Digital Cooperation Organization

Cooperative Digital Sovereignty and Artificial Intelligence

Promoting Resilience, Strategic Openness, and Self-Determination

Disclaimer

Authors and Contributors

Authors

Luca Belli
Professor at FGV Law School, Rio de Janeiro
Director of the Centre for Technology and Society at FGV

Ahmad Bhinder
Digital Policy & Intelligence Director
Digital Cooperation Organization

Reviewers

Walter Britto Gaspar
Professor at FGV EMAp,
Rio de Janeiro

Seabe Setshwaelo
Managing Director,
NAARA Group

Matthew Sharp
Associate Director,
Access Partnership

Alaa Abdulaal
Chief of Digital Economy Intelligence
Digital Cooperation Organization

Omar A. Alnemer
Chief of Council affairs,
Digital Cooperation Organization

Rashed Alsehaly
Chief of Legal & Governance,
Digital Cooperation Organization

Rebecca Cousins
Chief of Outreach & Global Communications,
Digital Cooperation Organization

Kevin Muvunyi
Digital Policy Assistant Manager,
Digital Cooperation Organization

Table of Contents

Executive Summary

Artificial intelligence (AI) is rapidly becoming a foundational layer of the global digital economy, shaping economic competitiveness, industrial development, public administration, security, military, and geopolitical influence. At the same time, the infrastructure and capabilities underpinning contemporary AI systems – including compute infrastructure, semiconductors, frontier AI models, data ecosystems, and advanced research capacity – are increasingly concentrated within a relatively small number of firms and jurisdictions. This growing concentration has intensified global debates around digital sovereignty, technological dependency, resilience, and strategic autonomy.

Digital sovereignty is not a universally defined concept, and uninformed debates risk presenting a false dichotomy, portraying sovereignty as autarky in opposition to openness. This paper argues that such binary framings are increasingly inadequate for understanding the realities of the contemporary AI economy and offers a way to frame a constructive notion of "Cooperative Digital Sovereignty."

In practice, few countries are likely to achieve technological self-sufficiency across every layer of the AI stack. As stressed by the study, this outcome is not necessarily desirable either, as the fundamental goal of Cooperative Digital Sovereignty must be to retain the capacity for choice, technological autonomy, and resilience, while avoiding lock-in and vulnerability to coercive use of dependencies. The extraordinary capital intensity, technological complexity, and structural concentration characterizing AI ecosystems significantly constrain the feasibility of complete technological autonomy, particularly for emerging and middle-income economies.

Under such conditions, the central policy question is not whether states should engage in global digital and AI ecosystems, but how they can participate in ways that capture meaningful economic and developmental value, while preserving their sovereign rights and technological autonomy.

Within this context, the paper advances the concept of Cooperative Digital Sovereignty, defined as: "the capacity of states and societies to understand, develop, govern, and benefit from digital and AI systems, advancing their national priorities while fostering their technological autonomy, including by leveraging open-source technologies, interoperability, and trusted cooperation."

This definition reframes sovereignty and cooperation not as contradictory objectives, but as mutually reinforcing dimensions of sustainable digital governance. The paper argues that carefully designed forms of interoperability, coordinated governance, resilience-oriented cooperation, and structured openness play an instrumental role in strengthening the states' ability to preserve self-determination and agency under conditions of deep technological interdependence.

Building on multiple research outcomes elaborated by the authors to discuss digital sovereignty, AI governance, innovation systems, and political economy, the study develops a comprehensive analytical framework: **DCO Framework for Cooperative Digital Sovereignty** – structured around twelve interconnected Key AI Sovereignty Enablers:

01 Data;

02 Software Ecosystems, AI Models & Open-Source Capabilities;

03 Compute, Semiconductors & Hardware Infrastructure;

04 Meaningful Connectivity;

05 Energy Availability & Resilient Power Infrastructure;

06 Skilled Human Capital, Research Capacity & Scientific Ecosystems;

07 Cybersecurity & Cyber-Resilience Capabilities;

08 Risk-Based Frameworks;

09 Cognitive-Informational Resilience;

10 Access to Capital & Financing Ecosystems;

11 Industrial & Supply-Chain Capabilities;

12 Technical Standardization Capacity.

These enablers can be grouped into four macro-categories:

01 Digital Assets, which includes data; software & AI models;

02 Foundational infrastructure, with include compute, hardware, connectivity energy and power;

03 Productive capacity, which includes skilled human capital, capital and financing, and supply chain capabilities;

04 and Safety and security, which include risk-based frameworks, cybersecurity and resilience, cognitive-informational resilience and technical standardization.

Importantly, the paper demonstrates that these enablers do not evolve independently. Rather, they interact continuously across governance, regulation, industrial policy, capacity-building, and international cooperation dimensions.

Hence, the study argues that isolated or fragmented interventions may be counterproductive as they are unlikely to produce meaningful and sustainable outcomes. What is required instead is a systemic and strategically prioritized approach capable of aligning technological, institutional, regulatory, economic, and governance ecosystems over time.

Figure 1. DCO Framework for Cooperative Digital Sovereignty: The twelve Key AI Sovereignty Enablers and the five dimensions of cooperative digital sovereignty

Cooperation is the cross-cutting 5th dimension applied across every enabler.

4 Categories of Key AI Sovereignty Enablers”.	Governance	Regulation	Industrial policy	Capacity building	Int’l cooperation & interoperability
1. Digital Assets • Data • Software & AI models					
2. Foundational Infrastructure • Compute & Hardware • Connectivity • Energy & power					
3. Productive Capacity • Skilled human capital • Capital and financing • Supply chain capabilities					
4. Safety and Security • Risk-based frameworks • Cybersecurity & resilience • Cognitive-informational resilience • Technical standardization					

The paper further emphasizes that international cooperation should not be understood as unstructured and generic participation to global forums. Instead, cooperation is conceptualized as a strategic instrument aimed at fostering scientific, trade and diplomatic efforts through organically structured participation into multistakeholder and multilateral processes.

The goal of such cooperation is therefore to leverage trusted partnerships to strengthen domestic resilience, diversify technological options, reduce excessive structural dependencies, and improve participation in the global AI economy and policymaking. However, it must be noted that cooperation does not always occur within fully trusted partnerships. In such cases, to balance the benefits of cooperation with the need to preserve strategic autonomy, open source and interoperability become particularly valuable as an enablers of both cooperation and switching.

Indeed, even where trust is limited but material value can be gained, interoperability and openness can provide the protections needed to safeguard autonomy while still capturing the benefits of cooperation. In this regard, interoperability – in both its technical and legal conceptions – emerges as a particularly important mechanism for operationalizing cooperative digital sovereignty. This study argues that, rather than seeking complete harmonization of legal or technical systems, interoperability-oriented approaches can enable trusted cross-border and cross-system cooperation while preserving autonomy.

To illustrate the current state of play, the study analyzes several structural dynamics shaping contemporary digital and AI sovereignty debates, including the concentration of compute infrastructure and cloud ecosystems, asymmetries in semiconductor production and advanced research capabilities, the strategic role of open-source ecosystems and Digital Public Infrastructure (DPI), the concentration of capital and the allocation decisions of major financing pools that shape who advances fastest, and the growing geopolitical significance of standards-setting and AI governance frameworks.

The paper argues that commitment to openness alone does not automatically produce equitable technological ecosystems. Notably, open-source models, interoperable infrastructures, and DPIs may strengthen innovation and participation under certain conditions, but may also reproduce dependency if underlying compute, cloud, or infrastructure layers remain highly concentrated. Consequently, digital sovereignty requires strategic use of openness.

The paper also highlights the increasing importance of resilience-oriented infrastructure partnerships, including federated compute systems, regional cloud ecosystems, coordinated cybersecurity architectures, trusted digital public infrastructure, and cross-border energy integration.

Such cooperative arrangements may provide more realistic pathways toward resilience and participation in capital-intensive AI ecosystems for technologically dependent countries, a term we use to encompass a heterogeneous array of countries – from emerging economies to highly developed ones – that share high levels of digital dependencies.

Based on this analysis and leveraging previous research aimed at identifying "Key AI Sovereignty Enablers", the study sets out strategic considerations and options that DCO Member States may wish to consider, in line with their national priorities. It argues that governments should adopt strategically prioritized, maturity-sensitive, and institutionally realistic approaches.

The study illuminates paths that DCO Member States may consider in order to strengthen institutional capacity and governance mechanisms, operationalize interoperability-oriented regulatory frameworks, invest selectively in resilient and cooperative infrastructure ecosystems, enhance cybersecurity and AI safety coordination, strengthen participation in international standards and governance processes, and develop sustainable financing and innovation ecosystems.

To achieve these goals, the paper further emphasizes the importance of trusted cross-border data transfers, resilient Digital Public Infrastructure, open-source ecosystems, and long-term investments in human capital, research ecosystems, and capacity-building mechanisms.

Conspicuously, the paper notes that intergovernmental platforms such as the Digital Cooperation Organization (DCO) are well positioned to support the operationalization of cooperative digital sovereignty among their membership and circles of influence.

The study highlights several DCO initiatives and instruments that collectively form the foundations of an emerging operational governance ecosystem, including the DCO Interoperability Mechanism for Cross-Border Data Flows, the DCO Privacy Principles, DCO Model Contractual Clauses (MCCs), the DCO Principles for Ethical AI, the DCO AI Ethics Evaluator, the Ethical AI Guidebook for Policymakers, the AI-REAL Toolkit, the Digital Economy Navigator (DEN), and the DCO Data Embassy concept.

Taken together, these initiatives — adopted through the DCO's established, Council-approved processes — provide a strong basis upon which interoperability-oriented governance, structured cooperation, and resilience-focused digital governance models can be built to support DCO Member States in strengthening technological agency while remaining integrated within global digital ecosystems. More broadly, the paper argues that the future of digital sovereignty is unlikely to depend on the pursuit of complete technological self-sufficiency.

Rather, it will increasingly depend on states' ability to govern technological interdependence strategically, operationalize trusted forms of cooperation, strengthen institutional and infrastructural resilience, and participate in the global AI economy and governance on strategically autonomous terms.

In this sense, the vision of Cooperative Digital Sovereignty put forward by this study offers not a retreat from globalization or technological interconnectedness, but a pragmatic assessment and operational framework for navigating an increasingly interdependent, concentrated, and geopolitically contested digital and AI landscape

1. Introduction: Digital Sovereignty, Artificial Intelligence and Cooperation

Artificial Intelligence (AI) is increasingly recognized as a foundational technology underpinning digital transformation, shaping economic development, redefining governance, and playing an increasingly essential role in geopolitical – and even military – competition [11] . AI technologies rely on complex ecosystems composed of data infrastructure, software and hardware resources, connectivity networks, highly specialized human capital, and robust cybersecurity and risk-management frameworks.

As a result, national control over digital infrastructure and technological capabilities has become a central element of economic competitiveness and strategic autonomy. Contemporary discussions on digital governance therefore increasingly emphasize technological capacity and regulatory authority over digital systems as central elements of digital sovereignty. [4,5,9,31,41,56]

This discussion is particularly relevant as most countries are "technologically dependent", a term we use in this study to encompass a heterogeneous array of countries – from emerging economies to highly developed ones – that share high levels of digital dependency of different sorts.

Importantly, this report aims to clarify that the pursuit of digital sovereignty should not be equated with the construction of technologically isolated ecosystems or forms of digital autarky. While attempts in this direction may exist, the research in this report posits that digital sovereignty should be understood as the capacity to shape domestic technological trajectories, as well as governance mechanisms and regulatory frameworks, while preserving the ability to engage in cross-border cooperation through open, secure, and interoperable digital systems.

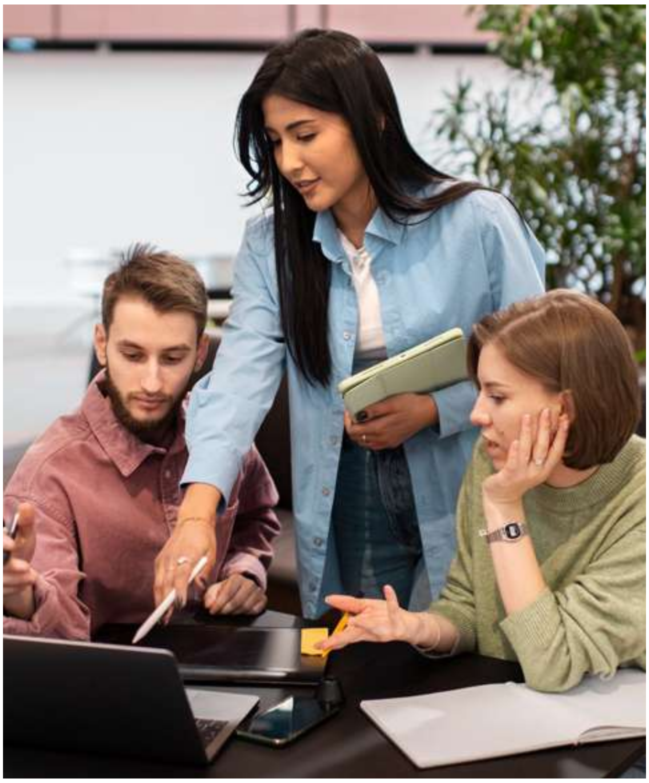
A decentralized yet cooperative model of digital governance reflects the foundational architecture of the internet itself – conceived as a global "network of networks" – in which autonomous systems interact through interoperable standards and mutually agreed governance mechanisms for their collective benefit. [2,48]

Building on this premise and on previous research on this issue, this paper advances the concept of Cooperative Digital Sovereignty, which this study defines as **"the capacity of states and societies to understand, develop, govern, and benefit from digital and AI systems, advancing their national priorities while fostering their technological autonomy, including by leveraging open-source, interoperability, and trusted cooperation." [5,6,9,11,32,41,56]**

Hence, this concept refers to the pursuit of technological autonomy in relation to the capacity to exercise control and preserve freedom of choice within and throughout critical digital and AI capabilities and governance, while maintaining the highest possible degree of openness, interoperability and multistakeholder cooperation.

By preserving access to diverse technological pathways, knowledge ecosystems, and international partnerships, such an approach enhances strategic agency, mitigates lock-in effects, and supports the effective exercise of self-determination.

Often considered by international law scholars as "the principle of principles" for its importance as an enabler of all other fundamental rights under international law, the right to self-determination is enshrined in Article 1(2) of the UN Charter and the International Covenants on Human Rights, which recognize that "all peoples have a right to self-determination" and may "determine their political status and pursue their economic, social and cultural development."



For the purposes of this report, references to self-determination are employed as an analytical and policy framework for discussing technological agency and autonomy.

Such references should not be construed as asserting that international law recognizes a distinct legal right to digital or AI sovereignty, but rather that such concepts can be built as an extension of the established right of peoples to self-determination.

In this context, this study aims at emphasizing that the internal dimension of self-determination – i.e. the right to freely determine and pursue one's economic, social, and cultural development enshrined by the UN Charter, the ICCPR and ICESCR – is a fundamental pillar of digital sovereignty as it encompasses the right to freely exercise autonomous choice regarding development, adoption and regulation of digital technologies and AI systems, in accordance with the fundamental values enshrined in national constitutions.[1]

Indeed, this conception is grounded in the recognition that states can effectively exercise the sovereign prerogatives regarding their economic, scientific and technological development only when they are able to shape and influence the key elements of research, development, adoption, and regulation of digital technologies and AI systems in accordance with their domestic law and constitutional values.

1. This internal aspect aligns with "informational self-determination," first recognized by the German Federal Constitutional Court in the 1983 Census decision, which forms the basis of personal data protection conferring to individuals the fundamental right to know who is collecting data about them, for what purpose and with whom such data are shared. In this perspective, digital sovereignty aims at preserving not only the individual dimension of informational self-determination, but also the collective one, according to which collective entities such as nation states have the right to know who is collecting data they generate, for what purposes and under what cybersecurity standards, and who is extracting value form such information and being fairly compensated for such value extraction.[9, 12, 14]

Importantly, this paper emphasizes that the exercise of this prerogative does not need to be translated into isolationist, protectionist or authoritarian practices, but rather be reflected in structured cooperation that enables systemic openness and innovation, while allowing for the implementation of national laws.

Ideally, to facilitate this approach, cooperation should be grounded in legally interoperable regulatory frameworks and technically interoperable digital architectures. Such a scenario can be achieved by the promotion of multinational research initiatives, shared technological and compute infrastructures, and the collaborative advancement of open protocols and open-source technologies.

Importantly, however, legal interoperability is not costless: because interoperable regimes must be mutually compatible, they exert pressure toward regulatory convergence, which can itself narrow the space for domestically determined rules.

An ideal approach to Cooperative Digital Sovereignty, therefore, should distinguish between the layers at which interoperability is pursued. Convergence can be enact more easily at the technical and procedural layer — shared formats, interfaces, conformity-assessment and mutual-recognition mechanisms — thus lowering the cost of cooperation.

The substantive determination of what behavior is permitted, prohibited, or protected remains a matter of domestic law and constitutional values, and is more difficult to subordinate to the demands of compatibility. Hence, sovereignty is preserved not by rejecting interoperability but by governing where, and at which layer, it applies.

Through interoperability mechanisms, cooperative digital sovereignty can reconcile national strategic objectives with the collective benefits of international cooperation in the development, deployment and governance of digital technologies and AI systems.

1.1 Structural Power and Technological Interdependence

Debates on digital sovereignty raise fundamental questions regarding the role of digital technologies and infrastructures – particularly those underpinning AI systems – in shaping national development trajectories and technological autonomy. These debates center on whether such technologies can function as drivers of innovation, productivity, and inclusive growth, or whether they risk reinforcing structural dependencies within the global digital economy.

Debates on digital sovereignty raise fundamental questions regarding the role of digital technologies and infrastructures – particularly those underpinning AI systems – in shaping national development trajectories and technological autonomy. These debates center on whether such technologies can function as drivers of innovation, productivity, and inclusive growth, and whether technological dependencies can be managed so they do not harden into structural subordination, given that dependencies are unavoidable in a globally distributed landscape of R&D and financing.

Notably, digital sovereignty discussions increasingly echo the concerns articulated in Susan Strange's analysis of structural power, highlighting how the capacity to understand and shape key technological infrastructures, data flows, financial resources, and knowledge systems is essential to determining the distribution of power between states, market players and individuals [65].

Such structural power, significantly more than classic national or international law tools, has become the primary modality of regulation [49] of digital systems.

Crucially, the 'winner-takes-most' logic inherent to digital platforms – coupled with the large-scale integration of AI across public and private sectors – threatens to foster a global dependency on a narrow oligopoly of providers [1,9,66]. These entities effectively exercise governance through private digital and AI infrastructure, displacing state authority, and bypassing democratic accountability despite the essential nature of the services they provide.

These considerations are particularly salient in the current geopolitical environment, characterized by increasing fragmentation, strategic competition, and technological rivalry. In this context, both states and private actors encounter significant opportunities to harness digital technologies and AI for social and economic development, while simultaneously facing risks associated with coercive use of interdependence [31], regulatory asymmetries, and external pressures that may unduly influence and undermine domestic policymaking, corporate competitiveness, and individual autonomy.

Against this backdrop, the modalities through which digital technologies and AI systems are adopted, developed, and regulated require careful and systematic policy assessment. Such evaluation is essential not only to mitigate the potential consequences of geopolitical volatility and to safeguard fundamental rights, but also to avoid policy responses that may lead to counterproductive outcomes, including excessive protectionism or unnecessary technological isolation.

A wide range of heterogeneous stakeholders – including governments, corporations, research institutions, civil society organizations and individuals – have a legitimate yet varying interests in maintaining effective control over the digital technologies they deploy, the data resources they generate and process, and the AI systems that increasingly shape social, economic, and political life. Importantly, these interests are not identical and often stand in tension: a state's authority, a firm's commercial control, and a community or an individual's autonomy can pull in opposing directions, and "control" therefore may mean something different for each.

