Building Digital Infrastructure Ready for the AI Era

Insights from 13 Middle Power Governments

June 2026

Project Liberty Institute

GLOBAL SOLUTIONS

Disclaimer & Methodology

This report is a qualitative synthesis of insights and does not function as a quantitative or statistically representative scientific study. The findings are based on interviews, surveys, and polls conducted with government officials across ministries of digital transformation, telecommunications, and infrastructure.
While the selection favors G20 member states, non-G20 nations were included as they offer distinctive evidence of how the Middle Power dynamics – which have intensified since early 2026 – shape infrastructure choices on the ground. Middle Powers collectively possess significant AI research capacity, democratic governance frameworks, technological sophistication, and economic weight. To best represent its diversity, our methodology prioritized a balance between:

- Large vs. Small economies.
- Global North vs. Global South perspectives.
- Diverse Geographic Representation across five continents.
- Advanced vs. Nascent digital infrastructure strategies and deployments.

The research was conducted between July 2025 and May 2026, timed with major milestones at key global forums including World Summit on Information Society and the AI For Good (7 to 11 July 2025), United Nations General Assembly (22 to 29 September 2025), and the India AI Impact Summit (16 to 21 February 2026).

Data was gathered through:

1. Direct Consultations: In-person and virtual interviews with government officials.
2. Quantitative Follow-ups: Supplemental surveys to validate interview themes and deepen specific aspects of the topic.
3. Comparative Analysis: Reviewing existing case studies
4. G7 and G20 Consultations: Engagement with G7 Canada and G20 South Africa processes, including events, consultations, and policy briefs timed with presidencies and relevant taskforces, to validate findings, to situate country-level findings within the broader multilateral policy landscape, and feeding research directly into communiqué language and working-group deliberations on digital infrastructure, AI governance, and data-for-development frameworks.
5. Digital Infrastructure Toolkit: Building on top of Project Liberty Institute and the Global Solutions Initiative's "Digital Infrastructure Solutions to Empower Citizens: A Toolkit for Policymakers - Designing, Scoping and Governing Digital Infrastructure to Advance Data Agency"

The interviews conducted do not capture all relevant ministries or agencies responsible for digital infrastructure within each government. As such, the findings provide a partial view of national systems. This partiality is itself indicative of a core challenge identified throughout the research: institutional fragmentation.

The views expressed herein represent an independent interpretation of gathered insights and are not to be attributed to any specific individual, government, or official position.

Please cite as: Nicole, S., Mishra, V., Theodule, J., Rodriguez, M. (2026, June). Building digital infrastructure ready for the AI era - Insights from 13 Middle Power governments. Project Liberty Institute & Global Solutions Initiative.

Governments interviewed*

Brazil
National Telecommunications Agency (ANATEL)

Cambodia
Ministry of Post and Telecommunications

Canada
Treasury Board of Canada Secretariat (TBS)

France
Interministerial Digital Directorate (DINUM)

Germany
Federal Ministry for Digital Transformation and State Modernization (BMDS)

Greece
Office of the Prime Minister of the Hellenic Republic

Indonesia
Ministry of Communications and Digital Affairs (Komdigi)

** The display of institutional logos is for descriptive purposes only, identifying the government entities that participated in the research process. Their inclusion does not constitute an endorsement of the report's findings or recommendations by the participating institutions.*

Governments interviewed*

デジタル庁
Digital Agency

Japan
Digital Agency of Japan

HARAMBEE
OFFICE OF THE PRESIDENT

Kenya
Office of the Special Envoy on Technology, Republic of Kenya

Transformación Digital

Mexico
Agency for Digital Transformation and Telecommunications

MCTN
Ministère de la Communication, des Télécommunications et du Numérique

Senegal
Performance and Quality Division of the Ministry of Communication, Telecommunications and Digital Economy

communications & digital technologies
Department: Communications & Digital Technologies
REPUBLIC OF SOUTH AFRICA

South Africa
Department of Communications and Digital Technologies (DCDT)

THE PRESIDENCY
REPUBLIC OF SOUTH AFRICA

South Africa
The Presidency of the Republic of South Africa

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Office of Communications OFCOM

Switzerland
Federal Office of Communications (OFCOM)

** The display of institutional logos is for descriptive purposes only, identifying the government entities that participated in the research process. Their inclusion does not constitute an endorsement of the report's findings or recommendations by the participating institutions.*

Authors

Project Liberty Institute
Sarah Nicole, Policy & Research Manager
Jessica Theodule, Research Manager of Strategic Insights

Global Solutions Initiative
Vidisha Mishra, Director, Global Outreach & Policy
Mateo Rodriguez, Senior Manager, Global Outreach & Policy

Leadership

"This report confirms that governments are not just building data layers, they are encoding values and social systems into the digital stack. In the AI era, that means the choices middle powers make today about data agency, open infrastructure, and cross-border cooperation will determine whether the next digital decade is defined by democratic resilience or by dependency."

