 5**.

Despite their considerable differences in political systems, economic models, demographic scale, and geopolitical positioning, these countries converge in maintaining exceptionally high levels of both Infrastructure Capacity and Actuation Capacity. Their common characteristic is not adherence to a single model of development, but the successful integration of advanced technological infrastructures with strong institutional coordination, domestic knowledge ecosystems, strategic planning, and international influence. The ranking demonstrates that the highest levels of digital sovereignty are achieved not through excellence in any single dimension, but through the sustained integration of technological and institutional capabilities across the entire digital ecosystem. At the same time, the differences within this group are equally revealing.

The comparison among the five highest-ranked countries also reinforces one of the central propositions of the DSI: **the dimensions of digital sovereignty are highly fungible and mutually reinforcing**. Improvements in one dimension frequently generate positive spillover effects across the others, while weaknesses likewise constrain the broader digital ecosystem. Consequently, digital sovereignty should not be understood as the simple aggregation of independent capabilities, but as an integrated system in which infrastructure, production, knowledge, and governance continuously shape one another.

Although China and the United States share the highest Infrastructure Capacity in the index (96.88), their markedly different Actuation Capacity (100.00 and 78.13, respectively) produces substantially different overall levels of digital sovereignty. The comparison between China and the United States illustrates this dynamic. Although both countries achieve identical Infrastructure Capacity (96.88), the United States records a substantially lower Actuation Capacity (78.13), resulting in a lower overall DSI score. This reflects the broader effects of a US regulatory model that cannot so much directly regulate Big Tech as it allows the technology market to be uncoordinatedly shaped by private policies from the corporations themselves.From the perspective of the DSI, the relative State's reduced ability to direct or constrain key digital actors diminishes the extent to which exceptional infrastructural resources can be converted into sovereign national capabilities. Table 5 presents the top 5 country scores.

Table 5 - Top 5 country scores.

Country	H1	H2	H3	H4	S1	S2	S3	S4	C1	C2	C3	C4	G1	G2	G3	G4	DSI
	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	
China	93.75				100				100				100				**98.44**
	Infrastructural Capacity: 96.88								**Actuation Capacity: 100**								
	4	4	3	4	4	4	4	3	4	2	4	4	4	4	4	4	
France	87.50				93.75				87.50				100				**92.19**
	Infrastructural Capacity: 90.63								**Actuation Capacity: 93.75**								
	4	3	2	4	4	3	3	4	4	3	4	4	4	4	4	3	
Russia	81.25				87.50				93.75				93.75				**89.06**
	Infrastructural Capacity: 84.3								**Actuation Capacity: 93.75**								
	4	4	3	4	4	4	4	4	4	2	4	3	2	4	2	4	
USA	93.75				100				81.25				75				**87.50**
	Infrastructural Capacity: 96.88								**Actuation Capacity: 78.13**								
	4	3	3	3	2	3	4	4	4	4	4	4	3	3	2	4	
Switzerland	81.25				81.25				100				75				**84.38**
	Infrastructural Capacity: 81.25								**Actuation Capacity: 87.50**								

Source: Authors

France illustrates the opposite dynamic. Its exceptionally strong regulatory and institutional architecture, supported by the broader European Union framework, extends beyond the Governance dimension itself. Through instruments such as data protection, competition policy, digital market regulation, public procurement, and industrial policy, governance strengthens domestic software ecosystems, stimulates investment in strategic technologies, and reinforces national and European technological capabilities. In other words, regulatory sovereignty becomes a driver of infrastructural sovereignty, demonstrating the fungibility between the Governance and Infrastructure dimensions.

Russia provides a third pathway. Its model has increasingly been shaped by geopolitical resilience. International sanctions accelerated policies of technological substitution, domestic software development, payment systems, cloud infrastructure, and industrial coordination. Strategic necessity therefore generated spillover effects across Hardware, Software, Cognition, and Governance, illustrating once again that advances in one dimension propagate throughout the wider digital ecosystem.

France, Russia, and China, therefore, illustrate three distinct paradigms through which high levels of digital sovereignty may be achieved:

The Chinese paradigm is characterized by the close integration of state planning, domestic industrial policy, digital infrastructure, and platform governance, producing high levels of both infrastructural and actuation capacity. **The Russian paradigm reflects a strategy of resilience and strategic autonomy**, in which domestic technological capabilities, institutional coordination, and regulatory mechanisms have been progressively strengthened in response to geopolitical pressures and international sanctions. **The French paradigm, embedded within the broader European Union model, places comparatively greater emphasis on sovereignty through regulation**, using comprehensive legal frameworks, including data protection, competition policy, digital market regulation, and institutional coordination, to increase State influence over digital infrastructures and transnational technology providers.