Cooperative digital sovereignty does not assume these interests align, but seeks arrangements in which each can be meaningfully exercised. At the same time, the global digital economy and AI ecosystems are characterized by strong asymmetries and concentration in technological capabilities and infrastructure ownership, which can undermine stakeholders' control over such strategic digital assets[58].

Indeed, a small number of large technology companies and technologically advanced countries dominate key segments of the digital economy and AI value chain, including cloud infrastructure, advanced semiconductor production, foundational model development, operating systems, and data processing.

These dynamics contribute to structural dependencies that may limit the ability of many countries to independently develop and govern digital technologies and AI systems[61]

These structural asymmetries create multiple risks and potential vulnerabilities for countries that lack domestic technological capabilities [9]. In response, governments around the world have adopted national AI strategies, data governance frameworks, and industrial policies aimed at strengthening technological capacity and reinforcing their ability to shape digital development processes. However, this report emphasizes that well-intentioned, digital and AI sovereignty initiatives may often suffer from lack of systemic thinking, operational capacity, or coherent implementation.

From this perspective, the work in this report advances a cooperative conception of digital sovereignty, grounded in the recognition that the legitimate pursuit of sovereignty may entail inherently complex policy and legal trade-offs.

States must reconcile the legitimate objective of capturing the economic and strategic benefits associated with the development of autonomous AI capabilities with the need to mitigate risks related to inefficient allocation of resources, adoption of underperforming technologies, and potential erosion of international competitiveness within an increasingly integrated global digital economy.

From a self-determination perspective, this also means guarding against the displacement of democratic state authority by an oligopoly of private providers whose control over essential digital systems can constrain state capacity to operate, citizens' freedoms and business capacity to innovate and compete [9].

1.2 From Digital Sovereignty to Cooperative Digital Sovereignty

The concept of digital sovereignty has emerged as a central analytical and policy framework in debates on digital governance and has been increasingly applied to AI governance. The growing prominence of digital sovereignty in policy discourse reflects legitimate concerns.

Yet, it is important to emphasize that the concept remains notably indeterminate and can be invoked to justify a wide range of highly heterogeneous policy choices. Some may be socially desirable, others may not, and some may even be internally contradictory. In the absence of a universally agreed definition of digital sovereignty, purported risks may be mobilized to advance agendas that have little to do with genuine technological autonomy or the promotion of public interest.

Such agendas may, in some cases, undermine openness, empowerment, innovation, competition and cooperation, despite being pursued in the name of digital sovereignty.

One of the core preoccupations of this study is therefore to dissipate potential confusion, shed light on the meaning of digital sovereignty – particularly in relation to AI governance – and propose a constructive approach to the concept. Based on relevant literature, digital and AI sovereignty can be understood as **"the capacity of a given country to understand, develop and regulate digital or AI systems, thus retaining self-determination, agency, and control over such systems."** [,6,9,11]

This definition emphasizes that sovereignty discussions applied to digital and, particularly, AI technologies involve not only formal regulatory authority, but also the technological, institutional, scientific, and policymaking capabilities necessary to shape the development, governance, and commercialization of such systems.

In this sense, AI sovereignty can be understood as a particularly demanding case of digital sovereignty: the compute, data, and talent-intensity of contemporary AI raises the threshold of capability a state must reach in order to exercise it.

From this perspective, digital sovereignty encompasses several interrelated dimensions which can be grouped as follows:

01 **Capability dimensions**
the capacity to generate technological knowledge and expertise; to develop, operate, and scale digital infrastructure and computational resources; and robust research and innovation ecosystems.

02 **Governance dimensions**
governance institutions capable of facilitating communication and coordination amongst the key stakeholders operating in these capabilities and translating them into actionable regulation, industrial policy, capacity-building, and strategic frameworks; and the ability of users and institutions to exercise meaningful control over data and digital technologies.

03 **Openness and cooperation dimensions**
competitive and contestable markets; innovation through open and interoperable systems; and cross-border, multistakeholder collaboration.

These elements collectively enable states and societies to exercise meaningful agency over digital transformation processes while ensuring that technological development aligns with national priorities and societal values [9,56]. These dimensions do not always reinforce one another.

Control, openness, and competition can pull in different directions, and the task of digital sovereignty is to define what is the most appropriate balance amongst them rather than to maximize any one in isolation. Hence, at its best, digital sovereignty can serve as a constructive organizing principle. Properly framed, it is not about insulation or technological nationalism, but about empowering individuals, institutions, and markets to participate meaningfully in digital ecosystems.

Understood in this way, sovereignty is not diminished by interdependence; it is strengthened by the capacity to navigate it strategically, as it is discussed in the following sections.

That said, it is important to emphasize that all stakeholders should be aware that, in the absence of a universally agreed definition, the use of the digital sovereignty concept is not without risks. Like many policy ideas that gain rapid traction, digital sovereignty is susceptible to instrumentalization.

On the one hand, it may be invoked to justify restrictive measures that consolidate undue censorship or surveillance, limit competition, or favor domestic incumbents under the guise of strategic autonomy. The line between legitimate industrial policy and protectionism is often thin; between public interest and cronyism, thinner still. These risks are not hypothetical and reflect well-documented tendencies in digital governance and AI policy debates.

On the other hand, a more recent concern is the rise of what might be described as "sovereignty washing." Both public and private actors increasingly label initiatives as "sovereign" – whether cloud services, data infrastructures, or AI systems – without providing meaningful guarantees of control, interoperability, or openness. In many cases, such initiatives amount to little more than the localization of certain technical components. This risks diluting the concept and misleading policymakers.

This study aims at reaffirming that digital sovereignty should not be interpreted as technological isolation or digital protectionism, considering that technological development relies heavily on international collaboration on research and development, cross-border data flows, and global supply chains. Building on this understanding, this study posits that the most effective, constructive, and sustainable way to promote digital sovereignty is through cooperative digital sovereignty, to be framed in the terms set out above.

Throughout this study, "cooperative" refers to structured, trusted cooperation among states and institutions — multilateral and multistakeholder — rather than to the cooperative or commons tradition in economic organization.

Crucially, a decentralized, autonomous, yet cooperative model of digital and AI sovereignty would reflect the foundational ethos of the Internet, which has driven digital governance debates over the past decades.

Indeed, the autonomous systems that compose the internet have been interacting for decades through mutually agreed and interoperable standards for their reciprocal benefit [40]. The same history is instructive in a second respect: openness at the protocol layer did not prevent concentration at the application layer.

This underscores that cooperative sovereignty depends not on openness alone, but on where openness and interoperability are deliberately located within the stack.

From this perspective, cooperative digital sovereignty denotes the pursuit of technological autonomy, including in critical AI capabilities and governance, combined with strategic openness, thereby preserving the widest array of technological options. Such an approach enhances agency, safeguards freedom of choice, and ultimately supports the effective realization of the fundamental right to self-determination.

Thus, a cooperative approach to digital sovereignty should enable countries to combine resources, align regulatory frameworks providing similar levels of rights-protection and legal certainty, and jointly develop digital infrastructures while maintaining their capacity to exercise sovereign authority.

Such alignment is best understood as convergence on shared principles, comparable levels of rights-protection, and interoperable mechanisms of mutual recognition, rather than full harmonization of substantive law. Significantly, recent scholarship highlights that this type of approach may be particularly beneficial for emerging economies, which must simultaneously ensure effective right-protections with development-favorable frameworks, while often facing structural constraints in developing large-scale technological infrastructures independently [11,41,].

1.3 The Role of International and Intergovernmental Organizations

International and intergovernmental organizations serve as important architects for a coherent and interoperable global digital architecture by facilitating the creation of shared rules, common standards, and trusted cooperation mechanisms. In a historical moment where digital ecosystems are highly susceptible to regulatory fragmentation, intergovernmental organizations provide an essential neutral ground, necessary to negotiate interoperable frameworks for most of the Key AI Sovereignty Enablers presented in Section 3 of this study.

By codifying these shared protocols, they can help prevent the emergence of conflicting national mandates that stifle global innovation, ensuring instead that emerging technologies develop within a cohesive, mutually recognizable legal and technical ecosystem - interoperable at the points of connection, without requiring uniformity of substantive law.

Furthermore, some of these platforms, particularly multilateral development banks and development-focused institutions, act as vital mechanisms for coordinating funding and technical assistance, ensuring that financial resources are strategically directed toward bridging various forms of digital divides.

By aligning the national investment priorities of their members, development institutions and intergovernmental organizations, working in cooperation with private stakeholders, can help de-risk infrastructure projects in underserved regions and scale up high-impact digital initiatives.

This coordinated stewardship of financial and institutional resources - through mechanisms such as blended finance, shared infrastructure projects, and coordinated technical assistance - transforms fragmented regional funding into a more coherent global effort to build equitable infrastructure, ensuring that digital advancement is not a privilege of wealthy nations but a shared global achievement.

Positioned at the intersection of policy coordination and international dialogue, organizations such as the DCO are particularly well placed to articulate and promote a normative baseline for cooperative digital sovereignty that resists both fragmentation and capture. By advancing shared principles grounded in openness, interoperability, and inclusive innovation, they can help align national strategies while preserving flexibility for local adaptation.

For such organizations, the task is therefore twofold: to promote a coherent and constructive vision of digital sovereignty, and to guard against its misuse. Doing so requires not only normative clarity, but also the development of practical criteria capable of distinguishing substantive sovereignty from its rhetorical approximations.

In practice, substantive digital sovereignty can be distinguished from its rhetorical approximations by four practical tests:

01 **Capability**
whether measures develop and sustain genuine domestic technological capabilities and reduce structural dependencies, rather than merely rebranding pre-existing initiatives while perpetuating unsustainable reliance on external providers.

02 **Rights and competition**
whether they protect fundamental rights and preserve competitive, contestable markets, rather than entrenching the power of incumbent firms or public authorities.

03 **Openness and interoperability**
whether they maintain openness, interoperability and effective switching possibilities, rather than reinforcing technological lock-in.

04 **Cybersecurity and data governance**
whether they demonstrably uphold information security, data protection and applicable legal safeguards, rather than treating these commitments as subordinate to claims of sovereignty.

Measures that fail these tests are more likely to represent 'sovereignty-washing' than substantive digital sovereignty.

Within this ecosystem, the DCO is uniquely positioned to facilitate dialogue and cooperation among its Member States on issues related to digital and AI governance, and technological development. As an intergovernmental organization dedicated to promoting inclusive and sustainable digital transformation, the DCO provides a neutral and trusted platform capable of supporting policy coordination, capacity building, and collaborative technological initiatives - as discussed in Section 6.

This role is reflected in a growing portfolio of initiatives, including the DCO Interoperability Mechanism for Cross-Border Data Flows, the DCO Privacy Principles, the DCO Model Contractual Clauses (MCCs), the DCO Principles for Ethical AI, the DCO AI-REAL Toolkit, the DCO AI Ethics Evaluator, the Digital Economy Navigator (DEN), the DCO Data Embassy initiative aimed at strengthening digital resilience and trusted data hosting, and emerging efforts to advance international cooperation on AI safety and governance.

Together, these initiatives seek to operationalize trusted and interoperable approaches to digital and AI governance.

As argued in Section 6, organizations such as the DCO may act as important catalysts for cooperative digital sovereignty by providing guidance on how to design and implement governance frameworks aimed at fostering interoperability across the AI stack — spanning infrastructure, data, compute, model development and deployment, and applications.

From legally interoperable data governance systems, and trusted cross-border data flows, to joint research and development initiatives aimed at strengthening digital and AI infrastructures, to collaborative AI safety efforts, ethical governance frameworks, and cybersecurity standards, such organizations can offer practical pathways for strengthening technological capacity while preserving integration within global digital and AI ecosystems.

2. Preliminary Considerations for Digital Sovereignty Debates: Innovation Systems, State Capacity, and AI Concentration

Digital sovereignty cannot be "achieved" through isolated use of regulation or industrial policy in specific sectors. Such a framing, indeed, would understate the structural complexity of the issue at stake. What is ultimately at stake is not a single capability, but the need to understand the interplay between a complex set of variables and to steer the reconfiguration of economic, institutional, normative, and technological power.

Indeed, AI systems do not arise or emerge in isolation and, as illustrated in the next section, depend on multiple interdependent enablers of technological development and strategic autonomy, including data availability, compute capacity, power availability and energy infrastructure, connectivity networks, semiconductors, software ecosystems, research capabilities, cybersecurity frameworks, access to capital, and highly specialized human talent [7,8,10,12].

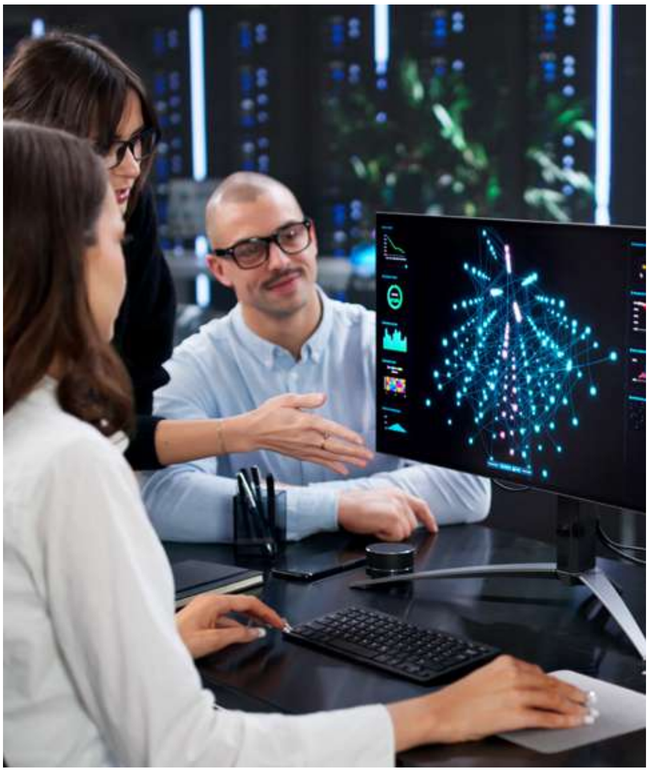
These enablers can be grouped into four macro-categories:

01 Digital Assets, which includes data; software & AI models;

02 Foundational infrastructure, with include compute, hardware, connectivity energy and power;

03 Productive capacity, which includes skilled human capital, capital and financing, and supply chain capabilities;

04 and Safety and security, which include risk-based frameworks, cybersecurity and resilience, cognitive-informational resilience and technical standardization.



Importantly, as we will argue in the following sections, the effective development, integration, and governance of these enablers typically occur within dense institutional ecosystems comprising research institutions, procurement regimes, capital markets, regulatory frameworks, and, increasingly, transnational digital and AI infrastructures.

1. Digital Assets

The core digital assets that enable innovation, services, and decision-making.

- **Data** sovereign access, governance, quality, and secure sharing
- **Software & AI models** domestic ecosystems, open source, and model development

2. Foundational Infrastructure

The resilient physical and digital infrastructure that underpins all critical services.

- **Compute** accelerators, data centres, HPC, and cloud services
- **Hardware** GPUs, servers, storage, and advanced manufacturing capability
- **Connectivity** high-performance networks, broadband, and global interconnection
- **Energy & power** reliable, affordable, and sustainable energy for digital infrastructure

3. Productive Capacity

The economic, industrial, and human capabilities that drive innovation and long-term value creation.

- **Skilled human capital** education, research, talent development, and lifelong learning
- **Access to capital & financing ecosystems** mobilize public and private capital to fund AI innovation, infrastructure, and scale-up
- **Industrial & supply chain capabilities** domestic capacity for semiconductors, critical components, and essential minerals

4. Safety and Security

The protection, governance, and standards that earn trust, stability, and responsible AI.

- **Risk-based regulatory frameworks** proportionate regulation, AI safety, ethics, accountability, and rights protection
- **Cybersecurity & resilience** protect systems, data, and services; build resilience and operational trust
- **Cognitive-informational resilience** information integrity to resist disinformation and manipulation
- **Technical standardization capacity** shape and adopt international standards to ensure interoperability and influence

Figure 2. The AI Sovereignty Stack — interdependent layers underpinning AI systems.
Source: adapted from [7,8,10,12]

To speak of "sovereignty" in this domain is therefore to ask a more difficult question: who is in a position to understand, govern, shape and benefit from these systems, and on what terms?

From the state perspective, three elements recur in that inquiry, as discussed below:

01 First, the structure, maturity, and strategic orientation of national innovation systems.

02 Second, the capacity of the state to direct or at least discipline technological development and avoid abusive behaviors, including by promoting the development of alternative options to dominant systems to avoid lockin.

03 Third – this is where much of the contemporary debates focus – the pronounced concentration of AI capabilities in a small number of dominant firms in few jurisdictions, raising important questions regarding technological dependency, market power, concentration of compute and data resources, and the distribution of innovation rents [60].

These are not separate issues. They interact – reinforcing one another where capability already exists, and compounding disadvantage where it does not — often constraining developing and late-industrializing economies more severely than the literature tends to acknowledge, particularly where these economies are attempting to build meaningful digital and AI capabilities within an increasingly concentrated global technological landscape.

The innovation economics literature has long emphasized coordination i.e., public institutions, industrial policy, and private firms do not operate independently [17,45,53]. What has changed in the AI era is the unprecedented concentration of control over critical enablers of technology – including hyperscale cloud infrastructure, advanced semiconductors, compute resources, frontier AI models, software ecosystems, and large-scale data infrastructures – in the hands of a limited number of corporations and economies [19,74].

Such a situation complicates any straightforward account of technological catch-up and, by extension, any credible claim to build AI sovereignty, as access to advanced AI capabilities increasingly depends on infrastructure and resources that are extraordinarily capital-intensive, geopolitically sensitive, and controlled by a narrow group of actors.[44,45]

Consequently, any credible discussion of digital or AI sovereignty must move beyond simplistic notions of self-sufficiency and instead engage with the structural realities of technological interdependence, concentration, and asymmetrical power within the contemporary digital economy.

Three interlocking constraints on AI sovereignty

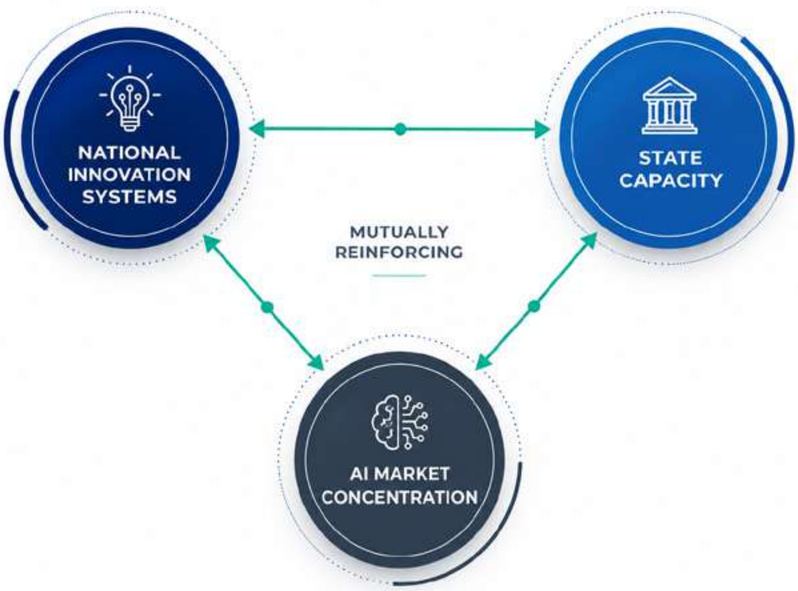


Figure 3. Three interlocking constraints on AI sovereignty: national innovation systems, state capacity and AI-market concentration.

2.1 National Innovation Systems and Technological Catch-Up

The language of "innovation systems" is sometimes treated as descriptive, whereas it may be more accurately understood as diagnostic. This helps explain why some states repeatedly generate technological capacity while others remain structurally dependent.