Jeb Bell, Executive Director, Project Liberty Institute

"Digital infrastructure is no longer just a technical matter but a governance imperative defining national resilience – and while global superpowers have historically led, the architecture of the next digital era will be shaped by the standards and policy choices of middle powers."

Christian Kastrop, President & CEO, Global Solutions Initiative

Project Liberty Institute //

About Project Liberty Institute

The Project Liberty Institute is an independent 501(c)(3) at the center of the global effort to build an open, pro-human AI ecosystem. We bring together technologists, researchers, policymakers, investors, and civic leaders to ensure that people have a voice, choice, and stake in the future of AI. Our work spans three areas: building open technology infrastructure that puts people in control of their data and digital identity, advancing policy frameworks that align legal code with technical architecture, and generating the research and models that prove pro-human AI can be technically excellent and commercially competitive.

GLOBAL SOLUTIONS

About Global Solutions Initiative

The Global Solutions Initiative (GSI) is an independent, non-profit platform bringing together international think tanks, civil society organizations, researchers, policymakers, and business leaders to develop evidence-based solutions to global challenges. Founded during Germany's G20 Presidency in 2017, GSI leverages its networks and regional hubs to foster dialogue and collaboration in support of the G7, G20, and other multilateral processes. A key focus of GSI's work is the transformative potential of digital technologies and AI. GSI addresses critical challenges such as inequitable digital governance, lack of data privacy, and the risks posed by advanced AI systems, while exploring opportunities for human-centered innovation.

Introduction

Digital infrastructure is becoming the primary lever through which governments shape outcomes in the Artificial Intelligence (AI) era. For decades, this infrastructure was treated as a purely technical concern – a domain of cables, servers, and isolated IT departments. But as AI reshapes the fabric of information environments and redefines the relationship between the individual and the state, that era of passivity is coming to an end.

Today, the design of a national digital stack is a fundamental act of governance. Evidence drawn from consultations with 13 middle and emerging power governments reveals a growing consensus: robust digital infrastructure is no longer optional, and the rise of AI has made its deployment urgent. However, success in this era is not merely a technical achievement; it depends on the complex interplay of adoption, scale, and collaboration. The importance of digital infrastructure for governments reflects a growing recognition that control over data, identity, and interoperability is now central to economic competitiveness, state capacity, and public trust.

The transition from recognition to implementation depends first on adoption, which is never merely a function of technical availability but is deeply mediated by citizens' trust. These challenges vary significantly by context: skepticism toward opaque, centralized systems persists in high-literacy environments, while emerging economies face risks related to uninformed consent. Regardless of the setting, the underlying design imperative remains the same – convenience without credible controls breeds public backlash, while privacy without usability leads to abandonment. Neither failure is easily reversible, and today's infrastructure decisions will determine whether societies remain governable and resilient in an AI-mediated world.

This dynamic of trust directly impacts a government's ability to achieve scale, the point where political ambition meets operational reality. Interviews reveal that the barriers to scaling digital systems are rarely technical; they are institutional. Fragmentation across administration, rigid procurement frameworks, and the absence of mutualized infrastructure create obstacles that are often invisible during the pilot stage. Scaling is not simply an extension of a pilot project but a distinct governance challenge, meaning the countries that scale successfully are not necessarily those with the most resources, but those that design for expansion from the beginning.

Underpinning these domestic efforts is the need for structured collaboration, which remains the missing piece of the global digital puzzle. While regional frameworks provide necessary starting points,

the development of shared, open infrastructure remains nascent. The cost of isolation is high, resulting in duplicated investments, incompatible standards, and an increased dependence on a small number of dominant platforms. Conversely, the upside of collaboration is substantial, offering a path toward shared open-source components, mutualized costs, and a stronger collective voice in shaping global AI governance.

There is no universal model for building digital infrastructure, and the absence of a common framework is not a minor semantic gap. It complicates investment prioritisation, reform sequencing, and the articulation of a coherent long-term vision. Many governments are, in their own words, “building the plane while flying it”.

This report is written as a practical synthesis of government experiences. Drawing on in-depth interviews and targeted survey insights, it provides a comparative view of how countries are designing and deploying digital infrastructure in practice. Rather than recommending a single model, it surfaces patterns, trade-offs, and points of divergence that enable governments to learn from one another as part of an emerging community of practice.

It also identifies where cooperation is both necessary and feasible, and where strategic competition is likely to persist. In doing so, the report highlights the contours of a more coordinated approach among middle powers, that balances national priorities with shared interests. The aim is to support more informed decision-making and to advance pathways for building digital infrastructure that is credible, scalable, and collectively fit for the AI era.

Key Trends & Comparative Analysis

Across 13 governments on five continents, efforts to build digital infrastructure converge on a common set of constraints. While political systems, economies, and starting points differ, the gap between policy ambition and delivery is governed by a handful of institutional and social realities that manifest consistently.