These paradigms illustrate that technological sovereignty is contingent upon the institutional, economic, social, and geopolitical trajectories of states rather than being ideologically predetermined. Distinct political economies may converge upon similar sovereign outcomes provided they successfully integrate productive capacity with institutional actuation.

Within this environment, China and Russia emerge as the two most significant challenges to the historical concentration of technological dominance in the Atlantic world, though each follows a different trajectory. China represents the clearest example of a State that successfully transformed industrial scale into systemic technological power. Its position at the extreme upper-right corner in **Chart 2** reflects the convergence of infrastructure, governance, cognition, and industrial policy into a coordinated State project capable of competing directly with Western technological centrality. China no longer appears as a peripheral manufacturing hub integrated into foreign value chains, but as an actor capable of constructing parallel ecosystems in cloud computing, artificial intelligence, digital payments, telecommunications, and strategic infrastructure. As the leader of not only the BRICS+ Tech Forum DSI, but also the Tricontinental DSI (2026), future studies investigating the case of China alone are warranted.

Russia, meanwhile, occupies a more complex position. Its infrastructural base remains relatively more constrained than China's or the leading Western economies, yet its exceptionally high actuation capacity (matching that of France) demonstrates the strategic importance of governance, institutional coordination, and cognitive sovereignty even under western sanctions and geopolitical pressure. This is because Russia increasingly reorganized technological policy around resilience, continuity, and defensibility against external coercion. Either way, both countries therefore approach digital sovereignty as protection against asymmetrical dependence on foreign-controlled technological systems.

A comparison, however, becomes relevant as we note the positions of both France and Russia. France, the second position in the overall rank of the DSI, overcoming Russia by 6.25 points in Infrastructural Capacity. The suggestion here is that Governance may act as an industrial leverage through fungibility, influencing the accumulation of productive capabilities over time. This observation also raises the possibility of path-dependent dynamics, whereby previous institutional, economic, and geopolitical trajectories shape the extent to which gains in Governance are translated into industrial capacity. This remains a preliminary finding, however, and constitutes a promising agenda for future longitudinal and comparative research.

However, there is a strong argument that would note Russia's industrial power as greater than that of France. This argument is supported by the OECD, resting primarily on a broader, more traditional understanding of industrial power, emphasizing the scale and strategic depth of the productive base rather than the sophistication of particular digital technologies. The OECD's 2011 review of Russia describes an economy with extensive capabilities in extraction, metallurgy, energy, medium-low-technology manufacturing and other large-scale industrial activities. It reports particularly strong Russian specialization in medium-low-technology manufacturing, alongside rapid growth in total manufacturing exports between 1998 and 2008. This assessment remains broadly consistent with subsequent OECD research. In a 2019 firm-level analysis, the OECD finds that Russian industry continues to be characterized by large and relatively productive enterprises, particularly in manufacturing and extractive sectors.

France presents the inverse profile. It retains advanced and internationally competitive industries, but its industrial base has contracted substantially relative to the wider economy. The OECD's 2026 survey finds that French deindustrialization has been more pronounced than the OECD average: by the end of 2025, manufacturing represented only 11.2% of value added and 9.1% of salaried employment, approximately one-third below its share in the early 2000s. The report therefore treats the preservation and rebuilding of a broad industrial base as a central policy challenge for France. Yet, the DSI indicates otherwise:

Table 6 - France and Russia scores.

Indicator	France	Russia
Hardware (H)	93.75	87.50
Software (S)	87.50	81.25
Industrial Capacity	90.63	84.38
Cognition (C)	93.75	93.75
Governance (G)	93.75	93.75
Actuation Capacity	93.75	93.75
Digital Sovereignty Index (DSI)	**92.19**	**89.06**

Source: Authors.

Looking closely into the actual differences between the countries:

Table 7 - France and Russia score differences.

Indicator	Difference (France-Russia)	Difference (Russia-France)
Hardware (H)	+6.25	-6.25
Software (S)	+6.25	-6.25
Industrial Capacity	+6.25	-6.25
Cognition (C)	0	0
Governance (G)	0	0
Actuation Capacity	0	0
Digital Sovereignty Index (DSI)	**+3.13**	**-3.13**

Source: Authors.

This contrast in the French industrial leverage may in fact be explained by the particularities of the regulatory environment. First, the implementation of broad and pioneering legislation on the protection of personal data, competition practices, cybersecurity and regulation of the use of artificial intelligence not only brought guarantees of fundamental rights to the forefront, but also, above all, conditioned the activities of both domestic and foreign actors in the French digital market on compliance with the French legal order. This is a common characteristic of European Union Member States, which adopt the rules of the bloc.