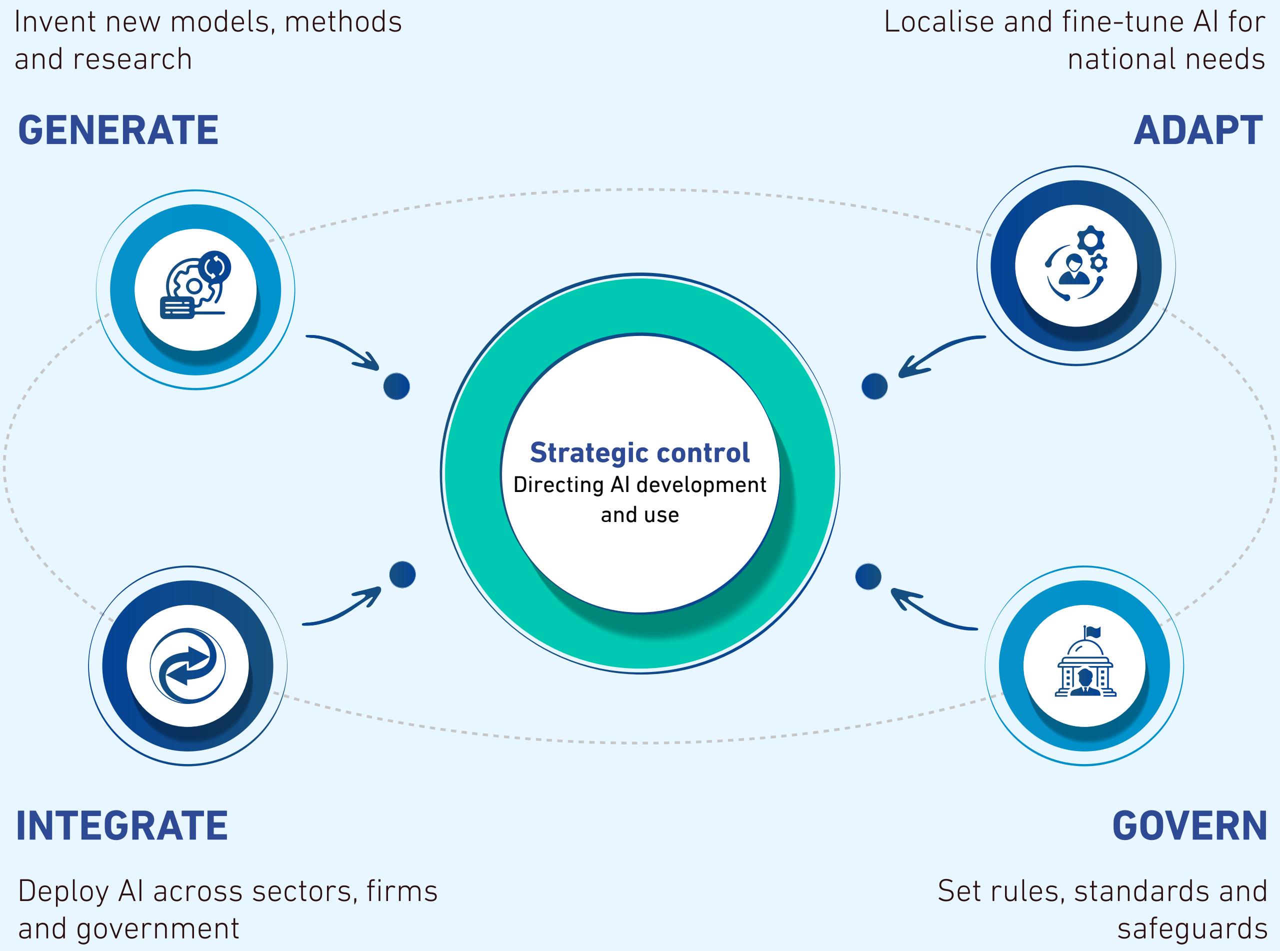
A conventional understanding of innovation from economics or innovation studies describes it as the introduction and diffusion of new products, processes, organizational forms, or services that create value.[33,60] From an AI sovereignty perspective, this understanding must be expanded to account not only for the creation of new technologies, but also for the institutional capacity to adapt, deploy, govern, and retain meaningful control over AI systems.

A national AI innovation system can therefore be understood as the configuration of institutions, infrastructures, actors, capabilities, and governance arrangements through which a state or society generates, absorbs, adapts, deploys, and governs AI-related knowledge and technologies. Its effectiveness depends not only on innovative performance, but also on the capacity to manage critical technological dependencies in ways that preserve strategic autonomy and resilience.

This definition intentionally expands innovation beyond invention. A country may possess a meaningful AI innovation system even when it does not develop frontier models itself, provided it can adapt, integrate, govern, and strategically control AI systems in ways that serve its national priorities. Innovation, in this sense, is cumulative and institutional [17].

It depends on durable linkages between universities and industry, between public finance and private risk-taking, and between regulatory stability and experimentation. Where those linkages are thin or episodic, technological development tends to be imported rather than produced [57].

An AI innovation system spans more than invention



A country can be innovative by adapting, integrating, governing and controlling AI it does not itself invent

Figure 4. An AI innovation system spans more than invention — from generation to adaptation, integration, governance and strategic control.

The significance of this definition becomes clear when distinguishing between the adoption of AI tools and the development of endogenous AI capabilities. It is one thing to adopt machine learning tools and generative AI systems; it is quite another to develop the underlying capabilities – data governance frameworks, computational infrastructure, and specialized talent pipelines, and research ecosystems – that make such tools endogenous to the economy. Many states are currently scrambling to do the former. Far fewer achieve the latter.

The catch-up literature offers a measure of optimism, but it should be read carefully. The current AI development presents highly concentrated dynamics, yet literature highlights that within the emergence of any technology, windows of opportunity exist, especially during periods of technological transition, and when States develop well-informed policies [44,45].

However, such windows do not remain open for long, and they are rarely accessible without prior institutional depth. In AI, the entry costs – especially in terms of compute, data, talent and, increasingly, energy [2,7] – are unusually high.

For that reason, the legitimate ambition of "autonomy" requires adjustment. Most states will not be able, nor need to, replicate the full AI stack.

A more plausible strategy lies in selective integration, developing capabilities in specific segments while relying on multiple external products and services elsewhere.

For instance, a medium-sized state may aspire to develop domestic AI capabilities but lack the financial and technical resources to build and maintain frontier-scale cloud infrastructure comparable to the largest hyperscalers.

Rather than pursuing complete self-sufficiency, it may invest in national research centers, AI expertise oriented towards national strategic sectors, and strategic applications, while obtaining compute resources through regional supercomputing facilities or diversified partnerships with multiple cloud providers. In this case, autonomy derives not from owning the entire AI stack, but from avoiding dependence on a single external supplier and retaining the capacity to direct AI development toward national priorities. **Cooperation therefore enhances rather than diminishes sovereignty.**

Openness and cooperation are therefore not alternatives to autonomy, but conditions for exercising it under contemporary technological conditions. The fundamental rationale underpinning **cooperative digital sovereignty** is that technological autonomy must be negotiated within interdependence, not achieved outside of it.

2.2 Mission-Oriented Innovation

If innovation systems set the stage, state capacity helps determine whether meaningful technological development can take place within them. The notion of the entrepreneurial state is often invoked with enthusiasm but limited precision. Properly understood, it is not a blanket endorsement of state intervention, but rather an analytical account of how certain governments have, under specific historical and institutional conditions, been able to absorb risk, coordinate stakeholders, and sustain long-term technological investments that private capital alone may have been unwilling or unable to undertake [53].

The pursuit of digital and AI sovereignty presents precisely this kind of problem [12]. The development of advanced AI models, semiconductor ecosystems, compute infrastructures, and large-scale data systems requires long investment horizons, substantial financial resources, and high tolerance for uncertainty, often extending beyond conventional market incentives. In such contexts, the state is not merely a regulator at the margins. It becomes, whether deliberately or not, a central participant acting as an essential coordinator of public action, addressing complex technological challenges [27,46].

Mission-oriented policy offers one way to structure this role. However, caution is warranted, as policy ambition does not automatically translate into implementation capacity. Not every state can successfully define and carry out such missions. Doing so requires administrative capacity, political continuity, policy coherence, financial resources, and sufficient insulation from short-term pressures [30]. These conditions, however, remain unevenly distributed across countries.

More to the point, missions require exclusion. To prioritize is to forego. This dimension is often underemphasized in contemporary policy discourse. It is not enough to declare AI a strategic sector. AI is not monolithic but encompasses a large spectrum of highly heterogeneous and complex systems. Governments must first assess their strengths and weaknesses across each of what the next section calls the **"Key AI Sovereignty Enablers"** [6,9,11], and subsequently decide which capabilities are attainable, which dependencies are tolerable, which applications matter the most, and what contingency measures must be required and adopted. Such decisions are not purely technical; they are inherently strategic, economic, and political.

Seen in this light, **AI sovereignty is less about control in the abstract and more about disciplined selectivity.** While sovereign states must recognize the necessity of a systemic approach to evaluate the multifaceted nature of the issue, attempts to simultaneously control all layers of the AI stack without clear prioritization may ultimately dilute resources, weaken implementation capacity, and undermine the objective of achieving meaningful technological agency.

2.3 Structural Concentration in the Global AI Economy

The preceding discussion might suggest that sufficient coordination and policy design could overcome most constraints. Such a conclusion, however, would risk underestimating the scale and advanced stage of concentration characterizing the contemporary AI economy. Indeed, the global AI economy is not simply competitive; it is structurally concentrated [60,74]. As stated earlier, a relatively small number of large technology corporations dominate key segments of the AI value chain spanning form training of AI models to distribution of AI services, including cloud computing infrastructure, advanced semiconductor production, large-scale data infrastructures, the development and deployment of frontier AI models, and increasingly, compute-intensive AI services and platforms.[1]

Layer	Who Dominates — And Why It Concentrates	Concentration Intensity
AI applications consumer-facing software	ChatGPT and other consumer apps. A thriving market — but vertically integrated firms can self-preference their own apps.	Moderate
AI models the "brains" of AI	A few firms with control over training data and compute dominate; vertical integration raises barriers for smaller developers.	High
Cloud infrastructure compute, servers, datacentres	AWS, Microsoft Azure and Google Cloud — an oligopoly with high switching costs, lock-in and minimal interoperability.	High
Microprocessing hardware chips & fabrication	Nvidia holds >80% of the AI chip market; TSMC leads fabrication and ASML the tooling. Very high entry barriers.	Very high

Figure 5. Structural concentration across the AI stack. Source: adapted from Washington Center for Equitable Growth, The AI Technology Stack (2025).

This is not an incidental feature of the market. It is the result of cumulative advantages, related to scale, network effects, and privileged access to capital, all of which are exceptionally difficult to reproduce [60].

Cloud infrastructure provides one of the clearest illustrations of this concentration [69]. Governments, businesses, and research institutions across the world now rely, often by necessity rather than deliberate choice, on a small number of providers headquartered abroad. This is not merely a procurement issue. It raises more fundamental concerns regarding technological dependency, jurisdictional exposure, resilience, cybersecurity, and the location of effective control over critical digital and AI functions.

What complicates matters further is the increasing integration of activities within a small number of platform ecosystems – not only vertical integration along a single value chain, but horizontal diversification and integration across many, producing ecosystem-wide economies of scale and scope. The same firms that provide infrastructure also develop models, capture data, and deliver services [1].

Google illustrates this trend well: it owns custom chips and cloud infrastructure, develops AI models such as Gemini, and distributes them through search and Android, creating a closed loop between compute, data, model training, and user-facing services.

As a result, entry points for new actors become progressively narrower. For technologically dependent countries, the problem is not simply catching up; it is finding a place to enter at all. These dynamics align with what has been described as intellectual monopoly capitalism [60].

As intellectual-monopoly firms, these actors extend their positions across multiple value chains simultaneously; vertical control is only one facet of a broader ecosystem dominance. Control over intangible assets, such as data, algorithms, proprietary architectures, and software ecosystems, translates directly into economic and political leverage.

The distributional consequences of such concentration are already becoming visible, particularly in relation to innovation capacity, bargaining power, access to compute resources, and the ability of states to shape domestic technological trajectories through national policy.

Under these conditions, **AI sovereignty cannot be reduced to domestic capability-building. It must also confront the structure of the global market itself, through competition law, regulatory intervention, strategic diversification, trusted international partnerships and innovative forms of international cooperation and coordination,** as proposed by this study's definition of cooperative digital sovereignty. Whether such efforts will succeed, however, is an open question. Conspicuously, success also depends on the availability of open technology for latecomers to leverage and learn from. In this perspective, open-weight models, while typically not categorizable open-source, lower inference costs, and shared tooling that reduce the cost of entry.

Multilateral platforms such as the Digital Cooperation Organization (DCO) may play an important role in facilitating dialogue, promoting interoperable governance approaches, and supporting cooperative pathways toward greater technological resilience and strategic autonomy.

2.4 Policy Implications

It is tempting to treat innovation systems, state capacity, and market concentration as distinct analytical categories. As highlighted above, in practice, they operate as a single constraint. A state may possess a reasonably developed research base and still lack the administrative coherence to mobilize it. Another may exhibit strong policy ambition but remain dependent on external infrastructures it cannot realistically replace. In both cases, concentration at the global level narrows the space for maneuvering.

This is why the language of sovereignty must be used with care. It does not denote independence. It describes a position –sometimes precarious – within a layered and asymmetrical system.

For emerging economies, the margin for error is thin. Strategies will necessarily be hybrid: partial domestic development, selective reliance on external providers, and, where possible, multilateral and regional collaboration.

What follows from this is less a program than a set of constraints.

01 First investments in "AI" or, more broadly, in digital transformation that are not anchored in an integrated approach – jointly leveraging education, research capacity, normative and institutional upgrade, and industrial organization – will have limited effect. The history of technological development offers little support for shortcuts.

02 Second state capacity remains the decisive variable, though it is often the least discussed. Without administrative competence and strategic discipline, even well-funded initiatives tend to dissipate.

03 Finally and perhaps most uncomfortably, the concentration of the AI economy cannot be treated as an externality. It is a structuring condition. Furthermore, such market reality must be seen within a highly conflictual and volatile geopolitical scenario.

Any serious account of AI sovereignty must grapple with such conditions directly, whether through domestic regulation, collective action, or some combination of both.

These constraints are precisely what cooperative digital sovereignty is designed to address: not by escaping interdependence, but by organizing it so that concentration is countered collectively rather than endured individually.

3. Key AI Sovereignty Enablers

What follows from the preceding discussion is that **AI sovereignty should not be understood as a singular capability, but rather as the outcome of a complex ecosystem of interdependent enablers spanning technological, economic, institutional, infrastructural, regulatory, and geopolitical dimensions.**

Thus, the ability of states and societies to meaningfully shape the development, deployment, and governance of AI systems depends not only on access to individual technological components, but also on the interaction between multiple enabling conditions that collectively determine technological agency, resilience, and strategic autonomy.

Importantly, as mentioned above, these enablers should not be interpreted as requiring complete national self-sufficiency across all dimensions of the AI stack. In many cases, effective AI sovereignty may instead depend on the ability to develop selected domestic capabilities while simultaneously leveraging trusted international partnerships, interoperable governance frameworks, and cooperative infrastructure arrangements.

Recent research on digital and AI sovereignty identifies several key elements that determine a country's capacity to develop and govern AI systems.

Belli [7,8,10,12] proposes a framework identifying eight core enablers of AI sovereignty:

01 Data resources and data governance frameworks;

02 Software ecosystems, AI models, and open-source capabilities;

03 Compute and hardware infrastructure, including advanced semiconductors and cloud infrastructure;

04 Meaningful connectivity;

05 Energy availability and resilient power infrastructure;

06 Skilled human capital, research capacity, and advanced scientific ecosystems;

07 Cybersecurity and cyber-resilience capabilities; and

08 Risk-based regulatory and governance frameworks.

The original version of this framework was subsequently expanded by Belli et al. [10] to include an additional enabler:

09 Cognitive-informational resilience.

Building on this framework, the present study further incorporates additional enabling dimensions that are particularly relevant to the cooperative and systemic understanding of digital and AI sovereignty advanced in this report:

10 Access to capital and financing ecosystems, particularly given the extraordinary capital intensity associated with advanced AI development and infrastructure;

11 Industrial and supply chain capabilities, particularly in relation to semiconductors and critical components, including minerals; and

12 Technical standardization capacity, especially as regards interoperability.

3.1 Data

As mentioned above, to facilitate the comprehension and organization of the technology stack, these enablers can be grouped into four macro-categories:

01 Digital Assets, which includes data; software & AI models;

02 Foundational infrastructure, with include compute, hardware, connectivity energy and power;

03 Productive capacity, which includes skilled human capital, capital and financing, and supply chain capabilities;

04 and Safety and security, which include risk-based frameworks, cybersecurity and resilience, cognitive-informational resilience and technical standardization.

The expanded version of the Key AI Sovereignty Enabler (KASE) [6,9,11] framework is briefly presented in the following subsections.

Being able to construct solid **data sovereignty,** defined as **"the capacity to understand how and why (personal) data are processed, and by whom; develop data processing capabilities; and effectively regulate data processing; thus retaining self-determination and control"** [12], is an essential component of AI sovereignty.

Particularly, being able to have access to high-quality, diverse, representative, secure, and lawfully sourced data is fundamental for training, finetuning, validating, and improving AI systems.

Sovereignty over data allows states to protect fundamental rights such as privacy and informational self-determination, ensure data security, and regulate the use of sensitive information, thereby maintaining control over the development of AI systems to reflect their cultural and societal norms rather than being regulated or controlled through such systems.

Importantly, effective data governance frameworks can also facilitate trusted cross-border data flows, interoperability, and lawful international cooperation in AI development.

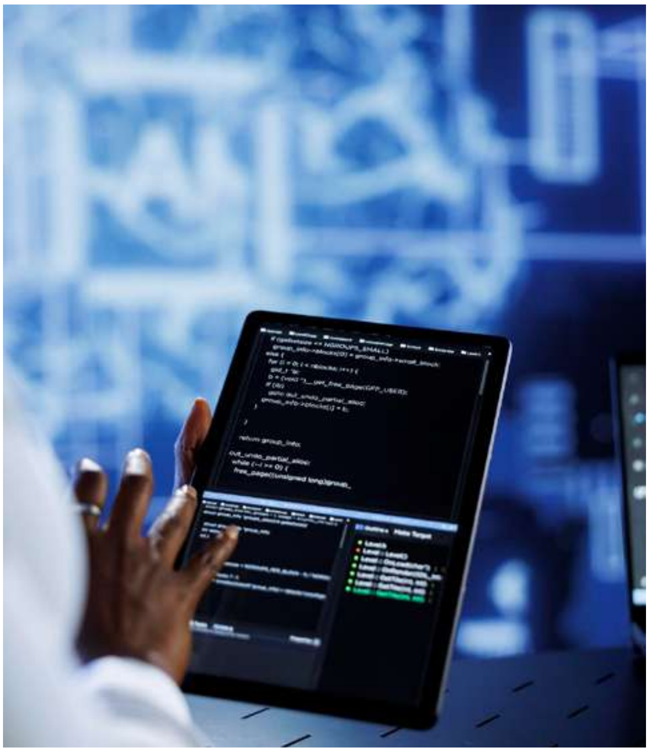
3.2 Software Ecosystems, AI Models & Open-Source Capabilities

Software ecosystems, AI models, and increasingly foundation and frontier models constitute the operational core of AI systems, enabling machines to perform tasks and make decisions. Sovereignty at this layer is not primarily a question of whether a country can build frontier models, a task that is prohibitive for most technologically dependent countries, but of whether it can choose, adapt, inspect, and govern the models it depends on. Importantly, algorithm development, deployment, regulation, auditing, and governance are all equally important dimensions of algorithmic governance where algorithmic models can be both the subject and facilitator of regulation [42].