Four patterns recur: institutional fragmentation, the critical interdependence of adoption and trust, the ongoing work of interoperability, and the financing models that ultimately sustain or constrain long-term infrastructure development.

The analysis draws on two complementary sources – in-depth interviews conducted with all 13 governments, which form the primary analytical foundation of this report, and a follow-up survey completed by a subset of seven governments. Survey findings are used selectively to illustrate or reinforce trends identified through the interviews.

Survey Snapshot: Digital Infrastructure Adoption and Implementation Barriers

Infrastructure Elements in Place	
Governments who reported having ____ as an existing digital infrastructure element in their country	
E-government services	8 out of 10
Sectoral registries	8 out of 10
National digital ID	6 out of 10
Digital payment systems	6 out of 10
Multi-purpose data exchange layers	5 out of 10
Public developer APIs / open data portals	5 out of 10
Survey Question: Which of the following digital infrastructure elements currently exist in your country?	
Barriers to Progress	
Governments who reported encountering ____ as a main challenge while advancing digital infrastructure	
Insufficient funding or investment	7 out of 10
Lack of inter-agency coordination	6 out of 10
Low public trust or engagement	5 out of 10
Political resistance or shifting priorities	5 out of 10
Limited technical capacity	2 out of 10

Survey Question: Which of the following challenges have you encountered in advancing digital infrastructure in your government?

**Survey Snapshot: Indicative findings from 10 of 13 governments that completed the quantitative follow-up survey. Interview findings across all 13 governments provide the primary analytical basis for this report. Results are not statistically representative and should be interpreted as directional insights only.*

Identifying and Addressing Institutional Fragmentation: How Governments Are Breaking Down Silos

Across all governments interviewed, addressing institutional fragmentation emerges as a consistent priority. Silos do not only constrain civil servants – they fragment the life-cycle of data itself.

When data cannot flow across administration, its value is diminished. Services go undelivered, inefficiencies compound, and citizens are often required to repeatedly provide information that governments already hold but cannot share. In response, governments are seeking more integrated, open, and collaborative approaches to digital infrastructure development.

Nearly half the countries in the sample have established centralised leadership through a dedicated digital ministry or interministerial directorate, while more than a quarter are using presidential or prime ministerial committees to force inter-departmental coordination and bypass traditional bureaucratic bottlenecks. While specific mechanisms differ, the direction is consistent – fragmentation is identified as a governance problem requiring institutional solutions, not a technical one requiring better systems.

How Governments Address Institutional Fragmentation

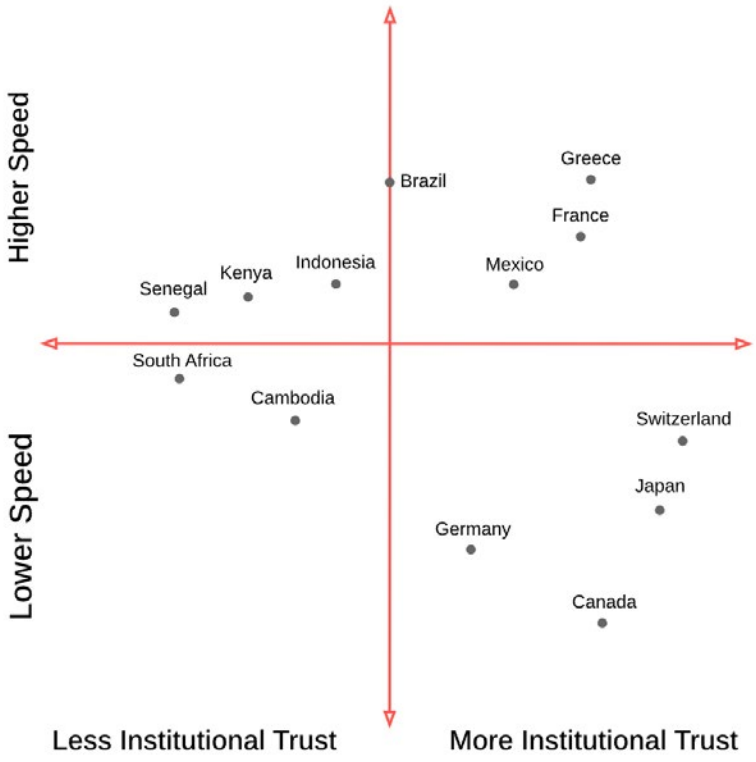
Coordination Strategy	Country Evidence
Centralised mandate or oversight body	**Senegal** routes all government IT projects through a single validation decree. **Greece** coordinates through Prime Minister Office oversight via an interoperability framework. **South Africa** convenes an inter-ministerial committee under the Presidency. Germany grants its new digital ministry veto power over other ministries' proposals. **Cambodia** is transitioning to a whole-of-government strategy through newly established committees. **Kenya** operates a whole-of-government approach with the Secretary to the Cabinet chairing the eCitizen Implementation Committee, spanning all relevant ministries and delivering over 22,000 services.
Networked coordination across ministries	**France**'s DINUM embeds correspondents in each ministry to coordinate open data, open source, and agile development. **Switzerland** works through interdepartmental groups and shared financing. **Brazil** convenes four ministries through an inter-ministerial committee.
Platform unification	**Mexico** replaced paper records across ministries with a unified "Digital File" and shared validation platform, eliminating duplication at source.
Persistent geographic fragmentation	**Canada**'s provinces lead independently, producing approximately 70 bespoke identity systems. **Indonesia**'s remote islands have sharply lower digital capacity than central agencies, the government is preparing a roadmap and strategy to tackle this issue. **Japan** is in the process of migrating 1,000+ local systems to the cloud which remains today an important interoperability challenge. **Switzerland** has set up interdepartmental groups and shared financing attempting to address the fragmentation from each federal office having their own strategy.