Second, official French government reports published over the past three years consistently portray the country's digital public policy as combining two complementary objectives: attracting foreign investment into strategic digital sectors while simultaneously strengthening domestic technological capabilities through initiatives such as France 2030 and French Tech 2030. This strategy relies on government incentives to attract international enterprises and capital, alongside substantial public support for French startups, innovation ecosystems, and national technological champions, enabling them to scale and compete in international markets (Macron, 2024; DGE, 2025; RAISE, 2026; Institut Montaigne, 2025).

These characteristics may explain France's high score for Actuation Capacity. Beyond that, the economic and technological integration between France and foreign actors, enabled by the French regulatory environment, appears empirically to have fostered the concentration and development of the digital ecosystem measured by the DSI's Industrial Capacity. By reducing regulatory uncertainty, coordinating public and private investment, protecting strategic sectors, and creating stable institutional conditions for innovation and market expansion, high Actuation

Capacity strengthens the incentives for firms to invest, locate production, and scale technological activities domestically. Rather than functioning independently from industrial capabilities, governance and cognition therefore act as multipliers that reinforce the accumulation of hardware and software capacities, illustrating how institutional coordination can translate into measurable industrial development.

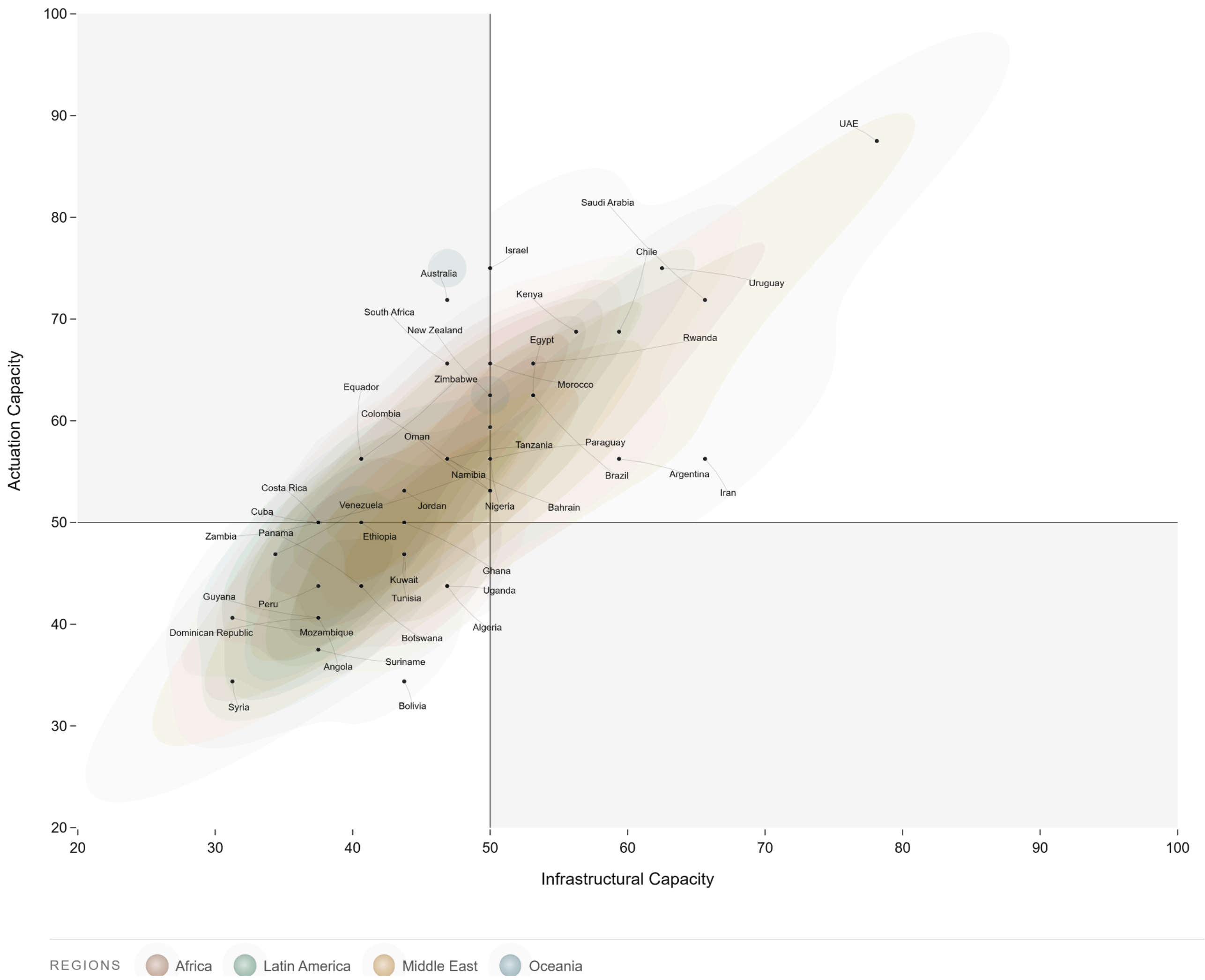
Although they demonstrated the same level of Actuation Capacity, the French scenario contrasts with the reality of Russia, which concentrated its efforts on developing its own technology industry despite Western economic isolation, centralizing solutions within its digital ecosystem throughout the consumer chain. This comparison suggests that Actuation Capacity may also operate externally, as states capable of projecting regulatory and economic power beyond their borders reshape the industrial trajectories of other countries. In the present case, the governance capacity exercised by Western states through sanctions, export controls, and financial restrictions appears to have constrained Russia's Industrial Capacity while simultaneously reinforcing France's by redirecting investment, technological cooperation, and access to international markets toward allied economies. This interpretation suggests that the benefits of high domestic Actuation Capacity may depend not only on national institutions but also on the country's position within broader geopolitical structures of regulatory influence and economic integration. Still, this is a preliminary finding for which a separate and in-depth case investigation is proposed.