By investing in algorithmic research and development (R&D), open-source ecosystems, and crafting sound policies and regulations, nations can develop cutting-edge algorithms that enable more accurate, efficient, adaptable, secure, and interoperable AI systems.

Importantly, for most states, replicating the frontier is neither feasible nor required. The dependency risk lies in building public services and critical functions on top of closed foreign models whose weights, training data, update cycles, safety filters, and terms of access are set by foreign actors and can be changed, priced, or withdrawn at any moment.

A state that cannot inspect, modify, or substitute the model beneath its services exercises little sovereignty over that layer, however capable the model. For this reason, open-weight and open-source foundation models should be seen as critical levers for non-frontier states: they allow both public and private actors to run, audit, fine-tune, and domesticate capable models on its own infrastructure and in its own languages, without having to build a frontier model of its own.



Furthermore, R&D in algorithmic models allows nations to tailor AI technologies to their specific needs and values, ensuring that AI systems align with their cultural and legal frameworks. This is particularly important in domains such as healthcare, finance, and public policy, where the responsible and fair use of AI is paramount.

By investing in R&D, nations can develop algorithms and AI models that are transparent, explainable, and accountable, thereby building public trust and facilitating the sustainable adoption of AI technologies.

3.3 Compute, Semiconductors and Hardware Infrastructure

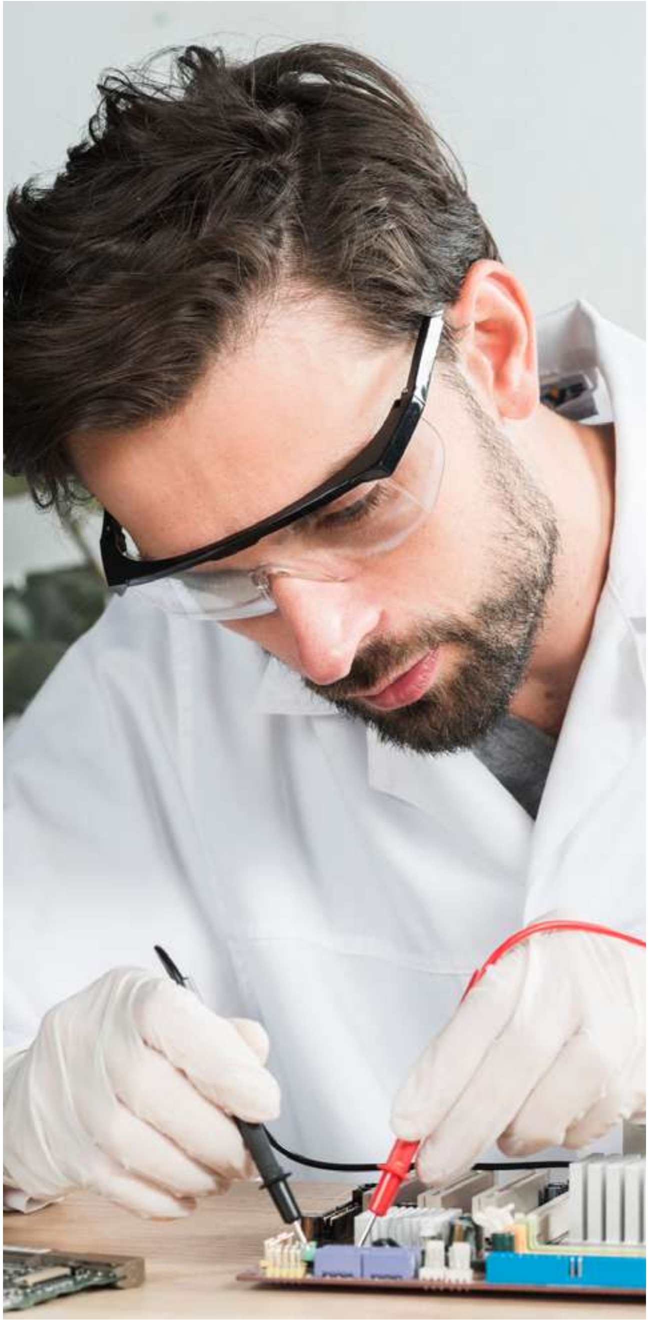
Training complex AI models and processing large datasets require substantial computational resources and sophisticated hardware infrastructure. In particular, frontier AI systems and generative AI models are remarkably compute-intensive due to their scale and complexity.

Global cloud computing capacity remains highly concentrated among a small number of hyperscale providers, with Amazon Web Services, Microsoft Azure, and Google Cloud collectively controlling a significant share of the global cloud infrastructure market [59].

Among the enablers of AI sovereignty, access to compute — together with the advanced semiconductors, data-center capacity, cloud infrastructure, and energy resources that support it — has become one of the most decisive bottlenecks for frontier AI development, warranting its treatment as a distinct strategic priority within this framework.

At the same time, advanced semiconductor production is concentrated within a limited number of firms and jurisdictions, creating additional supply chain vulnerabilities and geopolitical dependencies. Ensuring access to sufficient compute capacity, cloud infrastructure, advanced semiconductors, data center capacity, and high-performance computing systems is therefore critical for AI sovereignty.

By investing in domestic and regional compute infrastructure, adopting safeguards against excessive market concentration, and promoting competition, nations can mitigate external dependencies, strengthen resilience, accelerate AI research and innovation, and foster the growth of local AI ecosystems [69]



3.4 Meaningful Connectivity

Reliable, well-performing, universally accessible, and affordable connectivity infrastructure is essential for the development, deployment and operation of AI systems. **Meaningful connectivity requires not only infrastructure availability, but also non-discriminatory access to the open internet, and digital services.**

Practices such as "zero-rating" plans [3], which are common in many developing countries, may influence how users access digital services by privileging specific applications or platforms over others.

In some contexts, for example, in Brazil, concerns have been raised that such practices could limit users' exposure to the broader internet ecosystem, artificially concentrating user attention into zero-rated services, and potentially constraining opportunities for local innovation and competition [3,5]. Different jurisdictions have adopted different regulatory approaches to this matter.

For example, India's prohibition of zero-rating practices has played an essential role to preserve an open and competitive digital environment and enabling the broader digital-transformation success that was made possible by Digital Public Infrastructure (DPIs) such as UPI and Aadhaar.

Ensuring meaningful connectivity therefore entails preserving open, reliable and inclusive access conditions that enable broad participation in digital ecosystems, which in turn can support the development, diffusion, and autonomous governance of AI technologies.

At the cooperative level, this can be advanced through regional interconnection such as shared internet-exchange points, and submarine and terrestrial cable infrastructure, that lower costs and reduce dependence on distant hubs.

3.5 Energy Availability and Power Infrastructure

AI systems require substantial amounts of energy to train, deploy, and operate, making access to reliable, resilient and sustainable energy infrastructure a critical enabler of AI sovereignty.

As AI models increase in size and complexity, demand for electricity, cooling systems, and data center infrastructure grows significantly.

Ensuring stable and affordable access to energy and regulating it in a way that sustainably balance human and AI energy needs is therefore essential for maintaining uninterrupted AI operations while preserving the smooth functioning of domestic energy markets.

In this perspective, the environmental implications of large-scale AI systems are becoming increasingly significant.

Investment in resilient power infrastructure, renewable energy systems, and sustainable energy strategies have become essential to support AI development while reducing environmental impact, enhancing energy security, and improving the long-term sustainability of AI-driven economic growth.

Additionally, regional cooperation on energy connectivity, cross-border electricity infrastructure, and integrated power markets may also become strategically important for AI sovereignty while preserving sustainability, particularly by enabling countries with limited domestic energy resources to leverage reliable and sustainable energy supplies from energy-abundant partners.

3.6 Skilled Human Resources, Research Capacity, and Scientific Ecosystems

Enhancing the digital and AI literacy of the population through education, capacity building, research investment, and multigenerational training is essential not only for developing a skilled AI workforce but also for strengthening innovation capabilities, cybersecurity, and long-term technological autonomy.

Developing, attracting, and retaining highly skilled talent capable of designing, building, deploying, auditing and regulating AI systems is particularly crucial in an increasingly knowledge-intensive global economy.

Importantly, AI sovereignty depends not only on workforce availability, but also on the existence of robust scientific and research ecosystems, including universities, laboratories, innovation hubs, and interdisciplinary research networks.

AI literacy should also include critical understanding of AI's societal implications, including risks related to overdependence on AI systems, deskilling, labor displacement, cognitive manipulation, misinformation, and social fragmentation, all of which may require broader societal and policy responses.

At the cooperative level, this can be strengthened through international research networks, talent-mobility programs, and shared research ecosystems, amongst other scientific cooperation initiatives.

3.7 Cybersecurity and Cyber-Resilience Capabilities

The importance of cybersecurity cannot be overstated. AI systems, like other digital systems, remain vulnerable to cybersecurity threats and may themselves be exploited or turned to hostile use to conduct cyber-attacks, fraud, surveillance, data breaches, or automated malicious operations [36,51].

While AI can be leveraged to strengthen cyber defences and improve threat detection capabilities, it may also enable cybercriminals and hostile actors to launch targeted attacks at an unprecedented speed and scale, bypass traditional detection mechanisms, automate vulnerability discovery, and intensify the sophistication of cyber crimes [8,10].

As AI systems become increasingly integrated into critical infrastructure and public services, ensuring their resilience, security, and reliability becomes paramount.

Robust cybersecurity and cyber-resilience measures can help protect AI assets, maintain public trust, ensure operational continuity, and prevent the misuse or compromise of AI technologies for malicious purposes.

Importantly, cybersecurity and resilience capabilities are fundamental components of AI sovereignty, as excessive dependence on external providers for critical security functions, cloud protection, or incident response mechanisms may create strategic vulnerabilities and reduce countries' ability to exercise effective control over their digital and AI ecosystems.

National cyber-resilience planning and digital risk-management frameworks are therefore necessary not only to secure AI systems, but also to ensure the continuity, reliability, recoverability, and strategic autonomy of critical AI-enabled infrastructures and services. At the cooperative level, this includes cross-border threat-intelligence sharing, especially with trusted partners, joint incident-response arrangements, and common security standards across states.

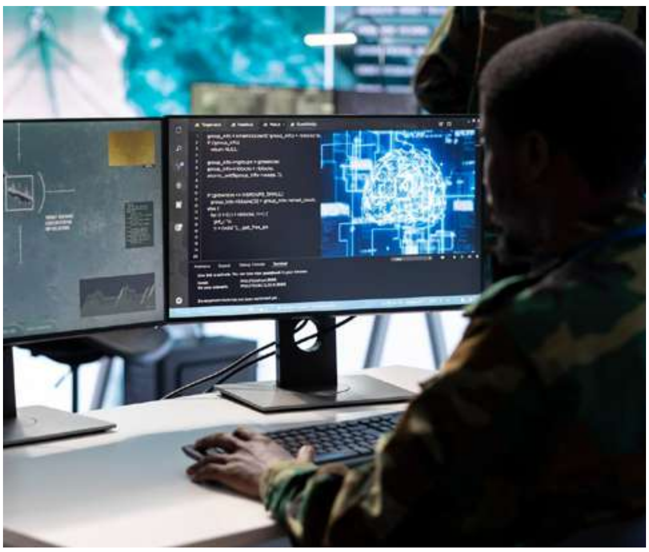
3.8 Risk-Based Regulatory and Governance Frameworks

Comprehensive governance frameworks capable of addressing AI-related risks [60] including regulatory measures, data protection regimes, accountability mechanisms, fundamental-rights safeguards, and risk-management tools is an essential component of AI sovereignty.

However, risk-based regulation alone is insufficient in addressing the broader societal, economic, and geopolitical implications of AI. Consequently, effective governance frameworks must provide the institutional capabilities necessary to operationalize transparency, accountability, interoperability, human rights protections, competition, innovation, and international cooperation.

Managing the legal, ethical, economic, and societal implications of AI is essential for maintaining public trust and ensuring the responsible development and deployment of AI systems.

By establishing clear, adaptable, and interoperable regulatory frameworks, nations can mitigate risks while harnessing AI in ways that align with their values, developmental priorities, and strategic objectives.



3.9 Cognitive-Informational Resilience

The capacity to detect, understand and respond to disproportionate and asymmetrical interference by foreign corporations, governments, or coordinated influence operators in public discourse and policymaking processes is becoming an increasingly important element of AI sovereignty [9,15,28].

This is particularly relevant where such influence seeks to shape narratives around digital and AI policy, undermine trust in sovereign infrastructure initiatives, or constrain national decision-making on critical technological choices. AI systems can amplify disinformation, manipulate narratives, influence public opinion, and shape cognitive environments with unprecedented scale and precision.

This concern becomes particularly salient in an AI scenario where some of the largest AI companies may have significant economic and political interests in shaping AI-related narratives and influencing national policy decisions, infrastructure choices, and governance frameworks.

Cognitive-informational resilience therefore includes the ability to safeguard public decision-making processes, maintain informational integrity, strengthen media and AI literacy, counter manipulative influence operations, and preserve societal capacity for informed and autonomous decision-making.

In furtherance of this objective, measures aimed at strengthening cognitive-informational resilience should be designed and implemented in a manner consistent with applicable international human rights obligations, including respect for freedom of expression, access to information, and due process guarantees.

This concern becomes particularly salient in an AI scenario where some of the largest AI companies may have significant economic and political interests in shaping AI-related narratives and influencing national policy decisions, infrastructure choices, and governance frameworks.

Cognitive-informational resilience therefore includes the ability to safeguard public decision-making processes, maintain informational integrity, strengthen media and AI literacy, counter manipulative influence operations, and preserve societal capacity for informed and autonomous decision-making.

At the cooperative level, this includes shared detection of coordinated influence operations and collaborative media-literacy and fact-integrity initiatives.

3.10 Access to Capital and Financing Ecosystems

AI development may be highly capital-intensive, especially as regards the training of frontier models [38]. Access to long-term financing, venture capital ecosystems, public funding mechanisms, and strategic industrial investment therefore constitutes a critical enabler of AI sovereignty [67].

The development of advanced AI models, compute infrastructure, semiconductor ecosystems, and large-scale research initiatives requires substantial financial resources that may exceed the capacities of many domestic markets.

Countries lacking sufficient financing ecosystems may struggle to scale domestic innovation, retain talent, support AI-enabled enterprises, or compete in advanced technological sectors.

This may deepen dependency on external platforms, infrastructure providers, and foreign sources of capital, particularly where domestic firms are unable to access patient financing for high-risk, long-term technological development. Financial capacity is therefore not merely an economic enabler, but a strategic condition for sustaining domestic technological agency.

Public-private partnerships, sovereign investment mechanisms, development financing, blended finance instruments, and regional cooperation frameworks can therefore play an important role in strengthening technological capacity and supporting sustainable AI ecosystems.

For emerging and middle-income economies in particular, cooperative financing models may help pool resources, de-risk strategic infrastructure investments, and expand access to capital-intensive AI capabilities while preserving policy flexibility and strategic autonomy.

3.11 Industrial and Supply Chain Capabilities

AI systems depend on highly complex global supply chains involving semiconductors, rare earth minerals, networking equipment, cloud infrastructure, manufacturing capacity, advanced packaging and specialized hardware components [73].

Concentration or disruption within these supply chains may generate significant strategic vulnerabilities, particularly where countries depend on a narrow set of suppliers, jurisdictions, or logistics routes for critical inputs [39].

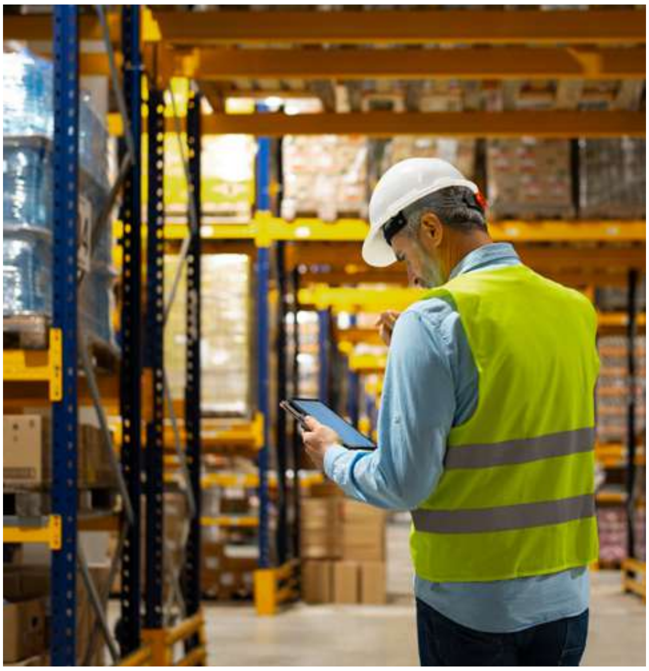
Industrial and supply-chain capabilities are therefore important enablers of AI sovereignty. Countries do not necessarily need to localize every layer of the AI supply chain, but they do need the capacity to understand critical dependencies, identify strategic bottlenecks, diversify sources of supply, and develop targeted industrial capabilities in areas of comparative or strategic advantage.

Developing industrial capabilities, diversifying supply chains, and strengthening trusted international partnerships therefore play an essential role in enhancing resilience, reducing excessive dependencies, and improving countries' ability to participate more effectively in the global AI economy [37].

However, for many countries, particularly emerging and middle-income economies, the most effective strategy is unlikely to consist in pursuing complete supply-chain self-sufficiency. Rather, it entails a dynamic process of strategic integration into global value chains, combining selective specialization, capability-building, trusted supplier diversification, and regional industrial cooperation.

Indeed, successful latecomer economies tend to follow an "in–out–in again" trajectory, whereby initial participation in global value chains is leveraged to acquire technological capabilities, followed by selective upgrading of domestic innovation and industrial capacities, and subsequent reintegration into global markets from higher value-added positions. [47]

From the perspective of AI sovereignty, this approach suggests that states should prioritize the development of strategic capabilities across critical segments of the AI value chain while relying on trusted international partnerships and regional cooperation to complement domestic strengths, thereby enhancing resilience without sacrificing the benefits of global technological interdependence.



3.12 Technical Standardization Capacity

The capacity to develop technical standards and meaningfully participate in international standardization processes are essential for ensuring that AI systems, digital infrastructures, governance frameworks, and cross-border data ecosystems can function effectively across jurisdictions and technological environments [18].

This makes standardization relevant to AI sovereignty because standards shape how AI systems are designed, evaluated, procured, connected, secured, and trusted across markets and jurisdictions.

The ability to shape, adopt, and participate in international standardization processes increasingly constitutes a strategic dimension of AI sovereignty.

Shared standards can support trusted cooperation, reduce fragmentation, enhance legal certainty, facilitate trade and innovation, and enable more inclusive participation in digital and AI ecosystems.

In particular, in the absence of binding international treaties on AI governance, global standards bodies such as ISO and ITU play an important role in establishing an essential "institutional and technical infrastructure" that diffuses best practices across borders, prevents regulatory races to the bottom, and creates the unified technical vocabulary necessary to secure transnational trust [19].

3.13 The need for an integrated approach

As a result, the Key AI Sovereignty Enablers cannot be approached as discrete policy levers or technocratic checklists. Their significance lies precisely in their interdependence.

Governance frameworks, regulatory choices, industrial policy instruments, infrastructure investments, international cooperation mechanisms, and capacity building efforts in each of the abovementioned enablers do not operate in isolation. Rather, they collectively shape the conditions under which AI capabilities can be understood, developed, deployed, governed, and contested.

While strategic prioritization is necessary, fragmentation should be avoided. A fragmented or excessively siloed approach – still visible in many national digital and AI strategies failing to consider the interconnectedness of abovementioned enablers – risks jeopardizing the effective use of resources and reinforcing technological dependency rather than mitigating it.