Findings are based on in-depth interviews conducted across all 13 governments in the sample. These qualitative insights form the primary analytical foundation of this report.

Adoption and Trust: The Design Imperative

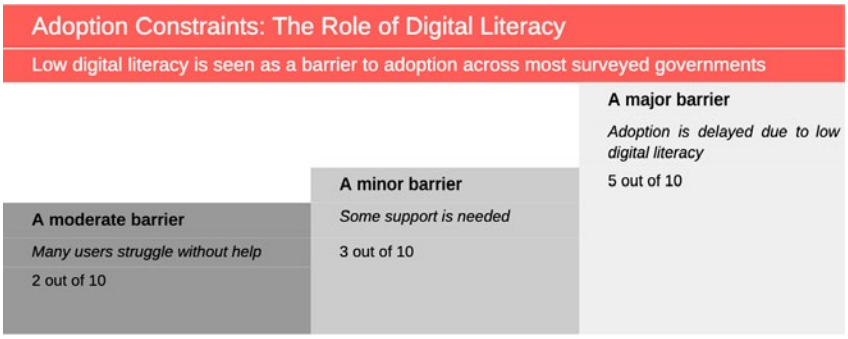
Interview findings reveal that adoption is never purely a function of technical quality – it is primarily mediated by trust.

The pattern varies by context but the underlying challenge is universal. In advanced economies with legacy infrastructure, skepticism toward centralized digital identity systems is a barrier to uptake. It can be inferred that citizens in these contexts demand higher transparency and auditability, before engaging with new government online platforms. On the other hand, in emerging economies without entrenched legacy systems, the need for digital public services is more acute and adoption has been faster, driven by strong demand for accessible public services and enabled by mobile-first infrastructure. However, speed carries its own risks – systems deployed with weaker guardrails from the outset risk future backlash and costly redesigns.



Findings are based on in-depth interviews conducted across all 13 governments in the sample. These qualitative insights form the primary analytical foundation of this report.

The design imperative is the same across both contexts – convenience without credible controls breeds long-term risks and backlash; privacy without usability breeds abandonment. Neither failure is easily reversible. The governments that have achieved sustained adoption at scale are those that designed their infrastructure with trust as a foundational priority from the outset. In both high-skepticism and high-adoption environments, the binding constraint is the same: the gap between the complexity of the systems being built and the capacity of citizens and institutions to engage with them meaningfully. Across the sample, digital literacy gaps persist on both sides of this divide – among citizens consenting to systems they do not fully understand, and among the government officials commissioning them.



Survey question: To what extent is a lack of digital literacy a barrier to citizen adoption of digital infrastructure in your country?

Infrastructure can scale: Key examples

FranceConnect processes 40 million authentications annually. Brazil's Pix payment system reached near-universal adoption within two years of launch. Japan's My Number card is held by over 80% of its 120 million citizens. Greece's Gov Wallet is used by nearly half of its total population and enables citizens to store and share official documents digitally.

**Adoption Constraints: Indicative findings from 10 of 13 governments that completed the quantitative follow-up survey. Interview findings across all 13 governments provide the primary analytical basis for this report. Results are not statistically representative and should be interpreted as directional insights only.*

Interoperability: Regional Progress, Global Gaps

Across the 13 governments interviewed, interoperability is universally recognized as a critical feature of digital infrastructure. Yet in practice, it is treated as an aspiration rather than a design principle – something to be achieved once national systems are built rather than embedded from the outset.

Where interoperability exists so far, it operates at the regional level rather than globally. While the Association of Southeast Asian Nations (Cambodia, Indonesia), the African Union (Kenya, South Africa, Senegal), and the European Union (France, Germany, Greece) have advanced interoperability within their own frameworks, cross-regional dialogue remains minimal.

Regional collaboration nonetheless emerges as a meaningful exception to this pattern. All three EU member states in the sample – France, Germany, and Greece – are aligning with common EU frameworks, particularly eIDAS and the EU Wallet, representing the most integrated infrastructure strategy observed across the 13 countries. Notably, the only two governments in the dataset that are actively co-developing shared technical components with foreign partners are both European, pointing to the EU's regulatory and political architecture as a rare enabler of genuine infrastructure convergence.