Most importantly, the comparison between France and Russia illustrates fungibility among the dimensions examined by the DSI. Although each dimension is operationalized through distinct indicators and supported by evidence that is analytically delimited and non-overlapping, developments in one dimension influence outcomes observed in others. Advances in governance, for instance, may create the institutional conditions for industrial expansion, while industrial capabilities may, in turn, strengthen cognitive and regulatory capacities. This interdependence highlights the dynamic interactions through which digital sovereignty evolves over time, while also reinforcing the need for the DSI to be periodically updated, as changes in one domain may progressively reshape the empirical evidence and scores associated with the others.

4.2.2 The Global South

The distribution of countries across the graph reveals a markedly more heterogeneous pattern within the Global South. Selecting only the regions of Africa, Latin America, the Middle East, and Oceania, countries are dispersed across the central and lower portions of the graph. This distribution suggests that digital sovereignty in the Global South is characterized by fragmented modernization, where advances in Infrastructure Capacity and Actuation Capacity often occur unevenly. While some countries have strengthened institutional, regulatory, and strategic capabilities despite only moderate technological infrastructures, others have expanded their digital infrastructures without achieving equivalent gains in state coordination or strategic autonomy.

Chart 3 - Infrastructural × Actuation Capacity - Africa, Latin America, the Middle East and Oceania.



Source: Authors. Visualization available at BRICS Tech Forum DSI page[7].

Representative cases such as Colombia (Infrastructure: 50.00; Actuation: 53.13), Nigeria (Infrastructure: 50.00; Actuation: 59.38), Oman (Infrastructure: 50.00; Actuation: 53.13), and New Zealand (Infrastructure: 50.00; Actuation: 62.50) occupy intermediary positions within the graph, illustrating diverse pathways toward digital development. While these countries exhibit meaningful advances in either infrastructural or actuation capacity, none has yet achieved the balanced combination of technological capabilities and institutional autonomy characteristic of the

[7] Available at: https://www.bricstechforum.org/dsi-capacity.

highest-performing states. Their distribution reflects uneven patterns of modernization in which gains in infrastructure, governance, or strategic capacity frequently coexist with persistent forms of technological dependency - see **Table 8** above.

The similarities in Infrastructure Capacity (all of them scoring an exact 50.00) may mask important differences in how these countries combine their hardware and software capabilities, unless we analyze the subdimensions. Colombia achieves its intermediate position through relatively stronger performance in software-related subdimensions, particularly state operating environments and productivity (S1) and critical public-sector systems (S3), despite more limited capabilities in data centers and cloud hardware (H2) and critical components and manufacturing (H3). Nigeria displays a more balanced infrastructural profile, with modest but consistent performance across both hardware and software subdimensions. Oman likewise combines intermediate levels of hardware and software development, although its infrastructural capacity remains constrained by dependence on foreign technological production, particularly in critical components and manufacturing (H3). New Zealand, by contrast, reaches a comparable level of Infrastructure Capacity through a different composition, combining relatively modest hardware capabilities with stronger software performance, especially in state operating environments (S1) and interoperability and data standards (S4). These cases demonstrate that similar aggregate levels of infrastructural capacity may emerge from distinct technological configurations, reflecting different pathways of digital development.

Table 8 - Selected countries scores.

Country	H1	H2	H3	H4	S1	S2	S3	S4	C1	C2	C3	C4	G1	G2	G3	G4	DSI
Colombia	2	1	2	2	3	2	2	2	2	2	2	1	3	2	3	2	**51.56**
	43.75				56.25				43.75				62.50				
	Infrastructural Capacity: 50.00								**Actuation Capacity: 53.13**								
Nigeria	2	2	1	3	2	2	2	2	2	2	2	3	3	2	3	2	**54.69**
	50.00				50.00				56.25				62.50				
	Infrastructural Capacity: 50.00								**Actuation Capacity: 59.38**								
Oman	3	2	1	2	2	2	2	2	3	2	1	2	2	3	2	2	**51.56**
	50.00				50.00				50/-00				50.00				
	Infrastructural Capacity: 50.00								**Actuation Capacity: 53.13**								
New Zealand	2	1	1	2	3	2	3	2	3	2	2	3	2	3	2	3	**56.25**
	37.50				62.50				62.50				62.50				
	Infrastructural Capacity: 50.00								**Actuation Capacity: 62.50**								

Source: Authors.