At the same time, it is important to acknowledge that very few countries are likely to possess the resources or structural conditions necessary to develop all enablers domestically and simultaneously.

This reality reinforces the importance of cooperative approaches to AI sovereignty, including trusted cross-border partnerships, interoperable governance frameworks, regional infrastructure cooperation, shared research ecosystems, and coordinated resilience mechanisms.

Accordingly, the more difficult – yet more consequential – task is to articulate a systemic vision in which each enabler is calibrated against the others, while taking into account domestic institutional realities, development priorities, and the structural asymmetries characterizing the global AI economy.

Such an approach inevitably entails trade-offs. Pursuing autonomy in certain layers of the AI stack may require openness in others; fostering domestic capacity may depend on selective integration with external infrastructures. The challenge, then, is not to resolve these tensions once and for all, but to govern them deliberately.

It is precisely this integrated and strategic approach, grounded in realism rather than technological maximalism, that informs the analytical framework developed in Section 5.

4. Open Source and Digital Public Infrastructure: Leveraging Openness Strategically

Over the past three decades, both large technology conglomerates and nation-states have strategically leveraged open-source software to strengthen their digital sovereignty, reduce technological dependencies, foster innovation, and improve their strategic positioning within digital markets [10,52].

Unlike the enablers cataloged in Section 3, openness is not itself an enabler but a cross-cutting strategy that can be applied across several of them, data, models, compute, and standards alike. Its promise and its limits therefore recur throughout the stack.

Global technology companies such as IBM, through its long-standing support for the Linux ecosystem, and Alphabet, through the Android operating system, illustrate how open-source components can be strategically leveraged within broader commercial ecosystems, including through their integration into proprietary technology stacks to create dominant, yet paradoxically open, digital platforms.

More recently, Meta's release of Llama, the growing adoption of open AI frameworks such as PyTorch, and the emergence of open-weight models such as DeepSeek have significantly contributed to reshaping innovation dynamics in AI by expanding collaborative development models across selected Key AI Sovereignty Enablers (KASEs).

In this context, open-source ecosystems and Digital Public Infrastructures (DPIs) emerge not only as technological choices, but also as strategic instruments through which states and organizations may seek to mitigate concentration risks, reduce dependencies, expand participation in digital and AI ecosystems, and strengthen technological agency within conditions of interdependence.

This trend also extends into the physical layer through the adoption of open hardware architectures like RISC-V and the development of open Electronic Design Automation (EDA) tools, both of which seek to reduce dependency on traditional highly concentrated semiconductor ecosystems. In this context, countries like China, India, South Korea, and to a lesser extent Brazil, have incorporated open-source technologies and open digital ecosystems into their national industrial and technological strategies aimed at strengthening domestic innovation capacity, reducing external dependencies, and enhancing technological autonomy.

At the same time, openness alone does not eliminate concentration dynamics. Many open-source ecosystems continue to depend on compute infrastructures, cloud services, and semiconductor supply chains controlled by a relatively small number of dominant actors. Likewise, open-weight AI models do not necessarily imply openness across the entire AI stack, particularly where training datasets, compute resources, orchestration layers, or deployment infrastructures remain proprietary or highly concentrated.

Expanding this logic to the public sector, governments have also recently leveraged open standards, interoperable protocols, and modular architectures to develop Digital Public Infrastructures (DPIs), to avoid excessive dependence on proprietary platforms or exclusive reliance on foreign technology providers for critical public service delivery. By building these essential societal "rails" – such as digital identity systems, payment infrastructures, and trusted data exchange layers – on interoperable, and in many cases, open standards, states are fostering more competitive and inclusive digital ecosystems while reducing certain forms of technological lock-in and dependency [54].

4.1. Leveraging Digital Public Infrastrucutre for Digital Sovereignty

DPIs are defined as **"a set of shared digital systems that are secure and interoperable, and can be built on open standards and specifications to deliver and provide equitable access to public and/or private services at societal scale"** [20,35]. Beyond mere technical tools, DPIs function as foundational "building blocks" that can support innovation, public service delivery, and broader digital transformation process.

Examples include India's Aadhaar and Unified Payments Interface (UPI), Brazil's Pix instant payment system, and the broader development of interoperable digital government architectures in countries such as Estonia and Singapore [5].

The Interoperable nature of the DPIs can help ensure that disparate platforms and services communicate effectively and seamlessly, thereby reducing barriers to entry, limiting certain forms of "vendor lock-in" and fostering greater competition and innovation [5].

Furthermore, by operating at societal scale, DPIs can lower entry barriers for startups and smaller firms, expand access to digital services, and strengthen governments' capacity to implement public policies in areas such as financial inclusion, healthcare, education, and digital service delivery.

From the perspective of cooperative digital sovereignty, DPIs and open digital ecosystems may provide mechanisms through which countries can strengthen domestic technological agency while preserving interoperability, trusted cooperation, and cross-border digital integration.

Empirical research examining the development of DPIs in countries such as India and Brazil suggests that, while not exempt from criticism or governance challenges, DPIs can foster inclusive digitalization, facilitate access to digital services, strengthen domestic technological ecosystems, and create enabling conditions for AI deployment and digital entrepreneurship [62]. In this regard, DPIs may enable interoperability and lower barriers to innovation, thus supporting technological autonomy at different layers of the AI stack.

At the same time, DPIs may also generate structural risks if their underlying technological dependencies are not carefully assessed. While DPIs are often conceptualized primarily as software-based infrastructures, their operation often depends on cloud computing services, data center infrastructure, semiconductors, and hardware ecosystems controlled by a relatively small number of dominant technology providers [62].

In practice, this may exacerbate concentration at the hardware layer and create additional vulnerabilities and external dependencies related to data hosting, compute availability, cybersecurity, and operational continuity.

These risks may become particularly significant in contexts where critical public digital infrastructures rely heavily on foreign cloud providers or externally controlled computational resources [59].

Consequently, while DPIs may strengthen digital governance and public service delivery, their implementation may simultaneously reinforce technological dependencies if countries lack sufficiently diversified, trusted, resilient, or domestically anchored access to underlying digital and AI infrastructure layers.

4.2 A Realistic Approach to Openness

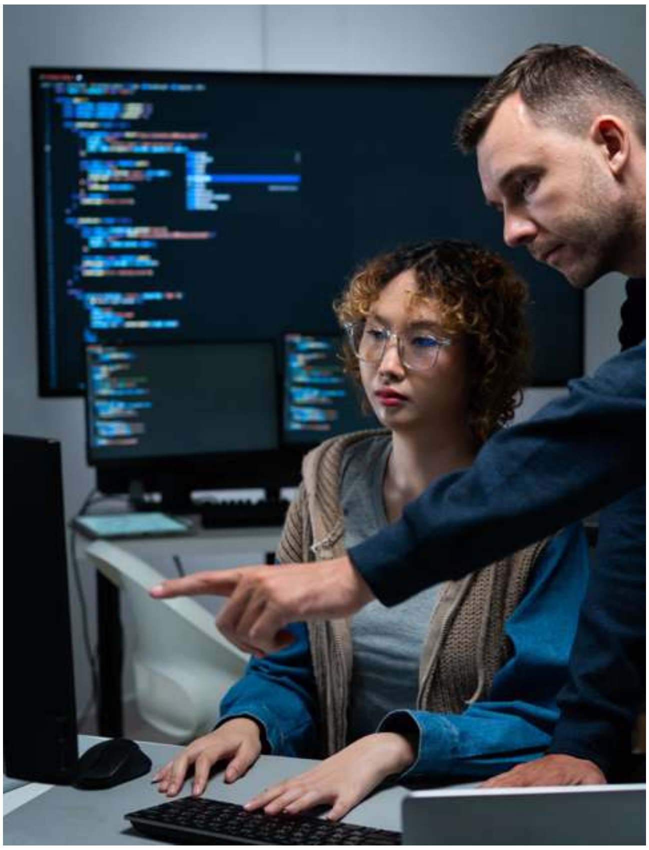
It would be a mistake to treat openness as inherently redistributive or automatically conducive to technological autonomy. Indeed, open-source ecosystems do not necessarily displace power; rather they often reorganize it [34,60].

The formal availability of source code or model weights, and the capacity to build upon them, reveal relatively little about who possesses the ability to set technical standards, who controls downstream integration, who shapes ecosystem governance, or who captures the economic value generated across the AI value chain.

In practice, the critical bottlenecks, such as compute infrastructure, advanced semiconductors, high-quality datasets, and deployment channels, may remain – and have frequently remained – highly concentrated. Openness, in other words, often operates unevenly across different layers of AI stack [10].

A similar consideration applies to the DPIs. When they are built around interoperable standards, modular architectures, and open protocols, they can indeed widen participation, facilitate innovation, and reduce certain forms of dependency on dominant digital platforms.

The more compelling examples, particularly in digital identity and payment systems, show how shared infrastructural layers can support both public administration and private innovation. However, these outcomes are contingent, not automatic [29].



The central challenge lies in the dependencies that may persist beneath apparently open systems. DPIs inevitably inherit many of the structural constraints of the environments in which they are deployed. Where they rely on external cloud providers, proprietary hardware, or foreign-controlled maintenance ecosystems, their contribution to digital sovereignty is, at best, partial [62].

In some cases, they simply relocate dependency on less visible layers of the technological stack. Although the architecture may be open, the underlying control remains externally concentrated.

A similar pattern can be observed in so-called open AI models [72]. Their proliferation has undoubtedly lowered the barriers to experimentation, and enabled universities, startups, researchers and even gave public agencies the ability to engage with AI capabilities that were, until recently, accessible only to a limited number of firms. That shift is significant and should not be dismissed. At the same time, it should not be overstated either.

The most consequential stages of AI development, such as large-scale training, data curation, hardware optimization, remain capital-intensive and highly concentrated. By the time many models are released in "open" form, substantial competitive and strategic advantages may have already been consolidated upstream.

This does not render openness irrelevant. On the contrary, it reinforces the importance of governing strategically. The question is therefore not whether open-source ecosystems and DPIs can contribute to digital and AI sovereignty – as they indubitably do – but rather under what governance, infrastructural, and institutional conditions such contributions become sustainable and meaningful.

Without broader strategies aimed at strengthening domestic capabilities, diversifying dependencies, developing trusted partnerships, and improving access to underlying infrastructure layers, openness risks becoming an aspirational goal resting on a relatively thin layer of accessibility superimposed upon structurally unequal technological ecosystems [58].

It may be tempting to frame contemporary technological governance debates as a binary choice between open and closed systems. In practice, however, such a dichotomy obscures more than it clarifies.

Contemporary AI ecosystems are rarely fully open or fully proprietary. They are hybrid arrangements, in which access, interoperability, and openness are granted selectively, while strategic control is retained over the layers that yield the greatest economic, technological, or geopolitical leverage [71].

Effective policymaking must therefore engage with this hybridity rather than relying on overly simplified distinctions.

The discussion above points in a consistent direction. **Under certain institutional, economic, and governance conditions, openness can support innovation, facilitate interoperability, and create opportunities for broader participation in digital and AI ecosystems. In other contexts, however, it may well redistribute advantages without fundamentally altering underlying hierarchies and structural asymmetries.** The difference often lies in the surrounding institutional and governance framework: who controls the infrastructure, who finances and sustains it, and who ultimately depends on it [10].

This returns us to the broader argument developed throughout this paper. Digital and AI sovereignty are unlikely to be secured through isolated technological interventions, however well intentioned. Rather, they depend on alignment between governance frameworks, industrial policy, infrastructure strategies, regulatory approaches, institutional capacity, and technological design choices.

Open-source ecosystems and DPIs have a considerable role to play as part of that alignment, particularly when integrated into broader approaches grounded in interoperability, resilience, and diversification, which this paper considers as contingent on cooperative digital sovereignty. On their own, however, they are unlikely to be sufficient.

5. DCO Framework for Cooperative Digital Sovereignty

The preceding sections have argued that digital and AI sovereignty cannot be meaningfully understood through simplistic notions of technological self-sufficiency, nor reduced to isolated policy interventions focused on individual sectors or technologies. Rather, cooperative digital sovereignty emerges from the interaction between multiple technological, institutional, economic, infrastructural, and governance dimensions that collectively determine a country's ability to shape, govern, secure, and strategically benefit from digital and AI systems.

At the same time, any strategy for strengthening AI sovereignty must confront the structural realities of contemporary AI development. Frontier capabilities are increasingly shaped by economies of scale, high capital intensity, concentrated compute infrastructures, access to advanced semiconductors, and cumulative advantages in data, talent, and platform ecosystems.

Under these conditions, few states are realistically positioned to replicate the full AI stack or compete directly with incumbent AI actors across all technological layers.

Efforts to pursue comprehensive technological self-sufficiency in the short-term risk dispersing limited resources across multiple domains without generating sufficient scale to establish meaningful capabilities.

The challenge is therefore not whether countries can reproduce existing models of technological concentration, but how they can develop sufficient agency to influence technological trajectories and reduce strategic dependence.

This suggests a different approach to sovereignty: one centered on selective capability development and coordinated interdependence. Rather than seeking full-stack control, states can identify strategic entry points within AI innovation systems – such as public data infrastructures, domain-specific models, model adaptation capacities, specialized compute resources, open technical standards, evaluation capabilities, or selected segments of the hardware value chain – and concentrate investment where durable capabilities and institutional leverage can emerge.

In many cases, achieving meaningful scale will require forms of cooperation that extend beyond traditional market integration, including shared infrastructures, coordinated industrial policy, joint procurement mechanisms, interoperable governance arrangements, and collaborative research ecosystems.

Such arrangements do not eliminate dependence but seek to organize it, transforming concentrated and potentially coercive dependencies into diversified and governable forms of interdependence that preserve strategic choice and reduce exposure to the exploitation of technological dependencies.

It is within this context that this study advances an analytical framework for Cooperative Digital Sovereignty. This analytical framework aims to support states seeking to strengthen domestic technological capabilities, institutional resilience, innovation ecosystems, and strategic autonomy while simultaneously leveraging trusted cooperation, interoperable governance mechanisms, shared infrastructures, and collaborative innovation arrangements. Rather than viewing sovereignty and cooperation as contradictory objectives, the framework treats them as mutually reinforcing dimensions of sustainable digital and AI governance.

The framework is structured around the previously identified twelve (12) Key AI Sovereignty Enablers (KASEs), which together form an interconnected ecosystem of technological and governance capacities.

Accordingly, this study acknowledges that international cooperation is an essential dimension of the construction of digital sovereignty, alongside other essential dimensions that typically retain a national remit, such as governance, regulation, industrial policy, and capacity building.

This consideration reflects the reality that, in highly interconnected AI ecosystems, meaningful digital and AI sovereignty increasingly depends both on the development of domestic capabilities and on countries' ability to participate in trusted, interoperable, and resilient forms of international cooperation.

In this framework, cooperation is therefore not treated as an essential instrument for constructing and sustaining digital sovereignty. Hence, cooperation is a means to sovereignty: it counts toward sovereignty only insofar as it builds domestic capability or secures the conditions for autonomous choice.

The framework therefore seeks to move beyond abstract or rhetorically expansive understandings of "AI sovereignty" by grounding the concept in institutional practice, infrastructural realities, governance capabilities, and cooperative mechanisms. Importantly, the effectiveness of the KASEs' operationalization relies on five interrelated dimensions of cooperative digital sovereignty: governance, regulation, industrial policy, capacity building, and international cooperation and interoperability.

None of these dimensions is sufficient on its own. Their effectiveness depends on whether they operate coherently and strategically across the broader technological ecosystem.

Before proceeding to the operational elements of the framework, a brief clarification of these dimensions is useful.

01

First, governance, in this context, extends beyond formal authority or state control. It refers to **the mechanisms through which diverse actors, such as governments, regulators, private firms, research institutions, technical communities, civil society organizations, and international partners, communicate, coordinate, cooperate, and align strategic priorities** [3]. Effective governance therefore depends not only on institutional authority, but also on the ability to effectively operationalize multistakeholder cooperation across increasingly complex technological ecosystems. This dimension also encompasses whole-of-government coordination, strategic foresight, and the long-term planning capacity required to translate policy ambition into implementation across the enablers.

02

Second, **regulation** should not be understood solely as a restrictive instrument. Rather, it encompasses **the broader set of legal, technical, contractual, and institutional tools through which states and societies shape technological development, rebalance asymmetrical market structures, protect rights, and create conditions for innovation and trust** [2]. Data protection regimes, cybersecurity frameworks, competition law, procurement policies, interoperability requirements, technical standards, liability regimes, and contractual governance mechanisms may all influence whether digital and AI ecosystems become more open, concentrated, resilient, or inclusive.

03

Third, **industrial policy** raises the strategic question of whether states seek merely to consume digital and AI technologies or to meaningfully participate in their production and evolution. In this regard, **long-term investments in all layers of the AI stack may become essential components of technological agency.** Yet, as argued throughout this paper, few countries are likely to develop all layers of the AI stack domestically. This reality reinforces the importance of selective specialization, trusted partnerships, and cooperative approaches to infrastructure and innovation development.

04

Fourth, **capacity building** may be the least visible, yet ultimately one of the most decisive dimensions of cooperative digital sovereignty. **Without capacitated human-ware [9] it becomes highly challenging to achieve administrative competence, institutional coordination, technical expertise, and broad digital and AI literacy, particularly within the public sector.** This challenge becomes even more pronounced in rapidly evolving AI ecosystems, where technological development and adoption often outpace regulatory evolution and educational capacity.

05

Finally, international and cross border **cooperation & interoperability** constitutes a distinct operational dimension of cooperative digital sovereignty. Particularly, intergovernmental organizations, multilateral forums, international standardization bodies, global research networks, cross-border energy and connectivity arrangements, and trusted data governance mechanisms play an essential role for the collective construction of cooperative digital sovereignty.

Specifically, within the framework proposed in this study, **cooperation refers to structured and strategically balanced forms of collaboration designed to strengthen domestic capabilities, diversify partnerships to mitigate dependencies, reduce structural asymmetries, and improve resilience across critical layers of the AI ecosystem.** From this perspective, cooperation becomes not merely a complement to the other domestic dimensions of digital sovereignty, but one of the core mechanisms through which sovereignty can be exercised. Indeed, when states act alone, they are more prone to "technological surprises" — failing to anticipate breakthroughs that leave gaps in their security and economic models [17] — whereas structured cooperation mitigates this exposure while preserving strategic autonomy.

The following subsection builds upon these considerations by outlining the operational elements of the DCO framework for Cooperative Digital Sovereignty that could support policymaking, institutional coordination, and international cooperation efforts within the membership of the of the Digital Cooperation Organization (DCO) and beyond.

5.1 Elements for an Analytical DCO Framework for Cooperative Digital Sovereignty

The framework outlined below provides an example of how the concept of Cooperative Digital Sovereignty may be operationalized by identifying how the five dimensions of public intervention, governance, regulation, industrial policy, capacity building, and international cooperation, may be strategically mobilized across the twelve Key AI Sovereignty Enablers (KASEs) outlined in Section 3.

Importantly, the framework is not intended as a prescriptive or one-size-fits-all model, and the elements suggested below should be considered indicative rather than exhaustive. Countries typically differ significantly in terms of institutional maturity, economic structure, technological capabilities, geopolitical positioning, infrastructure availability, and regulatory traditions.

Accordingly, the framework should be understood as an analytical and strategic tool capable of supporting context-sensitive policymaking, institutional coordination, prioritization, trusted international partnerships, and cross-border cooperation.

The framework is also action-oriented. Each cell of the table identifies a possible policy, institutional, regulatory, capacity-building, or cooperation measure that may be considered in relation to a specific enabler and dimension.

These measures are framed as practical entry points for policy design and implementation, rather than as abstract principles. As the matrix maps a wide option space, its purpose is to support prioritization, not comprehensiveness: states should prioritize strategic entry points rather than attempt to act simultaneously across every cell.