Interoperability in Practice: Coordinating Across Federal Systems

Switzerland illustrates the possibilities and limitations of interoperability in a federal system. Each federal office retains its own digital strategy, but coordination is achieved through interdepartmental working groups and shared financing mechanisms. The result is a pragmatic model – not unified architecture, but negotiated coherence. This model offers lessons for other federal or consensus-based systems where top-down harmonisation is politically challenging.

Financing Digital Infrastructure: Shared Approaches, Shared Vulnerabilities

Public-private partnership remains the dominant financing model, with over two thirds of the governments in the sample (Cambodia, Canada, Greece, Japan, Indonesia, Kenya, Senegal, South Africa, and Switzerland) each partnering with global hyperscalers for cloud and connectivity while attempting to retain data locally. Universal service obligation funds (USOs) – financial mechanisms designed to expand digital infrastructure and connectivity into rural or underserved areas – are an effective but exceptional alternative, notably in Senegal and Kenya.

The analysis highlights a series of shared strategies and vulnerabilities. Regardless of budget, governments consistently prioritize incremental proof-of-concept projects over comprehensive, large-scale overhauls. Similarly, investment remains strictly vertical; every country in the sample finances its own national stack rather than investing in shared horizontal layers. Consequently, each country bears the full cost of components that could otherwise be pooled, leaving them individually exposed to the pricing power of a few dominant providers. This lack of cross-border infrastructure investment becomes increasingly problematic as AI development demands compute power, data exchange, and interoperability at a scale that no middle power can sustain in isolation.

Financing Through Architecture: The Role of Open Source

Senegal shows how a lower-income middle power can build a financing strategy without complete hyperscaler dependency. By adopting Estonia's X-Road protocol rather than building a bespoke interoperability layer, Senegal turned an open-source platform into a financing decision, thereby cutting development costs while retaining sovereign control over its data architecture. A national USO channels telecommunications levies into public digital infrastructure. A centralized validation decree routes all government IT projects through a single approval body, preventing duplicated spending across ministries. This illustrates the potential open source as cost architecture, not just a procurement preference.

The Governance-Tech Nexus: Between Economic and Sovereignty Challenges

Governments are not merely building data layers; they are encoding rules, incentives, and social contracts that underpin their governance models into their digital stack. Whether a country chooses Estonia's X-Road model, a centralized ID, or a decentralized "use-case-first" approach, the choice is rarely purely technical. While dominant private sector players – hyperscalers – often treat governance as an afterthought often imposed by regulation, governments, on the other hand, increasingly approach digital infrastructure as a lever to translate governance models into technological pathways rather than as a purely technical challenge.

Governments are also using infrastructure to respond to systemic political challenges. Evidence drawn from government interviews suggests that two forces above all others have accelerated and defined digital infrastructure development in recent years:

1. The COVID-19 Pandemic which compressed timelines and forced delivery at scale under pressure. In Japan, it catalyzed the creation of the Digital Agency of Japan, in Greece to the digital vaccination certificates; in South Africa to the better delivering of the Social Relief of Distress grant; and in France it gave way to a sharper preoccupation with digital resilience and efficiency.

2. The rising imperative of digital sovereignty which has reoriented infrastructure decisions away from efficiency and toward resilience and control. This shift is most pronounced in Europe, where initiatives such as the Deutschland-Stack or the Commons European Digital Infrastructure Consortium (DC-EDIC) led by France, the Netherlands and Germany reflect infrastructure initiatives that have been preceded by political momentum.

Problem-Driven Design & Constitutional Guardrails

Kenya stands out as a compelling illustration of this nexus. Its approach is distinctly problem-driven – starting with what works, from M-Pesa to farmer registration, then scaling. However, beneath that pragmatism lies a clear governance logic: infrastructure choices are social contracts that must benefit citizens, not technical decisions. The Worldcoin controversy crystallized this most sharply, when a foreign company offered digital ID infrastructure in exchange for biometric data, the response was not merely regulatory, but a constitutional assertion of civil society's right to participate in every stage of the policy-making process.

Sovereignty Concerns and Motivations for Building National Digital Infrastructure

All countries interviewed face a common tension: how to retain control over critical infrastructure and data while reaching scale. More than half of the countries interviewed – including Brazil, France, Germany, Greece, Mexico, Senegal, and Switzerland – identify digital sovereignty, particularly reducing reliance on foreign technology providers, as a top strategic priority.

Approaches to this challenge generally fall into three categories:

- Sovereignty-first models in countries such as Germany, Indonesia, Senegal, and Switzerland ensure that sensitive data remains on domestic infrastructure.
- Hybrid strategies, utilized in Brazil, Cambodia, Canada, Greece, Japan, and Kenya, balance partnerships with global hyperscalers against localized hosting and skills transfer.
- State-built alternatives such as in France, Mexico, and South Africa involve building national infrastructure from the ground up. These models often favor open-source tools to reclaim technical capacity and eliminate vendor lock-in.