Greater variation emerges in Actuation Capacity, where institutional and strategic capabilities become more consequential than technological assets alone. Colombia exhibits moderate actuation through relatively balanced performance across the Cognition and Governance dimensions, although without exceptional strengths in any individual subdimension. Nigeria achieves a noticeably higher level of actuation, supported by stronger performance in formal strategies (C1), institutional architecture (G2), and regulatory capacity (G3), indicating a greater ability to coordinate and govern its digital transformation. Oman similarly benefits from comparatively developed governance structures, particularly in legal frameworks (G1) and institutional coordination (G2), although its cognitive capacities remain more limited. New Zealand records the highest Actuation Capacity among these representative cases, reflecting well-developed epistemic communities (C3), narrative autonomy (C4), and active participation in international standard-setting and Internet governance (G4). This illustrates how countries with nearly identical levels of Infrastructure Capacity may nevertheless differ substantially in their ability to formulate strategy, coordinate institutions, regulate digital ecosystems, and exercise influence within the international digital order. As seen previously in the France *versus* Russia case, this Actuation capacity directly impacts, through fungibility, countries industrial capacities.

Beyond these examples, many of the Global South States possess growing digital economies, expanding internet penetration, sophisticated fintech sectors, digital public services, and increasingly ambitious AI or cybersecurity initiatives. Yet these advances frequently remain layered upon infrastructures controlled externally; cloud services, semiconductor supply chains, operating systems, satellite infrastructures, and core platform ecosystems continue to be dominated by foreign actors (Srnickek, 2017). The broader condition observed in the Global South is that in which States modernize digitally without fully internalizing the material and strategic foundations of that modernization. Many aspects of the digitalization of life and the economy, such as connectivity or digital services expand, but infrastructural sovereignty often does not expand accordingly.

This dynamic reflects the recursive relationship previously identified between hardware, software, and cognition. External technological infrastructures frequently generate software lock-in, which subsequently shapes regulatory choices, educational systems, procurement practices, and strategic doctrines, progressively reproducing dependence even as domestic digital capabilities expand. Digital modernization may therefore deepen rather than reduce technological dependency when these layers remain externally governed.

This concentration reflects the emergence of what Srnicek (2017) describes as *platform capitalism*, in which digital platforms evolve from ordinary firms into essential infrastructures mediating economic exchange, communication, cloud services, and increasingly artificial intelligence, allowing technological dependence to become structurally embedded within contemporary capitalism.

This distinction becomes clearer when examining the gap between Infrastructure Capacity and Actuation Capacity. Some countries achieve substantial technological development while exhibiting comparatively weaker institutional capacities to discipline foreign platforms, establish national technological standards, coordinate industrial policy, or sustain long-term digital strategies.

Brazil (Infrastructure: 59.38; Actuation: 56.25) and Argentina (Infrastructure: 65.63; Actuation: 56.25) illustrate this pattern, combining relatively advanced productive capabilities with more limited strategic actuation. Conversely, countries such as South Africa (Infrastructure: 46.88; Actuation: 65.63), New Zealand (Infrastructure: 50.00; Actuation: 62.50), and Nigeria (Infrastructure: 50.00; Actuation: 59.38) demonstrate that stronger governance structures, institutional coordination, or strategic planning can partially compensate for more modest infrastructural foundations.

Iran (Infrastructure: 65.63; Actuation: 53.13) represents yet another trajectory: similar to Russia, the development of its Digital Sovereignty has been shaped by a paradigm of resilience under western sanctions, whereby external restrictions have stimulated domestic technological substitution, strategic planning, and institutional adaptation. Supporting this scenario, recent analyses of the Iranian strategic response to prolonged sanctions suggest that external pressure has accelerated the development of adaptive institutional mechanisms rather than simply constraining national capabilities. Iran progressively developed alternative mechanisms to circumvent international restrictions, including energy export networks, strategic partnerships with Asian markets, and domestic institutional arrangements capable of sustaining technological and economic activity despite prolonged external pressure. Its capacity to preserve strategic autonomy through institutional adaptation, technological substitution, and long-term State coordination appears greater than aggregate scores alone might indicate, and, in this sense, the Iranian experience reinforces one of the central propositions of the DSI: digital sovereignty should be understood not merely as the possession of technological assets, but as the State's capacity to adapt, reorganize, and sustain autonomous technological development under adverse structural conditions (Sousa and Rocha-Dashicheva, 2026).