Furthermore, the five dimensions presented below are analytical rather than mutually exclusive. In practice, many policy instruments and governance mechanisms need to operate simultaneously across multiple dimensions of cooperative digital sovereignty. For example, trusted cross-border data flows may involve governance coordination, interoperable regulatory frameworks, industrial and infrastructure considerations, institutional capacity-building, and international cooperation mechanisms concurrently.

Similarly, cybersecurity, AI safety, semiconductor ecosystems, standards development, and cloud infrastructure governance frequently require integrated approaches spanning several dimensions simultaneously. The framework should therefore be understood as an interconnected and systemic governance model rather than a rigid policy taxonomy.

The table below illustrates how each of the twelve Key AI Sovereignty Enablers may be approached through the five interrelated dimensions of Cooperative Digital Sovereignty, using action-oriented examples that can be adapted to national priorities, institutional capacities, and cooperation opportunities.

DCO Framework for Cooperative Digital Sovereignty

Dimension	How to mobilize it, and why it matters (strategic importance)
1. Data	
Governance	Establish national data stewardship councils to coordinate data access, sharing, reuse, portability, and cross-sector governance. Structured oversight is instrumental in defining interoperable standards and ensuring that data is mobilized for public value while safeguarding rights. (e.g., Saudi Arabia's National Data Management Office) **Strategic importance:** Strengthens trusted data ecosystems while enabling cooperative governance across jurisdictions.
Regulation	Introduce privacy, portability, interoperability, secure access, and data-sharing obligations especially for strategic sectors and dominant platforms, supported by mechanisms such as data trusts, contractual clauses, and federated governance models. This approach balances openness with safeguards against extractive practices. **Strategic importance:** Prevents data monopolization, enabling broader participation in data-driven innovation while preserving sovereignty over strategic datasets.
Industrial Policy	Invest in trusted data spaces, sectoral data exchanges, and public-interest data infrastructures in areas such as health, mobility, energy, agriculture, manufacturing, and public administration. These data platforms must be sustainably funded and governed to remain accessible and effective. **Strategic importance:** Builds foundational digital assets, enabling domestic actors to compete and innovate within national and regional data ecosystems.

Dimension	How to mobilize it, and why it matters (strategic importance)
Capacity Building	Develop public-sector expertise in data stewardship, anonymization, valuation, interoperability, and data diplomacy. Tools such as the DCO Digital Economy Navigator can help identify capability gaps and policy priorities. **Strategic importance:** Strengthens institutional autonomy, allowing states to manage, negotiate, and leverage data resources effectively.
International Cooperation & Interoperability	Develop and participate in interoperable cross-border data governance and institutional cooperation frameworks, including mutual recognition systems, MCCs, and trusted transfer mechanisms. Examples include the DCO Interoperability Mechanism for Cross-Border Data Flows, and CBPR. **Strategic importance:** Enables trusted data cooperation while preserving sovereignty, resilience, and legal certainty.
2. Software Ecosystems, AI Models & Open-Source Capabilities	
Governance	Establish multistakeholder governance mechanisms and boards for oversight of AI model development, release practices, open-source ecosystems, and public-interest AI. Examples include UK AISI evaluation work, Singapore's AI Verify, and collaborative AI platforms such as Hugging Face and the Frontier Model Forum. **Strategic importance:** Fosters shared oversight of AI systems, reducing unilateral control by dominant ecosystem players, and aligning AI deployment with societal priorities.
Regulation	Mandate transparency, explainability, auditability, safety testing, and liability obligations for high-risk AI systems. These measures address risks stemming from AI systems while enabling responsible deployment. Examples include the EU AI Act and ISO/IEC 42001 on AI management systems. **Strategic importance:** Promotes trustworthy AI ecosystems, ensuring that sovereignty is not undermined by opaque or unaccountable systems.

Dimension	How to mobilize it, and why it matters (strategic importance)
Industrial Policy	Fund open-source AI ecosystems and support local innovation in open AI enablers to reduce reliance on proprietary technologies. Investments should target adaptable and domain-specific applications. For example, open model ecosystems hosted on Hugging Face. **Strategic importance:** Advances technological autonomy, enabling states to shape AI development rather than merely adopting external solutions.
Capacity Building	Invest in AI engineering, model evaluation, open-source development, AI safety, and interdisciplinary AI governance expertise. For example, Singapore Unified AI Literacy Framework. **Strategic importance:** Strengthens state's capacity to adapt, audit, govern, and deploy AI systems.
International Cooperation & Interoperability	Promote trusted and diversified regional and global AI R&D partnerships, federated open-source ecosystems, shared model-evaluation practices, and cooperative AI safety initiatives. **Strategic importance:** Expands cross-border participation in AI innovation while reducing structural asymmetries.
3. Compute, Semiconductors & Hardware Infrastructure	
Governance	Establish a strategic coordination body to align long-term national priorities across stakeholders for AI compute, cloud infrastructure, data centers, and semiconductors, enabling coherent governance, and resilient AI infrastructure planning. **Strategic importance:** Supports strategic positioning in global value chains, mitigating fragmentation and misaligned investments.

Dimension	How to mobilize it, and why it matters (strategic importance)
Regulation	Establish regulation on infrastructure resilience, supply-chain security, data and cloud security, and investment-screening frameworks, including assessment of exposure to foreign export controls on compute and semiconductors, to protect critical infrastructure from external vulnerabilities and geopolitical risks. Examples include NIS2 supply-chain security requirements. **Strategic importance:** Mitigates geopolitical, operational, and cybersecurity vulnerabilities.
Industrial Policy	Invest selectively in areas of strategic interest and strength, including semiconductors, advanced packaging, regional cloud infrastructure, sovereign or federated compute, and data centers. Complement targeted investment with national research-compute access programs that pool GPUs and cloud credits for domestic researchers and startups. This enables states to build targeted capabilities without overextending resources. Examples include the US CHIPS-funded TSMC Arizona project and the EU Chips Act. **Strategic importance:** Supports participation in critical AI infrastructure layers without requiring full-stack self-sufficiency, enabling selective autonomy.
Capacity Building	Build expertise in chip design, cloud architecture, data-center operations, and high-performance computing. **Strategic importance:** Anchors sustainable capability development in compute-intensive sectors.
International Cooperation & Interoperability	Develop trusted and diversified regional compute, cloud, and infrastructure coordination arrangements, including federated cloud models, shared compute access, and semiconductor cooperation. Examples include the EU InvestAI initiative. **Strategic importance:** Enables resource pooling, diversification, and resilience under conditions of global concentration.

Dimension	How to mobilize it, and why it matters (strategic importance)
4. Meaningful Connectivity	
Governance	Establish national connectivity coordination mechanisms to align broadband deployment, spectrum planning, internet exchange development, open internet principles, infrastructure resilience, and critical communications security across relevant ministries, regulators, operators, and infrastructure providers. Examples include Brazil's CGI.br. **Strategic importance:** Promotes system-wide coherence, ensuring inclusive, and secure connectivity ecosystems.
Regulation	Adopt regulatory frameworks that promote interoperability, infrastructure sharing, communications network security, open internet access, quality of service, and resilient digital communications. India's net-neutrality approach and EU open internet framework provide examples. **Strategic importance:** Safeguards open and secure networks, preventing fragmentation and external dependency.
Industrial Policy	Invest in resilient national broadband networks, IXPs, edge infrastructure, 5G/6G readiness, satellite connectivity, rural and underserved-area access, and alternative connectivity models such as community networks. Such investments can reduce dependence on single routes, providers, or infrastructure layers. **Strategic importance:** Reduces infrastructural asymmetries, and strengthens infrastructural autonomy.
Capacity Building	Build technical and regulatory expertise in network planning, spectrum management, vendor assessment, infrastructure auditing, cybersecurity-by-design, traffic routing resilience, and continuity planning for critical communications infrastructure. **Strategic importance:** Strengthens sovereign oversight and reduces informational asymmetries with infrastructure providers.

Dimension	How to mobilize it, and why it matters (strategic importance)
International Cooperation & Interoperability	Promote resilient and diversified cross-border connectivity corridors, submarine cable cooperation, regional IXPs, trusted telecom ecosystems, spectrum coordination, and regional infrastructure partnerships to reduce chokepoints, strengthen redundancy, and support secure participation in regional and global digital markets. Examples include 2Africa sub-sea cable initiative. **Strategic importance:** Strengthens regional integration while reducing excessive reliance on concentrated infrastructure providers.
5. Energy Availability & Resilient Power Infrastructure	
Governance	Establish AI-energy coordination mechanisms that align AI infrastructure planning with energy policy, grid capacity, sustainability targets, data-center permitting, and long-term demand forecasting. The UK AI Energy Council provides a relevant example of institutional coordination between AI infrastructure development and energy-system planning. **Strategic importance:** Aligns AI expansion ambitions with reliable and sustainable power systems.
Regulation	Introduce transparency, disclosure, efficiency, and sustainability obligations for data centers and AI infrastructure, including reporting on energy consumption, water use, emissions, and grid impacts. The EU Energy Efficiency Directive provides a useful example of data-center energy reporting obligations. **Strategic importance:** Integrates AI development with resource constraints, preventing bottlenecks, and supports sustainable and accountable AI infrastructure development.

Dimension	How to mobilize it, and why it matters (strategic importance)
Industrial Policy	Invest in renewable energy, resilient grids, energy storage, efficient cooling technologies, grid-connected data centers, and low-carbon AI infrastructure. Singapore's Green Data Centre Roadmap provides a relevant example of linking data-center growth with energy efficiency, sustainability, and infrastructure planning. **Strategic importance:** Aligns sovereignty objectives with sustainability goals by reducing external energy dependencies, mitigating energy bottlenecks, and supporting resilient and sustainable AI growth.
Capacity Building	Develop public sector and technical expertise in energy-aware computing, data-center cooling systems, grid planning, energy demand modelling, infrastructure permitting and integrated digital-energy policy to ensure that AI infrastructure expansion does not outpace energy-system capacity. **Strategic importance:** Improves cross-sectoral governance capacity and long-term integrated infrastructure planning.
International Cooperation & Interoperability	Develop regional electricity interconnection, cross-border energy-sharing arrangements, cooperative clean-energy infrastructure, and coordinated grid-resilience planning. The GCC Interconnection Authority provides a relevant example of how power grids can be linked into a regional network to improve reliability, redundancy, and energy security. **Strategic importance:** Enables AI infrastructure development through shared energy resilience and diversification.
6. Skilled Human Capital, Research Capacity & Scientific Ecosystems	
Governance	Establish AI skills councils, national AI academies, research coordination platforms, and science-policy interfaces to align education systems, research priorities, labor-market needs, and national AI strategies. **Strategic importance:** Aligns talent development with long-term AI priorities, reducing structural mismatches.

Dimension	How to mobilize it, and why it matters (strategic importance)
Regulation	Reform education, labor, immigration, and professional development frameworks to introduce mandatory digital and AI literacy, support upskilling and reskilling, facilitate smoother transitions between academia and the private sector, and promote the attraction and retention of highly skilled talent. **Strategic importance:** Mitigates talent shortages, and enhances talent valorization, mobility and retention, critical for competitive AI ecosystems.
Industrial Policy	Support university-industry partnerships, AI innovation hubs, applied research centers, doctoral programs, testing facilities, and scientific infrastructure that connect research capacity with domestic economic and public-sector priorities. **Strategic importance:** Connects research capacity with industrial transformation.
Capacity Building	Invest in AI literacy, STEM education, interdisciplinary AI governance, public-sector technical capacity, and research training, so that governments, firms, and society can understand, adopt, and govern AI systems effectively. UNESCO's AI competency frameworks for teachers and students provide useful examples. **Strategic importance:** Develops sustainable innovation and governance capacity.
International Cooperation & Interoperability	Promote international scientific cooperation, joint research centers, talent mobility partnerships, regional AI training ecosystems, shared doctoral programs, and collaborative research networks. The ELLIS network in Europe provides a relevant example of cross-border cooperation aimed at strengthening AI research excellence, talent development, and scientific collaboration. **Strategic importance:** Expands access to expertise while strengthening cooperative innovation ecosystems.

Dimension	How to mobilize it, and why it matters (strategic importance)
7. Cybersecurity and Cyber-Resilience Capabilities	
Governance	Create AI cybersecurity coordination centers, multistakeholder cyber-resilience forums and platforms, and joint incident-response mechanisms to align national cybersecurity authorities, sector regulators, cloud providers, critical infrastructure operators, and AI developers. **Strategic importance:** Strengthens collective resilience and coordinated risk management.
Regulation	Mandate security-by-design, vulnerability management, incident reporting, cybersecurity certification, and cyber-resilience protocols for critical digital and AI systems, including AI-specific protections such as safeguarding model weights and building resistance to data-poisoning and adversarial/prompt-injection attacks. Examples include EU NIS2 Directive, the EU Cyber Resilience Act, and Saudi Arabia's Essential Cybersecurity Controls. **Strategic importance:** Reduces systemic vulnerabilities by establishing baseline protection for critical AI ecosystems.
Industrial Policy	Support domestic cybersecurity industries, trusted cloud-security capabilities, secure-by-design technology providers, AI assurance services, and resilience-oriented digital infrastructure firms to reduce dependence on external providers for critical security functions. The UK's Cyber Growth Action Plan provides a useful example of policy efforts to strengthen domestic cybersecurity capabilities and industry growth. **Strategic importance:** Strengthens strategic autonomy in infrastructure protection and security provision.
Capacity Building	Train specialists in AI security, digital forensics, threat intelligence, secure software development, vulnerability assessment, incident response, and resilience planning. Saudi Arabia's National Cybersecurity Academy provides a useful example of institutionalized cyber-capacity development. **Strategic importance:** Builds defensive expertise necessary for AI sovereignty.

Dimension	How to mobilize it, and why it matters (strategic importance)
International Cooperation & Interoperability	Promote cyber threat intelligence-sharing, regional CERT cooperation, coordinated incident response, cyber-resilience exercises, and cooperative AI safety mechanisms. The Forum for Incident Response Security Teams (FIRST) provides a useful example of international cooperation among computer security and incident-response teams. **Strategic importance:** Strengthens collective resilience against cross-border cyber and AI risks.
8. Risk-Based Regulatory and Governance Frameworks	
Governance	Establish adaptive governance mechanisms, regulatory sandboxes for collaborative experimentation, AI testing frameworks, interoperability forums, evidence-based policymaking, AI incident-reporting systems and coordination among regulators, developers, public institutions, and affected stakeholders. Singapore's AI Verify is a relevant example of a practical AI testing and governance framework. **Strategic importance:** Facilitates innovation-friendly governance while reducing policy fragmentation.
Regulation	Implement tiered AI risk frameworks, procurement safeguards, liability rules, accountability obligations, impact assessments, audit requirements, compute-threshold / frontier-model governance and due-diligence mechanisms to ensure that regulatory obligations are proportionate to the risks posed by different AI systems. The EU AI Act provides a useful example of a risk-based regulatory model. **Strategic importance:** Enables proportionate oversight while supporting trust and legal certainty.

Dimension	How to mobilize it, and why it matters (strategic importance)
Industrial Policy	Provide compliance support for SMEs and startups through regulatory guidance, model documentation, shared testing infrastructure, subsidized audits, advisory services, and simplified compliance pathways to avoid regulatory burdens that entrench incumbents. **Strategic importance:** Supports inclusive AI innovation ecosystems.
Capacity Building	Build technical expertise among regulators, judges, auditors, procurement officials, and policymakers in AI risk assessment, algorithmic auditing, impact assessment, model evaluation, and responsible AI governance. DCO's Ethical AI Initiative and AI Ethics Evaluator provide relevant examples of tools that can support capacity-building and practical AI governance. **Strategic importance:** Strengthens implementation capacity and regulatory credibility.
International Cooperation & Interoperability	Promote interoperability between AI governance regimes through mutual learning, AI safety cooperation, shared standards, cross-border testing approaches, and mutual recognition where appropriate. DCO Principles for Ethical AI, and ISO/IEC 42001 provide relevant examples of principles and management-system standards that can support alignment across jurisdictions. **Strategic importance:** Reduces fragmentation while enabling trusted international AI governance.

Dimension	How to mobilize it, and why it matters (strategic importance)
9. Cognitive-Informational Resilience	
Governance	Develop multistakeholder resilience platforms to detect, assess, and respond to disproportionate or asymmetrical influence by foreign corporations, governments, or coordinated actors in AI-related public discourse and policymaking. UK's Online Information Advisory Committee provides a relevant example of expert advice supporting policy responses to online information risks. **Strategic importance:** Strengthens societal resilience and informational sovereignty by protecting public decision-making from manipulative influence.
Regulation	Introduce transparency, accountability, researcher access, and duty-of-care obligations for AI-mediated information ecosystems, especially where platforms or AI systems may influence public discourse, policy debates, infrastructure choices, or national technology decisions. The EU Digital Services Act is a relevant example. **Strategic importance:** Limits opacity, asymmetrical influence and manipulation in AI-mediated information ecosystems, reinforcing public trust and accountability.
Industrial Policy	Support pluralistic media ecosystems, public-interest digital platforms, trusted information infrastructure, local content ecosystems, and locally relevant AI models and datasets to reduce dependency on externally controlled information channels and strengthen domestic capacity to shape informed AI policy debates. **Strategic importance:** Reduces excessive platform dependency and strengthens informational diversity, pluralism, and locally grounded public discourse.

Dimension	How to mobilize it, and why it matters (strategic importance)
Capacity Building	Invest in media literacy, critical AI literacy, policy literacy, and public-sector capacity to identify AI-enabled manipulation, synthetic media, coordinated influence operations, and narrative campaigns affecting digital and AI policy choices. Finland's National Media Education Policy provides an example of a structured approach to media literacy and societal resilience. **Strategic importance:** Strengthens citizens' and institutions' capacity to navigate AI-mediated information environments and make informed decisions.
International Cooperation & Interoperability	Promote international cooperation on information integrity, AI-generated content transparency, countering coordinated influence operations, and shared standards for trustworthy digital information ecosystems. UNESCO's Media and Information Literacy (MIL) Alliance, International Fact-Checking Network (IFCN), and DCO Online Content Integrity Initiative provide relevant examples. **Strategic importance:** Strengthens collective resilience against transnational influence operations and AI-enabled manipulation of public discourse.
10. Access to Capital & Financing Ecosystems	
Governance	Establish coordinated national financing governance committees and mechanisms to align sovereign funds, innovation agencies, development banks, public financing institutions, and sector ministries around strategic AI priorities, including compute infrastructure, research capacity, startups, and AI adoption in priority sectors. **Strategic importance:** Strengthens national capacity to allocate capital toward long-term AI and digital development objectives.

Dimension	How to mobilize it, and why it matters (strategic importance)
Regulation	Develop regulatory frameworks governing investment transparency, competition safeguards, responsible AI investment, foreign investment screening where appropriate, and anti-concentration measures to ensure that digital and AI financing does not reinforce excessive dependency or market capture. **Strategic importance:** Supports sustainable financing ecosystems while reducing excessive market concentration and dependency risks.
Industrial Policy	Support venture capital ecosystems, sovereign AI funds, public-private partnerships, blended finance instruments, and strategic investment vehicles capable of financing compute, cloud, semiconductor, research, and AI-enabled enterprise development. **Strategic importance:** Addresses the capital intensity of AI infrastructure and innovation while expanding domestic participation in capital-intensive AI ecosystems and strengthening long-term technological resilience.
Capacity Building	Develop expertise in technology finance, AI valuation, innovation economics, procurement finance, infrastructure finance, blended finance, and strategic investment planning so that public institutions can assess, structure, and monitor AI-related investments effectively. **Strategic importance:** Strengthens countries' ability to sustainably finance and strategically govern AI ecosystem development over time.
International Cooperation & Interoperability	Enable structured financing cooperation through regional innovation funds, MDB-supported digital infrastructure financing, co-investment platforms, shared AI infrastructure initiatives, and cross-border public-private investment mechanisms to expand access to capital-intensive AI capabilities while preserving strategic autonomy. **Strategic importance:** Enables emerging economies to participate in capital-intensive AI ecosystems through trusted and diversified multilateral financing arrangements, while preserving strategic autonomy and reducing financial dependency asymmetries.