Economic Drivers and Dependencies

Alongside sovereignty, the governments interviewed all face a parallel economic challenge: delivering meaningful public benefits while managing current deep dependencies on dominant technology platforms and hyperscalers. While the economic rationale is a universal factor, the logic varies depending on a country's level of connectivity, inequality, and market development.

Two distinct economic logics emerge from the interviews:

- Connectivity as foundational infrastructure: Investment targets populations and geographies excluded from the digital economy – areas where private markets have not reached – serving as a precondition for economic participation (Indonesia, Kenya, Senegal, South Africa)
- Infrastructure for competitiveness and resilience: Leveraging digital infrastructure for economic positioning, whether through problem-solving at scale or industrial capacity, ensuring that gains from digitalization accrue domestically (Brazil, France, Japan, Mexico, Switzerland)

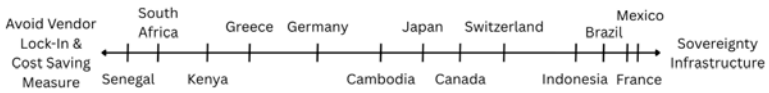
These logics are not mutually exclusive. Five of the 13 countries interviewed – Indonesia, Kenya, Mexico, Senegal, and South Africa – are pursuing "full-stack" developments, building connectivity, identity, and service layers simultaneously. Across context, the underlying challenge remains the same – delivering high-quality public services while operating within a market whose terms are often set by dominant platforms whose commercial interests do not always align with public ones.

Open Source: From Procurement Tool to Sovereignty Architecture

Roughly one third of countries interviewed have implemented either a strict mandate or a strong legal preference for open source code. Motivations vary from procurement strategy mostly aimed at avoiding vendor lock-in to building a sovereign infrastructure ensuring public ownership of digital public goods.

Open Source Adoption Spectrum: From Procurement to Sovereignty

How governments use open source, from reducing costs to building sovereign digital systems.



Evidence from interviews, supported by survey input and comparative case analysis, reveals a spectrum of motivations for open source adoption – from pragmatic cost-saving to principled sovereign infrastructure. Countries like Senegal and South Africa adopt open source primarily to avoid vendor lock-in and reduce costs by deploying proven solutions like X-Road and Modular Open Source Identity Platform (MOSIP). Further along, Greece, Cambodia, and Japan treat open source as one technical solution among others. At the sovereignty end, Indonesia, Brazil, France, and Mexico have institutionalized open source as a strategic infrastructure principle, mandating “public code”, building in-house, and leveraging open foundations to retain domestic control at scale.

Public Money, Public Code in Practice

Mexico provides a clear example of the "public money, public code" principle. By law, every line of code developed by its Ministry of Digital Transformation is open source, ensuring that publicly funded projects remain public assets shared across all levels of government. This stack is maintained in-house by approximately 300 civil servant developers, transforming the national digital identity and citizen "digital file" into sovereign infrastructure rather than a vendor-dependent service. In this context, open source is not merely a procurement preference; it is the architecture of public ownership.

Findings are based primarily on in-depth interviews conducted across all 13 governments in the sample, complemented by survey responses from 10 governments. Qualitative insights form the primary analytical foundation, while survey data provides directional support.

Open source is perceived as a leapfrog mechanism for countries seeking rapid modernization. Nearly a quarter of the countries interviewed, including Cambodia, Senegal, and South Africa, are piloting or adopting Estonia’s X-Road protocol or India’s MOSIP as a foundational data interoperability layer. For these countries, open source is not merely a cost saving measure, it is the fastest path to building sovereign infrastructure without building from scratch.

Strategic Implications for the AI Era

A country's data architecture dictates its AI trajectory. Nearly half of the governments interviewed are actively drafting or finalizing national AI policies that explicitly link AI readiness to their foundational data architecture, including Brazil, Germany, Greece, Japan, Kenya, and South Africa. However, at this stage, only 2 countries, Germany and Greece, have explicitly proposed modular "building block" architectures to ensure AI services can be developed using shared national infrastructure. Most governments interviewed report managing digital infrastructure and AI stack efforts separately, but many say they are actively moving from separate to integrated approaches.

That gap – between policy ambition and architectural readiness – is the central finding of this section. Nearly half of the governments in the sample are actively connecting AI strategy to data infrastructure in their policy frameworks, yet only two have translated that connection into a concrete modular design. The rest are, in effect, writing AI strategies on top of infrastructure that was not designed for AI. This is a structural mismatch that, if left unaddressed, will constrain the range of AI applications governments can deploy, the degree of sovereignty they can exercise over those applications, and the public trust they can sustain.