The United Arab Emirates (Infrastructure: 78.13; Actuation: 87.50) represents a case in which both capacities have advanced simultaneously, occupying the frontier of the Global South. Unlike countries that have prioritized either productive development or institutional coordination, the UAE demonstrates how sustained investment in digital infrastructure, combined with coherent state strategy and governance, can produce comparatively high levels of digital sovereignty despite a relatively recent process of technological modernization.

More broadly, these cases illustrate that digital sovereignty is determined not simply by the accumulation of technological assets, but by the interaction between productive capabilities and the State's capacity to strategically mobilize them. Cognition and Governance therefore act as multipliers of Infrastructure Capacity, enabling States to transform technological resources into enduring sovereign capabilities through strategic planning, institutional coordination, regulatory authority, and knowledge production. Conversely, where these dimensions remain underdeveloped, technological modernization may expand connectivity and digital services without producing equivalent gains in strategic autonomy.

Where these cognitive and governance layers remain comparatively weaker, technological modernization risks remaining externally dependent despite substantial advances in material development. Instead of competing with markets, the Big Tech occupies, more and more, positions from which they extract continuous rents from dependent users and States (Silva et al., 2025). Whether interpreted as the monopolistic evolution of capitalism (Durand, 2024) or as the emergence of a techno-feudal logic centered upon platform ownership and digital rents (Varoufakis, 2024), both perspectives highlight the strategic significance of controlling the infrastructures through which digital activity itself is organized.

These contrasting trajectories ultimately reinforce a broader structural pattern. Although many countries of the Global South have become deeply integrated into the digital economy, integration alone does not necessarily translate into sovereignty. Where Infrastructure Capacity remains externally dependent or Actuation Capacity proves insufficient to strategically govern digital transformation, technological modernization mostly occurs without proportional control over the systems enabling it: States become deeply embedded in global digital networks while exercising only limited authority over the infrastructures governing data storage and cloud computing (H2; S2), semiconductor production and critical technological manufacturing (H3), technical standards and interoperability (S4), digital public platforms and critical state systems (S3), the strategic development of artificial intelligence (C1-C3), and the regulatory frameworks through which digital platforms, data flows, and international digital governance are exercised (G1, G3, G4).

The result resembles earlier historical dependency structures, now reorganized through digital systems. Where colonial economies once extracted raw materials and agricultural commodities, contemporary digital ecosystems increasingly extract data, behavioral information, market dependence, and infrastructural rents. This emerging condition closely resembles the concept of data colonialism (Couldry and Mejias, 2019), whereby the extraction of data replaces earlier forms of colonial resource extraction while preserving the underlying asymmetry of ownership and control. In other words, populations generate enormous informational and economic value through digital participation while ownership, computation, and strategic control remain concentrated elsewhere. And, at the same time, the value extracted is not limited to data itself, but derives from what Zuboff (2019) terms *behavioral surplus*, whereby human experience becomes raw material for predictive products, algorithmic optimization, and commercial governance.

Digital dependency therefore reproduces and expands upon older centre-periphery dynamics in technological form. Cloud dependency replaces industrial dependency; platform dependency replaces communications dependency; algorithmic visibility replaces earlier mechanisms of informational asymmetry. Yet, as Morozov (2022) observes, these emerging forms of dependency should not necessarily be understood as a rupture with capitalism itself, but rather as new mechanisms through which long-standing monopolistic and imperial dynamics continue to operate under digital conditions.

From the perspective developed throughout this study, these mechanisms should not be understood as isolated phenomena, but as mutually reinforcing layers of technological dominance. Platform capitalism (Srnicek, 2017) describes the concentration of digital infrastructures; surveillance capitalism (Zuboff, 2019) explains the extraction of behavioral value from those infrastructures; data colonialism (Couldry and Mejias, 2019) situates this extraction within enduring centre-periphery relations; while debates surrounding techno-feudalism (Varoufakis, 2024) and digital capitalism (Morozov, 2022) seek to characterize the political-economic form through which such dependence is reproduced. The DSI operationalizes these dynamics by measuring the productive and institutional capacities that determine whether states remain embedded within, or can progressively escape, these asymmetric structures.

5 CONCLUSIONS and FINAL CONSIDERATIONS

This article proposed the Digital Sovereignty Index (DSI) as a comparative framework for measuring one of the defining public policy problems of the contemporary technological era: the capacity of states to exercise meaningful control over the technological systems upon which their political, economic, industrial, military, and social functions increasingly depend. Building upon recent debates on technological sovereignty, platform capitalism, surveillance capitalism, data colonialism, techno-feudalism, and digital political economy, the paper argued that digital sovereignty should be understood as a multidimensional state capacity rather than as the possession of individual technologies, the adoption of specific software, or the implementation of isolated regulatory measures.