Dimension	How to mobilize it, and why it matters (strategic importance)
11. Industrial & Supply Chain Capabilities	
Governance	Establish integrated national industrial governance mechanisms to map, monitor, and coordinate critical AI supply-chain dependencies across semiconductors, advanced packaging, cloud infrastructure, data center equipment, networking hardware, rare earth inputs, and specialized components. **Strategic importance:** Strengthens institutional capacity to manage vulnerabilities across critical AI supply chains.
Regulation	Develop regulatory frameworks governing supply-chain security, trusted supplier requirements, export-control resilience, strategic procurement, vendor risk assessment, and critical infrastructure dependencies to reduce exposure to supply disruptions and coercive dependencies. **Strategic importance:** Mitigates vulnerabilities associated with concentrated and geopolitically exposed supply chains.
Industrial Policy	Align industrial policy with national strategic objectives by supporting targeted domestic manufacturing capacity, trusted suppliers, industrial diversification, strategic reserves, and participation in high-value segments of AI supply chains. Japan's Economic Security Promotion Act and semiconductor supply-chain resilience measures provide a useful example of targeted industrial support for critical technologies and supply-chain diversification. **Strategic importance:** Strengthens participation in strategically important segments of the AI value chain while reducing excessive dependency on concentrated production ecosystems.

Dimension	How to mobilize it, and why it matters (strategic importance)
Capacity Building	Develop expertise in semiconductor engineering, advanced packaging, logistics, industrial resilience planning, advanced manufacturing, supply-chain intelligence, and strategic technology assessment to strengthen domestic capacity to identify and manage critical dependencies. **Strategic importance:** Supports long-term domestic industrial capability and strategic technological resilience.
International Cooperation & Interoperability	Enable structured industrial cooperation through regional semiconductor partnerships, diversified manufacturing arrangements, friend-shoring mechanisms, trusted supplier ecosystems, supply-chain resilience partnerships, and coordinated investment in strategic AI supply-chain segments. Chip 4 / Fab 4 semiconductor alliance provides one relevant example. **Strategic importance:** Diversifies dependencies and expands technological options while preserving strategic flexibility and sovereign industrial priorities.

12. Technical Standardization Capacity

Dimension	How to mobilize it, and why it matters (strategic importance)
Governance	Establish national standardization coordination mechanisms that align regulators, industry, technical communities, academia, certification bodies, and national standards organizations around strategic AI, data, cybersecurity, cloud, and interoperability priorities. Participation in ISO, ITU, and IEEE processes provides relevant pathways for shaping international technical governance. **Strategic importance:** Strengthens national influence over global technical governance.

Dimension	How to mobilize it, and why it matters (strategic importance)
Regulation	Develop regulatory and technical frameworks that support interoperable AI governance, cybersecurity, data governance, conformity assessment, digital identity, cloud, and cross-border data standards. ISO/IEC 42001 provides a relevant example of an AI management-system standard that can support structured governance and risk management. **Strategic importance:** Creates trusted and interoperable digital environments while reducing implementation uncertainty and fragmentation.
Industrial Policy	Support domestic standards-development ecosystems, testing laboratories, conformity assessment mechanisms, open technical architectures, and participation in global standards bodies so that domestic firms and institutions can implement and influence technical requirements rather than merely comply with standards developed elsewhere. **Strategic importance:** Strengthens technological competitiveness and strategic participation in global digital ecosystems.
Capacity Building	Develop expertise in standards development, conformity assessment, interoperability governance, accreditation, testing, certification, and technical diplomacy among engineers, regulators, auditors, policymakers, and industry actors. This strengthens the ability to translate policy objectives into operational technical requirements. **Strategic importance:** Strengthens countries' ability to shape, implement, and strategically leverage technical standards.
International Cooperation & Interoperability	Enable structured cooperation through coordinated participation in international standards-development processes, interoperability frameworks, standards-mapping initiatives, and technical governance platforms. The ITU-led AI Standards Exchange provides a relevant example of a global initiative bringing together standards bodies and AI stakeholders to advance responsible, safe, and inclusive AI standards. **Strategic importance:** Expands countries' influence over global digital governance while preserving domestic implementation flexibility and strategic autonomy.

6. Policy Recommendations for DCO Member States

As argued above, operationalizing cooperative digital sovereignty with particular regard to AI requires coordinated policy action across governance, regulatory, industrial policy, infrastructure, and capacity building domains [5,9,11].

DCO Member States can strengthen their capacity to understand, develop, govern, and strategically benefit from AI systems by adopting integrated and strategically prioritized approaches that reinforce the Key AI Sovereignty Enablers while fostering trusted international cooperation, interoperability, resilience, and technological openness.

The preceding sections argued that cooperative digital sovereignty should not be understood as a pursuit of technological isolation or full-stack self-sufficiency. Rather, it concerns the capacity of states and societies to participate in interconnected digital and AI ecosystems on more resilient, strategically autonomous, and interoperable terms.

The policy challenge facing governments is therefore not whether to engage globally, but rather how to shape the conditions under which such engagement occurs.

This section advances a strategic action agenda for DCO Member States grounded in that premise. Importantly, the recommendations below do not seek to propose a uniform governance model applicable to all states.

Member States with highly diverse institutional capacities, economic structures, technological capabilities, and levels of digital maturity will therefore need to identify strategic priorities based on the analysis of their national contexts.

The Digital Cooperation Organization (DCO) is uniquely positioned to support Member States' efforts to jointly build cooperative digital sovereignty, given its growing ecosystem of interoperability mechanisms, governance frameworks, capacity-building initiatives, policy tools, and multilateral cooperation platforms.

Rather than proposing entirely new governance architectures, the recommendations below focus on how Member States may strategically leverage existing governance instruments, strengthen institutional coordination, and foster structured cooperation.

6.1 Move from Aspirational Sovereignty to Strategic Prioritization

One of the central risks in current digital sovereignty debates is the tendency to frame sovereignty as a generalized aspiration detached from institutional and economic realities.

While the ambition to strengthen technological autonomy is legitimate, few countries are likely to possess the financial resources, industrial depth, research capacity, compute infrastructure, and supply-chain access required to achieve sovereignty across every layer of the digital and AI stack.

Against this background, selective specialization and strategic prioritization provide an increasingly realistic and sustainable approach. **Governments should identify those segments of the digital and AI ecosystem where domestic assets can be leveraged and national capabilities can realistically be strengthened, where dependencies are strategically manageable, and where cooperation may produce the greatest resilience gains.**

From aspirational sovereignty to strategic prioritization

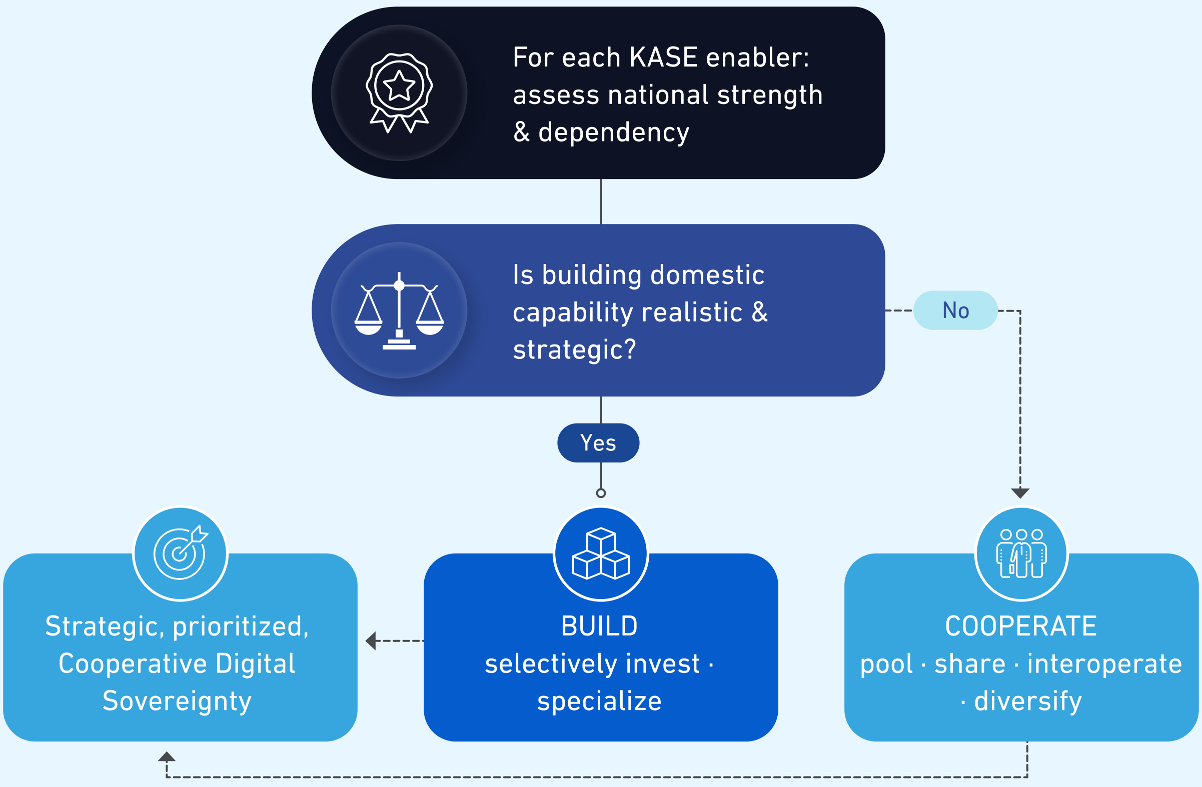


Figure 6. A build-versus-cooperate logic for moving from aspirational sovereignty to strategic prioritization

For some countries, this may involve prioritizing AI-enabled public services, trusted data ecosystems, AI governance and auditing expertise, cybersecurity and resilience capabilities, or AI applications tailored to national development priorities.

For others, emphasis may be placed on strategic sectors such as semiconductors, advanced packaging, cloud infrastructure, advanced connectivity, or energy-intensive compute ecosystems.

Several existing approaches reflect this maturity-sensitive logic. UNESCO's AI Readiness Assessment Methodology, Singapore's phased AI strategy, the EU's Tech Sovereignty Package, and emerging sovereign AI infrastructure initiatives in the Gulf region all illustrate the growing recognition that AI governance and ecosystem development must be sequenced according to institutional readiness and economic capacity.

In this regard, the DCO Digital Economy Navigator (DEN) and DCO AI-REAL Toolkit may provide DCO Member States with operational tools for assessing digital maturity, identifying structural gaps, sequencing reforms, prioritizing investments, and evaluating AI readiness according to domestic conditions.

The central policy objective should therefore not be the pursuit of symbolic sovereignty, but rather the development of strategically prioritized and institutionally sustainable pathways toward technological agency and resilience.

6.2 Build Institutional Capacity Before Expanding Regulatory Complexity

The effectiveness of AI governance depends less on the formal adoption of policies than on the institutional capacity required to implement, coordinate, and enforce them effectively. Many countries now possess national AI strategies, data protection laws, cybersecurity frameworks, and digital transformation agendas. Yet implementation capacity often remains fragmented, under-resourced, or institutionally incoherent.

This implementation deficit represents one of the most significant yet underappreciated constraints on digital sovereignty.

In this perspective, **Member States should prioritize strengthening public-sector technical competence, improving inter-agency coordination, expanding regulatory expertise, enhancing digital procurement capabilities, and building long-term institutional capacity across governance ecosystems.**

Several jurisdictions increasingly illustrate importance of institution-centered AI governance. Singapore's centralized AI governance coordination model, Canada's institutional focus on AI implementation and public-sector capability, and Saudi Arabia's dedicated AI governance structures all demonstrate that institutional coordination potentially retains as much significance as regulation itself.

Importantly, governance fragmentation constitutes a strategic vulnerability. AI systems interact simultaneously with data governance, industrial policy, cybersecurity, energy systems, competition policy, education ecosystems, and critical infrastructure governance.

As a result, siloed governance structures may unintentionally weaken national resilience and policy coherence.

Member States should therefore establish integrated coordination mechanisms capable of linking the sectoral mechanisms operating within each Key AI Sovereignty Enabler (KASE).

Such an integrated approach is instrumental to align KASEs within coherent long-term national frameworks. The DCO can support this process through interoperability-oriented policy dialogue, multistakeholder governance coordination, peer-learning initiatives, policy experimentation, and collaborative implementation support among Member States.

6.3 Operationalize Interoperability as a Sovereignty Strategy

One of the central arguments advanced throughout this study is that the operationalization of both legal and technical interoperability may provide a realistic pathway toward digital sovereignty. This is particularly visible in the domain of cross-border data governance.

AI systems increasingly depend upon access to diverse, interoperable, and high-quality data ecosystems. Yet divergent national governance frameworks frequently create legal fragmentation, regulatory uncertainty, and barriers to innovation and digital trade.

Rather than seeking complete harmonization of legal systems, several international initiatives increasingly pursue more flexible contractual approaches to legal interoperability. Examples include the EU's adequacy and Standard Contractual Clauses (SCCs) mechanisms, the Global CBPR Forum, and ASEAN Model Contractual Clauses. These approaches demonstrate that trusted interoperability can support cross-border cooperation while preserving sovereign governance flexibility.

In this regard, the DCO Interoperability Mechanism for Cross-Border Data Flows — including the DCO Privacy Principles, Model Contractual Clauses (MCCs), accreditation pathways, and data classification guidance — already provides Member States with an important operational foundation for trusted and legally interoperable data governance.

Importantly, the strategic value of interoperability extends beyond data governance alone. Similar logic applies to AI governance frameworks, cybersecurity coordination, technical standards, digital public infrastructure, AI auditing, and cloud and compute ecosystems. **The strategic objective for Member States should therefore not be uniformity, but rather the ability to participate in interconnected ecosystems without surrendering regulatory flexibility, strategic agency, or institutional autonomy.**

6.4 Prioritize Resilient and Cooperative Infrastructure Models

The concentration of compute infrastructure, cloud systems, semiconductor production, and AI training capabilities increasingly represents one of the defining structural characteristics of the global AI economy.

Under such conditions, purely national infrastructure strategies may prove economically unsustainable or strategically insufficient for many countries. **The challenge is therefore not simply to build more infrastructure, but rather to develop resilient, diversified, and strategically balanced infrastructure ecosystems.**

Several international initiatives already illustrate emerging approaches in this direction. The EU Chips Act and EuroHPC initiatives, regional cloud and semiconductor partnerships in East Asia, and sovereign AI infrastructure investments in the Gulf region all reflect attempts to reduce excessive concentration and diversify strategic dependencies.

For DCO Member States, cooperative infrastructure models may provide more realistic pathways toward resilience and participation in the AI economy.

Such approaches, for example, **a GenAI Center of Excellence for the DCO Member States,** may include federated compute infrastructure, regional cloud ecosystems, shared AI testing environments, coordinated cybersecurity architectures, trusted digital public infrastructure, and cross-border energy integration capable of supporting compute-intensive AI systems.

These approaches may allow Member States to pool resources, diversify infrastructure dependencies, reduce concentration risks, improve resilience, and strengthen participation in capital-intensive AI ecosystems without undermining strategic autonomy.

The DCO Data Embassy concept may also play an important role in this regard by supporting continuity, redundancy, and resilience for critical governmental and strategic data systems through trusted cross-border infrastructure arrangements.

Importantly, infrastructure resilience should increasingly be understood not only as a technical issue, but as well an essential geopolitical resilience issue.

6.5 Treat AI Safety, Cybersecurity, and Cognitive Resilience as Strategic Sovereignty Issues

The increasing integration of AI systems into critical infrastructure, governance systems, financial ecosystems, media environments, and security architectures means that AI resilience and cybersecurity can no longer be treated as isolated technical domains.

Rather, they increasingly constitute intertwined strategic issues that compose an array of risks that must be assessed and mitigated when approaching digital sovereignty.

Member States should therefore strengthen coordination and cooperation in regard to risk assessment, governance and response to cybersecurity governance, AI safety, supply-chain resilience, critical infrastructure protection, and resilience planning across interconnected digital ecosystems.

Emerging international initiatives demonstrate the growing importance of structured resilience cooperation. Examples include the Joint Guidelines for Secure AI System Development developed by the UK's NCSC, the US CISA, and international partners; collaborative cybersecurity initiatives such as FIRST; and growing international discussions around AI safety governance and systemic AI risks.

Conspicuously, resilience-oriented cooperation should not undermine sovereign cyber governance. Rather, structured cooperation may strengthen collective resilience while preserving national operational autonomy and governance flexibility.

6.6 Strengthen Strategic Participation in Standards and Governance Processes

Technical standards increasingly shape the architecture of the global AI economy. Countries that do not participate actively in standards-development processes risk becoming passive rule-takers within governance systems designed elsewhere.

Standards influence AI governance, cybersecurity, cloud interoperability, digital public infrastructure, AI auditing, semiconductor ecosystems, and trusted data governance frameworks.

Consequently, standards participation increasingly constitutes a strategic governance capability rather than merely a technical exercise.

Member States should therefore strengthen and coordinate participation in international standardization bodies. In this context, the DCO may play an important coordinating role in supporting interoperability-oriented standards discussions, coordinated engagement in global governance processes, technical capacity-building, and strategic participation by Member States in standards-development ecosystems.

6.7 Build Sustainable Financing and Innovation Ecosystems

The extraordinary capital intensity of AI infrastructure and advanced research risks deepening structural asymmetries between countries capable of mobilizing large-scale financing and those that remain dependent on external infrastructure ecosystems.

As a result, financing ecosystems constitute a core dimension of digital sovereignty. **Member States should therefore strengthen sovereign innovation financing mechanisms, blended financing ecosystems, AI-focused public-private partnerships, regional innovation funds, and strategic infrastructure financing arrangements.**

Examples such as sovereign AI investment initiatives in the Gulf region, the EU's InvestAI and AI Factories initiatives, and growing multilateral development bank engagement in digital infrastructure financing all illustrate the growing importance of patient and long-term strategic investment ecosystems in shaping participation within the global AI economy.

Importantly, financing strategies should prioritize strategic infrastructure, research ecosystems, AI-enabled SMEs, public-interest AI initiatives, and locally relevant AI applications aligned with national development priorities.

The DCO could also play a relevant role in facilitating the study and testing of cooperative financing approaches that enable Member States to access capital-intensive AI ecosystems while reducing dependency asymmetries and preserving strategic flexibility.

6.8 Consolidate Coordination Through a Standing DCO Platform for Cooperative Digital Sovereignty

The recommendations above can be pursued through national, regional, bilateral, and multilateral channels. Within this broader landscape, the **DCO can serve as an important enabling platform for Member States seeking to operationalize cooperative digital sovereignty through structured cooperation, interoperability-oriented governance, capacity building, and coordinated policy action.**

Such a platform could integrate three mutually reinforcing functions.

02 First, it could support knowledge exchange, peer learning, and coordinated participation by Member States in international forums and standards-development processes.

03 Second, it could advance regulatory and technical interoperability, building on the DCO Interoperability Mechanism for Cross-Border Data Flows, the Privacy Principles, and the Model Contractual Clauses.

02 Third, it could facilitate cooperative financing, investment coordination, and joint procurement models for shared digital and AI infrastructure.

By bringing these functions together, the DCO could help give cooperative digital sovereignty a more concrete operational pathway while complementing other national, regional, and international efforts.

As global debates intensify around AI safety, governance interoperability, technological concentration, digital resilience, and strategic technological dependencies, the DCO may emerge as a platform capable of advancing more inclusive, operationally grounded, and cooperation-oriented approaches to digital and AI governance [5,9,11].