Three strategic imperatives emerge from the evidence. First, that national resilience in the AI era begins not with regulating models but with securing citizen data agency – and that data agency, in turn, depends on digital literacy at a scale most governments have not yet attempted. Second, that no middle power can build sovereign AI capacity alone, making open infrastructure collaboration not an ideological preference but a strategic necessity. Third, that the window for architectural intervention is narrow: the infrastructure decisions governments make in the next two to three years will determine whether their societies enter the AI era as informed participants or as passive consumers of systems designed elsewhere, for purposes that may not align with the public interest.

National Resilience Starts with Data Agency

The AI era is redefining what infrastructure sovereignty means. Where the previous decade's digital infrastructure strategy approaches centered on data storage and cross-border data flows, the more consequential question today is who controls the information space itself – the models, interfaces, and algorithmic layers through which citizens increasingly perceive and interpret the world.

This shift raises urgent stakes for democratic resilience. Large language models (LLMs) are not neutral systems; they mediate how citizens are informed, and increasingly shape how they reason, and what they trust. In this context, restoring meaningful sovereignty over digital infrastructure begins with genuine citizen control over their data – but extends well beyond it. This is not merely a privacy objective. It is a structural defense against a "single point of failure". When a country's information ecosystem runs on opaque, closed systems governed

primarily by corporate profit imperatives, it creates a structural single point of failure – regardless of where those systems originate.

Resilience, in this sense, is not built through restriction alone. It is built through architecture: infrastructure that is distributed, transparent, and governed in the public interest creates no single lever to pull, no single dependency to exploit.

Yet infrastructure alone cannot close the sovereignty gap.

The data underscores this point sharply. Over one third of countries in the sample identify a significant digital literacy gap within their own government administrations – not just among citizens, but among the officials responsible for designing and procuring the systems that will mediate public life. Canada, Germany, Japan, Kenya, and South Africa all report this as a binding constraint. When the people building the infrastructure do not fully understand the systems they are commissioning, sovereignty becomes nominal rather than substantive. The risk is not merely inefficiency; it is that governments become sophisticated purchasers of dependency rather than architects of autonomy.

Meanwhile, approximately a quarter of countries in the sample report that their citizens currently prioritize convenience over privacy, leading to rapid adoption of digital services despite low understanding of the underlying data architecture. Brazil, Cambodia, Indonesia, and Kenya all exhibit this pattern. In an AI-mediated environment, this creates a particular vulnerability: citizens may consent to systems whose implications they cannot evaluate, while governments may lack the technical capacity to audit them. The convergence of low citizen literacy and low institutional literacy could materialize into a governance crisis.

Data agency, then, is not a downstream benefit of good infrastructure. It is a precondition for it. Without informed citizens who can meaningfully exercise choice over how their data is collected, processed, and used – and without public officials who can evaluate the systems they are building – even the most technically sound architecture will fail to deliver on its democratic promise. Elevating digital literacy from a "nice to have" to a core pillar of national security and economic resilience is no longer aspirational. It is operationally urgent.

Global Resilience Starts with Open Infrastructure Collaboration

None of the 13 countries interviewed is building its AI future in isolation, nor could it. The computational resources, foundational models, and technical expertise required to develop sovereign AI capabilities exceed what any single middle power government can realistically assemble alone. International reliance is therefore a structural feature of the current AI landscape rather than a failure of ambition.

In this context, interoperable and open frameworks are essential. They enable countries to develop shared AI capabilities without surrendering control over the data, governance, and decision-making that underpin them. They allow middle powers to pool resources, align on standards, and develop "Sovereign AI". This does not mean full self-sufficiency, but instead a cooperative architecture where countries retain meaningful agency within a system that is not dominated by a single provider or power.

The evidence from this study suggests that the preconditions for such collaboration are unevenly distributed but not absent. The EU member states in the sample – France, Germany, and Greece – represent the most advanced model of cross-border infrastructure convergence observed, driven by regulatory alignment through electronic Identification, Authentication and Trust Services (eIDAS) and the EU Wallet, and by joint initiatives such as the recently launched Digital Commons European Digital Infrastructure Consortium (DC-EDIC) consortium. Notably, the only three governments in the dataset (France, Germany and Greece) actively co-developing shared technical components with foreign partners are both European, suggesting that political and regulatory architecture – not just technical ambition – is the decisive enabler of genuine infrastructure convergence.

Outside Europe, collaboration remains largely regional and protocol-based. The Association of Southeast Asian Nations (ASEAN) and African Union (AU) member states in the sample operate in separate tracks with minimal cross-regional interoperability dialogue. While the adoption of shared open-source protocols – such as X-Road and MOSIP in countries like Cambodia, Senegal, and South Africa – demonstrates that open standards can serve as a bridge across development contexts, so far, these remain point solutions rather than elements of a coordinated strategy. The current landscape is one of parallel pilots and experiments, not convergent architecture.