To operationalize this concept, the DSI combines four analytically distinguished dimensions of Hardware, Software, Cognition, and Governance; evaluated through a common developmental scale based on the progressive expansion of technological control from Use to Value Chain. This architecture allows heterogeneous technological domains to be assessed through a common measurement framework while preserving the multidimensional character of digital sovereignty. At the same time, the framework explicitly recognizes the fungibility of technological power: although analytically separated for measurement purposes, the four dimensions remain empirically interconnected, allowing developments in one domain to reinforce or constrain outcomes in another. The distinction between analytical separation and empirical interaction constitutes one of the principal methodological contributions of the index.

The comparative review of existing measurement initiatives reinforces this conclusion. The Nextcloud Digital Sovereignty Index, EDRIX, the conceptual framework proposed by Di Marco et al. (2025), and the Tricontinental BRICS Digital Sovereignty Index each make valuable contributions to the literature while illustrating different approaches to operationalizing the concept. Their comparison demonstrates that the principal challenge in measuring digital sovereignty is not merely the selection of indicators, but the alignment between ontology, analytical architecture, operationalization, and public policy objectives. By distinguishing analytical dimensions from developmental stages and treating fungibility as an empirical relationship rather than an analytical category, the DSI seeks to strengthen construct validity, transparency, reproducibility, and cross-national comparability.

The empirical application of the index further demonstrates that digital sovereignty is neither binary nor geographically uniform. The DSI reveals multiple developmental trajectories resulting from different combinations of Infrastructure Capacity and Actuation Capacity, and while the Global North continues to concentrate the highest levels of both capacities, distinct paradigms emerge among leading states, including industrial scale, regulatory sovereignty, and resilience under geopolitical constraint, across the Global South, technological modernization follows considerably more heterogeneous trajectories, illustrating that advances in infrastructure, governance, cognition, and industrial capability rarely occur simultaneously. These findings reinforce the proposition that digital sovereignty is accumulated progressively through the interaction of productive, institutional, and cognitive capacities rather than through isolated technological achievements.

Like any comparative index, the DSI also presents limitations. The expert-coded methodology necessarily involves interpretative judgment, despite explicit coding criteria, publicly archived evidence, and systematic documentation intended to maximize transparency and reproducibility. The framework likewise captures technological sovereignty at a particular moment in time, whereas technological capabilities, institutional arrangements, and geopolitical conditions continue to evolve rapidly. Consequently, the DSI should be understood as an evolving measurement framework subject to continuous refinement rather than as a definitive representation of technological sovereignty.

These limitations simultaneously define the future research agenda. First, subsequent versions of the DSI will continue expanding temporal coverage, allowing the construction of longitudinal series capable of identifying trajectories of technological development and institutional change. Second, additional theoretical and empirical work may refine existing subdimensions, improve coding procedures, and incorporate emerging technological domains as they become strategically relevant. Third, the framework opens new possibilities for investigating the causal relationships implied by fungibility, examining how developments in hardware, software, cognition, and governance reinforce one another across different institutional and geopolitical contexts. This also includes assessing whether these interactions exhibit path-dependent dynamics, in which historical institutional, economic, and geopolitical trajectories condition how advances in one dimension are translated into progress in another. Finally, the DSI provides an empirical foundation for future comparative research exploring the relationship between digital sovereignty and broader outcomes such as economic development, industrial policy, state capacity, democratic governance, geopolitical influence, and international technological competition.

Ultimately, the contribution of the DSI extends beyond the construction of a comparative index. It proposes a coherent measurement architecture through which digital sovereignty can be analyzed as a multidimensional, policy-oriented, and empirically observable phenomenon. As technological systems become increasingly central to state power, economic development, and international order, the ability to measure technological sovereignty and to reflect on the processes through which it is constructed - with conceptual clarity, methodological transparency, and comparative rigor - becomes an increasingly necessary condition for understanding and governing the digital age.

REFERENCES

COULDRY, Nick, MEJIAS, Ulises A. **The Costs of Connection**. Stanford University Press, 2019.

DURAND, Cédric. **How Silicon Valley Unleashed Techno-Feudalism: The Making of the Digital Economy**. London: Verso, 2024.

DI MARCO, D.; THABIT, S.; KOTSEV, A.; CHRISTENSEN, A.; MINGHINI, M. et al. **Open but Not Powerless: Towards a Common Understanding of EU Digital Sovereignty**. Ispra: European Commission, Joint Research Centre, 2025.

FRANCE. **Direction générale des entreprises (DGE). La France mobilise l'écosystème numérique pour renforcer sa souveraineté technologique**. Paris: Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, 2025.

HARDT, Michael, NEGRI, Antonio. **Empire**. Harvard University Press, 2001.