7. Conclusion: Operationalizing Cooperative Digital Sovereignty within the DCO

This study has argued that the central digital policy challenge for states and societies currently lies in strengthening their capacity to govern technological interdependence, reduce excessive structural dependencies, diversify technological options, and participate in global digital ecosystems on more resilient, interoperable, and strategically autonomous terms.

Within this context, the concept of cooperative digital sovereignty offers an operationally realistic and institutionally sustainable approach to digital governance. In particular, the analytical framework advanced in this study conceptualizes sovereignty and cooperation as mutually reinforcing dimensions of contemporary digital governance.

Carefully designed forms of legal and technical interoperability, coordinated governance, resilience-oriented infrastructure cooperation, and multistakeholder coordination may strengthen states' ability to preserve agency while remaining integrated within global digital and AI ecosystems.

The analysis argued that AI sovereignty depends upon the interaction of multiple interconnected enablers, including data governance, compute infrastructure, software ecosystems, energy availability, human capital, cybersecurity, standards participation, and financing ecosystems.

Importantly, these enablers do not evolve independently. Rather, they interact continuously across the dimensions of governance, regulation, industrial policy, capacity-building, and international cooperation, among others.

As a result, in a rapidly evolving AI landscape, isolated or fragmented interventions are unlikely to yield sustainable outcomes. What is required instead is a systemic and strategically prioritized approach capable of aligning technological, institutional, economic, and governance ecosystems over time.

Within this context, the Digital Cooperation Organization (DCO) is uniquely positioned to play a significant role in operationalizing cooperative digital sovereignty.

As an intergovernmental platform focused on inclusive digital transformation and multistakeholder cooperation, the DCO can support DCO Member States not only through policy dialogue, but increasingly through operational governance mechanisms, interoperability frameworks, capacity-building initiatives, and resilience-oriented cooperation models. Importantly, the organization already possesses several institutional building blocks capable of supporting such an approach.

The future relevance of cooperative digital sovereignty may ultimately depend less on the creation of entirely new governance principles than on the ability to operationalize existing governance instruments more coherently across jurisdictions and institutions.

In this regard strategic coordination, and resilience-oriented cooperation increasingly emerge not as alternatives to sovereignty, but rather as mechanisms through which sovereignty may be exercised and sustained under conditions of deep technological interdependence.

In this perspective, for the DCO and its Member States, the operationalization of Cooperative Digital Sovereignty should begin with the development of a Digital Sovereignty Toolkit, as a follow-up to this report. This report aims at providing the information necessary to nurture a DCO reflection, that can feed into the development of a toolkit capable of systematically assessing technological dependencies, identifying strategic vulnerabilities across the AI value chain, and benchmarking national capabilities.

Building on this diagnostic framework, Member States could then pilot the Key AI Sovereignty Enablers (KASE) matrix as a maturity-based self-assessment instrument to identify national priorities and sequence investments according to their institutional capacities and development objectives.

A third step would involve establishing dedicated DCO working groups to foster regulatory interoperability, develop mutual-recognition mechanisms, and advance joint initiatives such as regional research networks, federated compute infrastructures, and trusted digital public infrastructure.

Ideally, the DCO should also and institutionalize a recurring multistakeholder dialogue bringing together governments, industry, academia, civil society, and technical experts to monitor progress, exchange best practices, and coordinate policy development.

Finally, the Organization could develop model cooperation instruments – including common templates for agreements on cross-border data governance, compute sharing, cybersecurity cooperation, and AI research collaboration – to facilitate trusted cooperation and progressively strengthen the digital resilience and technological autonomy of its Member States.

Ultimately, the contribution of this study lies not in proposing a singular governance model applicable to all countries, but rather in advancing an analytical and operational framework capable of helping policymakers navigate the growing tensions between openness and security, autonomy and interdependence, and national governance and global technological concentration.

For DCO Member States, cooperative digital sovereignty may therefore offer a pragmatic pathway enabling the simultaneous strengthening of technological autonomy and meaningful integration within fast-evolving digital ecosystems and AI supply chains.

Annex 1. Methodological Approach

This study adopts a qualitative and interdisciplinary research methodology combining conceptual analysis, comparative policy mapping, and institutional analysis. The objective is to clarify the concept of cooperative digital sovereignty in the context of AI and develop an analytical framework capable of informing policy development among DCO Member States, and beyond.

The conceptual analysis draws on existing scholarship on digital sovereignty, law and technology, digital governance, and political economy of technological development. In particular, the study builds upon recent contributions examining the evolution of digital sovereignty debates and their implications for emerging economies [7,8,9,41,56].

These works provide a theoretical foundation for understanding how states seek to exercise agency over digital infrastructures and technologies.

The study also integrates insights from the literature on national innovation systems and technological catch-up. Research in this field demonstrates that technological development is strongly shaped by institutional structures, industrial policies, and research ecosystems. This perspective highlights the importance of coordinated policy interventions in enabling countries to develop domestic technological capabilities.

The analytical framework of the study is structured around the Key AI Sovereignty Enablers (KASE) identified by Belli [5,8].

The KASE framework, enhanced in this study, provides a multidimensional model for assessing national AI capabilities and governance frameworks, and direct strategic actions in a coordinated fashion.

By organizing the analysis around these elements, the study aims to identify policy instruments and governance strategies that can strengthen technological capacity while promoting international cooperation.

Furthermore, the study emphasizes the existence of policy tools and governance frameworks developed by the DCO that should be leveraged to operationalize the proposed conceptualization of cooperative digital sovereignty.

These instruments — including those developed under the DCO Interoperability Mechanism for Cross-Border Data Flows, the DCO Principles for Ethical AI, the AI-REAL Toolkit, the DCO AI Ethics Evaluator, the Digital Economy Navigator (DEN), the DCO Data Embassy initiative, and emerging initiatives related to international cooperation on AI safety and governance — are identified as potential mechanisms aimed at assisting policy making and implementation of cooperative digital sovereignty across diverse national contexts.

A final methodological clarification is warranted. Generative AI tools – notably ChatGPT, Google Gemini, and Claude – were employed in a limited and clearly circumscribed manner to i) distill and reorganize the author's prior research findings mentioned throughout the study; and to ii) facilitate the specification of the Key AI Sovereignty Enablers across the five proposed dimensions in the analytical framework proposed in Section 5.

All substantive arguments, interpretations, and normative positions remain the responsibility of the authors, who elaborated, critically reviewed, validated, and refined all outputs.

References

1. AGRAWAL, Ajay; GANS, Joshua; GOLDFARB, Avi. Prediction machines: the simple economics of artificial intelligence. Boston: Harvard Business Review Press, 2018.

2. BELLI, L. (2015). De la gouvernance à la régulation de l'Internet. Paris: Berger Levrault. https://hdl.handle.net/10438/33380

3. BELLI, L. (2017). Net neutrality, zero rating and the Minitelisation of the internet. Journal of Cyber Policy, 2(1), 96–122. https://doi.org/10.1080/23738871.2016.1238954

4. BELLI, L. (2021) BRICS Countries to Build Digital Sovereignty. In: BELLI, L. (Ed.). CyberBRICS: Cybersecurity Regulations in the BRICS Countries. Cham: Springer International Publishing. p. 271–280

5. BELLI, L. (2023a). Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil. T20 India. https://t20ind.org/research/building-good-digital-sovereignty-through- digital-public-infrastructures/

6. BELLI, L. (2023b). "To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE)." In FELDSTEIN S. New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms. Carnegie. http://dx.doi.org/10.2139/ssrn.4465501

7. BELLI, L. (2024). BRICS countries and AI sovereignty: Introduction to Thematic Section . AJIC, 34, 1–6. https://doi.org/10.23962/ajic.i34.128842

8. BELLI, L. (2025). How are BRICS countries building AI sovereignty? AJIC, 35, 1–4. https://doi.org/10.23962/ajic.i35.23192

9. BELLI, L. et al. (2026). Soberania Digital e Inteligência Artificial no Brasil: Rumo à autonomia tecnológica. Lumen-Juris.

10. BELLI, L.; GASPAR, W. B & KREWER, J. (forthcoming). "Leveraging Open Source Technologies as a Techno-regulatory Strategy to Advance Digital Sovereignty" in SAPPA C. Research Handbook on Sovereignty and Dependence in IPRs. Edward Elgar Publishing

11. BELLI, L.; GASPAR, W. B. (Eds.) (2025). The Quest for AI Sovereignty, Transparency and Accountability. Springer-Nature. https://link.springer.com/book/10.1007/978-3-032-02762-7

12. BELLI, L.; GASPAR, W. B.; SINGH J.S. (2024). Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. Computer Law & Security Review, vol. 54, p. 106017. https://doi.org/10.1016/j.clsr.2024.106017

13. BELLI, L. et al. Cibersegurança: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. Rio de Janeiro: FGV Direito Rio, 2023. 118 p. ISBN 978-65-00-72715-9.

14. Belli, L. & ZINGALES , N. (2025). Building sovereign and integrated data governance, from Latin America to the G20, International Data Privacy Law, Vol. 15, Issue 4, Pages 319–322. https://doi.org/10.1093/idpl/ipaf021

15. BORDEN, A.C. What is Information Warfare?. Air University Press, [s. d.]. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf.

16. CANFIL, J. K. (2026). Convergent Flexibility: How International Law Keeps Pace with Technological Change. International Organization. Published online 2026:1-44. doi:10.1017/S0020818326101295

17. CASSIOLATO, J. E. The Brazilian System of Innovation policy Challenges . Discussion Paper, TD DIT. v. 16, p. 44, 2008.

18. CIHON, P. (2019). Standards for AI Governance: International Standards to Enable Global Coordination in AI Research & Development. Future of Humanity Institute, University of Oxford.

19. COHEN, J.E., Between Truth and Power: The Legal Constructions of Informational Capitalism (OUP 2019).

20. DIGITAL COOPERATION ORGANIZATION (DCO). (2024). Digital public infrastructure: A catalyst for socio-economic growth and digital transformation. Digital Cooperation Organization Insights. https://dco.org/digital-public-infrastructure-2/

21. DIGITAL COOPERATION ORGANIZATION (DCO). (2025) The Digital Economy Navigator (DEN). https://den.dco.org/.

22. DIGITAL COOPERATION ORGANIZATION (DCO). (2025). Ethical Guidebook for Policymakers. https://dco.org/ai-ethical/.

23. DIGITAL COOPERATION ORGANIZATION (DCO). (2025). AI-REAL Toolkit: Measuring AI Maturity and AI Adoption Playbook. https://dco.org/initiatives/ai-real-toolkit/.

24. DIGITAL COOPERATION ORGANIZATION (DCO). (2025). DCO Ethical AI Initiative. https://dco.org/initiatives/ethical-ai/

25. DIGITAL COOPERATION ORGANIZATION (DCO). (November 2025). Policy Watch – Edition 6: Interconnected Digital Economy. https://dco.org/dco-policy-watch-sixth-edition/.

26. DIGITAL COOPERATION ORGANIZATION (DCO). (September 2025). Policy Watch – Edition 5: Digital Resilience. https://dco.org/dco-policy-watch-fifth-edition/.

27. DOSI, G. et al. Mission- oriented policies and the " Entrepreneurial State " at work : An agent-based Exploration Journal of Economic Dynamics and Control . Elsevier BV, 2023

28. DOWSE, A.; BACHMANN, S.D. (2022). Information warfare: methods to counter disinformation. Defense & Security Analysis, v. 38, n. 4, p. 453–469.

29. EAVES D. & SANDMAN I. 'Digital Public Infrastructure: A Framework for Public Digital Transformation' (2023) Government Information Quarterly 40(3) 101835

30. EDLER J. & FAGERBERG J., 'Innovation Policy: What, Why, and How' (2017) 46 Oxford Review of Economic Policy 2

31. FARRELL, H.; NEWMAN A.L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. International Security 2019; 44 (1): 42–79. https://doi.org/10.1162/isec_a_00351

32. FLORIDI, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. Philosophy and Technology, 33(3), 369–378.

33. FREEMAN, C. The Economics of Industrial Innovation. 2. ed. London: Frances Pinter, 1982

34. FUKAWA, N.; ZHANG Y. & EREVELLES S. (2021). 'Dynamic Capability and Open-Source Strategy in the Age of Digital Transformation' 7(3) Journal of Open Innovation: Technology, Market and Complexity 175 https://doi.org/10.3390/joitmc7030175

35. G20 (GROUP OF TWENTY) (2023). G20 New Delhi Leaders' Declaration. New Delhi: G20. https://www.g20.org/content/dam/gtwenty/gtwenty_new/document/G20-New-Delhi-Leaders-Declaration.pdf

36. GELUVARAJ, B.; SATWIK P. M.; ASHOK KUMAR T.A. (2019). The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. International Conference on Computer Networks and Communication Technologies: ICCNCT 2018. Springer.

37. GLATTER, R. (2025). From Overdependence to Independence: European Policy Frameworks for Semiconductor Supply Chain Resilience. IE University Repository Working Paper.

38. GROGAN, J. J. (2026). The end of the foundation model era: Open-weight models, sovereign AI, and inference as infrastructure. Universitas AI Preprint. https://arxiv.org/pdf/2604.06217

39. HARAMBOURE, A. et al. (2023). Vulnerabilities in the semiconductor supply chain. OECD Science, Technology and Industry Working Papers, No. 2023/05.

40. HAWKINSON, J.; BATES, T. (1996). RFC 1930: Guidelines for creation, selection, and registration of an Autonomous System (AS). IETF. https://www.rfc-editor.org/rfc/rfc1930.html

41. JIANG, M., & BELLI, L. (Eds.). (2024). Digital Sovereignty from the BRICS: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance Countries. Cambridge University Press. https://doi.org/10.1017/9781009531085

42. JIANG, M., (2025). Automated authority: AI algorithms. New America. https://is.gd/SK7vEt

43. JOHANSSON G. P., FARIAS, V. & GASPAR, W. B. (2024). Brazil's Artificial Intelligence Plan (PBIA) of 2024: Enabler of AI sovereignty ? African Journal of Information and Communication, 34.

44. LEE, K ; MALERBA, F. (2014). Changes in Industry Leadership and Catch -up by the Latecomers: Toward a theory of catch- up cycles . In : GLOBELICS CONFERENCE. Anais... Ankara: sea.

45.LEE, K.; MALERBA, F. (2017). Catch-up cycles and changes in industrial leadership : Windows of opportunity and responses of firms and countries in the evolution of Sectoral systems. Research Politics , vol. 46, no. 2, p. 338–351.

46. LEES, S; EDLER, J. (2020). The roles of the state in the governance of socio- technical systems' transformation . Research Policy . Elsevier BV.

47. LEE, K;; SZAPIRO, M;; MAO, Z. From global value chains (GVC) to innovation systems for local value chains and knowledge creation: the case of China. The European Journal of Development Research, London, v. 30, n. 3, p. 424–441, 2018

48. LEINER, B. M. et al. A brief history of the Internet. Internet Society, 1997. Disponível em: https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf

49. LESSIG, L. Code: and other laws of cyberspace. New York: Basic Books, 1999

50. MA, A. (2024). Regulation in pursuit of artificial intelligence (AI) sovereignty: China's mix of restrictive and facilitative modalities. African Journal of Information & Communication. N. 34. https://scielo.org.za/pdf/ajic/v34/06.pdf

51. MALATJI M.; A. TOLAH. (2024). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. AI and Ethics.

52. MAYER, K.; MAGER, A.; RIDGWAY R. (eds), The Politics of Open Infrastructures: Power, Governance, and Justice in Digital Knowledge Practices. Cambridge: Open Book Publishers, 2026, https://doi.org/10.11647/OBP.0528

53. MAZZUCATO, M. The Entrepreneurial State . London: Penguin , 2018.

54. MAZZUCATO, M., COLLINGTON, R., & KATTEL, R. (2026). Digital public infrastructure and the economics of public value: what is 'public' about DPI? Innovation and Development, 16(1), 34–58. https://doi.org/10.1080/17487870.2026.2662285

55. OWCZAREK, Michał; WŁOCH, Renata. The power of digital infrastructure: how conflicts between platforms and states redefine sovereignty? Athenaeum. Polskie Studia Politologiczne, v. 88, p. 92–115, 2025. DOI: 10.15804/athena.2025.88.05

56. POHLE, J., & THIEL, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1532
RADOSEVIC S AND YORUK E, 'Entrepreneurial Propensity of Innovation Systems: Theory, Methodology and Evidence' (2018) 47 Research Policy 103.

57. REID SMITH S. et al., 'Taking Forward Digital Public Infrastructure for the Global South' (2025) South Centre Policy Brief 146

58. RICHTER, F. (2026). Infographic: Big Three Hold Dominant Lead in Accelerating Cloud Market, Statista Daily Data: https://www.statista.com/chart/18819/worldwide-marketshare- of-leading-cloud-infrastructure-service-providers

59. RIKAP, C. (2021). Capitalism , Power and Innovation ; Intellectual Monopoly Capitalism Uncovered . London & New York: Routledge.

60. SCHUMPETER, Joseph A. The Theory of Economic Development. New Brunswick: Transaction Publishers, 1934. (Originally published in German in 1911.)

61. SENGUPTA, A.; BARBOSA, A. C.; SAMDUB, M. (2025). Understanding interrelationships between AI and digital public infrastructure in India and Brazil. African Journal of Information and Communication. N. 35. 2025. https://ajic.wits.ac.za/article/download/20800/24560/143742

62. SILVA, E. G.; TEIXEIRA, A. Does structure influence growth ? A panel data econometric assessment of "relatively less developed" countries, 1979-2003. Industrial and Corporate Change. Oxford University Press, 2011.

63. SLATTERY P. et al. (2024). The AI risk repository: A comprehensive meta-review, database, and taxonomy of risks from artificial intelligence. Massachusetts Institute of Technology.

64. STRANGE, Susan. States and Markets: An Introduction to International Political Economy. London: Pinter Publishers, 1988. 263 p. ISBN 0-86187-942-2.

65. VAN DER VLIST, F; N. et al. (2024). Big AI: cloud infrastructure dependence and the industrialisation of artificial intelligence. Data & Society, v. 11, n. 1. https://doi.org/10.1177/20539517241232630

66. VELASCO, L. et al. (2026). Financing the AI Triad: Compute, Data and Algorithms. Oxford Martin AI Governance Initiative. https://aigi.ox.ac.uk/wp-content/uploads/2026/02/Oxford-Financing-the-AI-Triad-V6.pdf

67. VIPRA, J. (2025). Towards AI sovereignty: the good, the bad, and the ugly of AI policy in India. African Journal of Information and Communication. N. 35. https://scielo.org.za/pdf/ajic/v35/05.pdf

68. VIPRA, Jai; WEST, Sarah Myers. Computational Power and AI. New York: AI Now Institute, 2023. Disponível em: AI Now Institute Report Page

69. WANG, W. W. et al. (2025).Artificial Intelligence "Law(s)" in China: retrospect and prospect. Journal of AI Law and Regulation. Journal of AI Law and Regulation (AIRe).

70. WHITTAKER, M. (2026). 'Open Source AI: Narrative Arbitrage and the Concentration of Power'. AI Now Institute Reports

71. WIDDER, D., WEST S. & WHITTAKER M. (2024). 'Open (Source) AI: Is Open Source Initializing Pixel-Level Democracy or Just Redefining Concentration?' 2024 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) 1 https://doi.org/10.1109/CVPR56322.2024.00014

72. XIONG, W., WU, D. D., & YEUNG, J. H. Y. (2024). Semiconductor supply chain resilience and disruption: insights, mitigation, and future directions. International Journal of Production Research, 1–24. https://doi.org/10.1080/00207543.2024.2387074

73. ZUBOFF, S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (Profile Books 2019).

Digital Cooperation Organization

Follow us on

@dcorg | www.dco.org