This is both a risk and an opportunity. The risk is that middle powers, acting individually, will continue to finance infrastructure vertically – national stacks built in isolation – rather than investing horizontally in shared layers that could reduce costs, increase resilience, and strengthen collective leverage in global AI governance. The opportunity is that the very countries in this sample – with their democratic governance frameworks, significant research capacity, and growing political alignment around digital sovereignty – are precisely positioned to pioneer a new model of shared infrastructure demanded by the current geopolitical environment. Governments interviewed identify two equally pressing motivations for building an open and common AI stack: reducing dependence on global hyperscalers, and improving interoperability with like-minded partners. The central challenge remains whether they will organize to do so before the architecture of the AI era is set by other actors.

Japan's Approach to Adopting an Open and Common AI Stack with Allies

Japan Ministry of Economy, Trade and Industry developed the report "Toward the Second Revision of the Action Plan for Strengthening the Industrial and Technological Base for Economic Security" which warns of "the risk of losing Japan's autonomy and indispensability due to major powers establishing dominant positions in the AI domain." while acknowledging that "it is not realistic for Japan to immediately catch up with others in the field of general-purpose AI". Open-source and open-weight models are emphasised in Japan's "AI Basic Plan" as means to reduce structural dependence by diversifying and domesticating the AI stack through allied cooperation.

Building Together: Key Takeaways and Way Forward

The 13 governments in this study occupy a unique position in the global order. They are neither the architects of dominant AI platforms nor passive recipients of technologies designed elsewhere. They are middle and emerging powers with the capacity to shape how digital infrastructure evolves in the AI era. Yet today, they are building similar systems, solving the same problems, and doing so largely in isolation. No country interviewed sees full-stack sovereignty as achievable, and only few are willing to accept long-term reliance on external dominant platforms. As AI becomes embedded in public services and information environments, fragmented infrastructure reduces leverage, increases dependency, and constrains governments' ability to shape outcomes.

The primary constraint is coordination, not ambition. The core building blocks of digital infrastructure are converging in form but not in approach. Systems are financed and developed vertically, with limited mechanisms to scale successful models across borders. Interoperability remains an aspiration, not a design principle embedded from the outset. The current model carries increasing costs, including duplicated investment, incompatible standards, and structural dependence on a small number of providers.

If AI-ready infrastructure cannot be built by any single country alone, and if vertical national investments continue to produce fragmented, incompatible systems, the logical response is to define a minimum viable set of shared infrastructure components that middle powers could co-develop and co-govern.

The evidence from this study points toward three interlocking pillars.

Technology: shared open layers, not shared systems. Convergence is most achievable at the protocol and standards layer, not at the application layer. The adoption of X-Road and MOSIP across diverse governance contexts demonstrates that open interoperability protocols can bridge radically different national architectures without requiring harmonization of domestic systems A minimum viable shared infrastructure would prioritize common data exchange protocols to enable cross-border interoperability, shared identity verification standards allowing citizens to authenticate across jurisdictions, and open-source AI auditing tools that allow governments to assess models regardless of origin. The design principle is modularity, featuring shared components that can be adopted incrementally, adapted locally, and governed collectively.

Policy: mutual recognition over harmonisation. Full regulatory harmonization across 13 diverse governance contexts is neither realistic nor desirable. What is achievable is mutual recognition through agreements that allow systems built under different regulatory frameworks to interoperate on the basis of shared minimum standards. For middle powers, this means developing a common policy floor for data governance, algorithmic transparency, and cross-border data flows that preserves national regulatory autonomy while enabling technical interoperability. It also means building shared capacity for AI governance. Over one third of countries in this sample identify a significant digital literacy gap within their own government administrations. Without institutional capacity to understand, evaluate, and govern AI systems, even well-designed policy frameworks will remain aspirational.

Capital: horizontal financing for shared layers. Most countries in this sample are financing digital infrastructure vertically, investing in national stacks rather than shared layers. Each country currently bears the full cost of developing components that could be pooled, while remaining individually exposed to the pricing power of a handful of dominant providers. A shift toward horizontal financing – through pooled investment in shared open-source components, mutualized compute capacity, and joint R&D on interoperability standards – would reduce per-country costs, distribute risk, and create collective leverage that no middle power can generate alone. Existing models offer precedent: USO funds in Kenya and Senegal demonstrate that public financing instruments can be repurposed for infrastructure investment; and the DC-EDIC consortium in Europe shows that pooled sovereign investment is politically achievable. The task is to extend these models beyond their current regional boundaries.

Finally, underpinning all three pillars is a fourth requirement: collaboration. The 13 governments in this sample – along with the institutions, private sector partners, and civil society organisations that support them – represent a critical mass of democratic middle and emerging powers with aligned interests in open, transparent, and citizen-centric digital infrastructure. Convergence does not require uniform systems; it requires alignment at the level of components, including interoperable protocols, open standards, and modular building blocks that enable countries to scale collectively while retaining control over domestic implementation.

The question is no longer whether a shared infrastructure layer is needed. It is whether middle and emerging powers can organize to build it before the architecture of the AI era is set elsewhere.