INSTITUT MONTAIGNE. **Toward European Digital Sovereignty: The Implementation Test**. Paris: Institut Montaigne, 2025.

MOROZOV, Evgeny. Critique of Techno-Feudal reason. **New Left Review**, 133/134, 2022.

OECD. **OECD Economic Surveys: France 2026.** OECD Publishing, 2026. DOI: https://doi.org/10.1787/e88a1716-en.

_____. **OECD Reviews of Innovation Policy: Russian Federation**. OECD Publishing, 2026. DOI: http://dx.doi.org/10.1787/9789264113138-en.

_____. **What makes a productive Russian firm? A comparative analysis using firm-level data**. Paris: OECD Publishing, 2019. (OECD Economics Department Working Papers, n. 1592). DOI: https://doi.org/10.1787/8590f752-en.

MACRON, Emmanuel. **Faire de la France une puissance de l'intelligence artificielle**. Paris: Présidence de la République (Élysée), 2025.

NEXTCLOUD. Digital Sovereignty Index. 2025. Available at: https://dsi.nextcloud.com/report.php.

RAEL, Robson. O Novo Banco de Desenvolvimento: Um meio de exercício de poder para o BRICS. Editora Dialética, 2022. DOI: https://doi.org/10.48021/978-65-252-2718-4.

RAISE SUMMIT. **Geopolitics of Chips**. Paris: RAISE Summit, 2026.

RESNIK, David B., HOSSEINI, Mohammad. The ethics of using artificial intelligence in scientific research: new guidance needed for a new tool. **AI Ethics**. 5(2), 2025. DOI: https://doi.org/10.1007/s43681-024-00493-8.

ROCHA-DASHICHEVA, Isabela Wagnerovna. The three levels of Technological Dominance: hardware, software and cognition in global south defense architectures. **Revista InterAção**, v. 17, n. 1, 2026. DOI: https://doi.org/10.5902/2357797595118.

ROCHA-DASHICHEVA, I. W.; DASHICHEV, A. D.; LUDOVICO, L. B.; PIAZZA, F. C.; SILVA, E. C. de M.; VAZ, J. C.; LUCENA, J. P. F. de O.; CARNEIRO, G.; TEIXEIRA, L.; ROCHA, I.; MAGALHÃES, N.; CAMELLO, J.; SIMONI, C. I.; RAEL, R. C.; SILVA, I. V. C. A. de S. e.; TÉLLEZ-ZEPEDA, C. A. **Digital Sovereignty Index [v. 1.0]: an expert-coded country ranking**

of digital sovereignty. Versão 1.0. Zenodo, 2026a. DOI: 10.5281/zenodo.20277297. Disponível em: https://doi.org/10.5281/zenodo.20277297.

ROCHA-DASHICHEVA, Isabela; DASHICHEV, Alexander; LUDOVICO, Laura Beatriz; PIAZZA, Felipe Camargo; SILVA, Ergon; VAZ, José Carlos; LUCENA, João Falcão de Oliveira. **Digital Sovereignty Index (DSI): Country Evidence Dataset**. Versão 1. Harvard Dataverse, 2026b. DOI: https://doi.org/10.7910/DVN/QOIA6F.

SILVA, E. C. de M.; ROCHA, I.; VAZ, J. C.; VENEZIANI, J. R. de A.; MODANEZ, C. de C. Entre licenças bilionárias e nuvens internacionais: um mapeamento sistemático de contratos do setor público brasileiro com fornecedores internacionais de tecnologias. InterAção, [S. l.], v. 16, n. 4, 2025. DOI: https://doi.org/10.5902/2357797593697.

SILVA, Luciana Mara; DORNELLES, Dayane (org.). **Guia para uso ético da inteligência artificial generativa**. Florianópolis: UDESC, 2025.

SRNICEK, Nick. **Platform Capitalism**. Cambridge: Polity Press, 2017.

TRICONTINENTAL: INSTITUTE FOR SOCIAL RESEARCH. **BRICS Digital Sovereignty Index Report**. Tricontinental: Institute for Social Research, 2026.

VAZ, José Carlos. Access to technology as the subject of public policy: rights, democracy, development and national sovereignty. In: Survey on the use of information and communication technologies in Brazilian households : ICT households 2015. São Paulo, Comitê Gestor da Internet no Brasil, pp. 197-206, 2016.

________________. Soberania e autonomia tecnológica: a tecnologia como capacidade estratégica do Estado. In.: SILVA, Orlando, MIELLI, Renata, CUGLER, Ergon. **Soberania Digital: Desafios do presente para um Brasil do Futuro**. Kotter editorial, 2026. ISBN: 978-65-5361-584-7.

VAROUFAKIS, Yanis. **Technofeudalism: What Killed Capitalism**. London: The Bodley Head, 2024.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. New York: PublicAffairs, 2019.