THE DEPENDENCY ECONOMY OF AI

What 25 national AI strategies reveal about the reality of sovereignty.

The playbook enterprise leaders need to drive their digital resilience

By Damien Kopp

THINK-DO-TANK
DIGITAL NEW DEAL

February 2026

AI IS NO LONGER JUST A TECHNOLOGY: IT HAS BECOME A GEOPOLITICAL SUPPLY CHAIN

FOREWORD

For several years, our think tank has been working on a key concept: strategic autonomy. In a first cycle of publications devoted to "Trusted Digital"*, we transposed to the digital domain an essential Gaullist principle, valid as much for energy as for defense: **autonomy does not exclude alliances**. The objective is neither autarky nor the denial of interdependencies; on the contrary, it is to map them, prioritize them, and **master them within ecosystems of trust, so as to choose one's alliances rather than be subjected to them**.

We are now opening a **new cycle**, "Digital Resilience," based on a simple observation: what cannot be measured cannot be governed. The challenge is therefore no longer merely conceptual, but fully operational. The aim is to equip both public and private organizations with a **comprehensive, cross-cutting, and fact-based view of their digital dependencies**—an indispensable condition for coordinating action, arbitrating technological choices, and regaining control over their digital destiny.

This cycle opens with an initial report dedicated to artificial intelligence (AI), which has become both a **critical economic value chain and a strategic geopolitical infrastructure**. To move beyond exclusively European analytical frameworks, we chose a **deliberately international perspective** by entrusting this study to an author based in Singapore. Built on a **global benchmark** of national strategies, his work highlights the dependency models at play and identifies concrete options for governance and coordination for both public and private stakeholders.

By making digital dependencies measurable, comparable, and subject to arbitration, this report makes it possible to **move beyond what we describe as "voluntary digital servitude,"** in favor of a clear-eyed and realistic analytical framework. For decision-makers, the message is clear: AI can no longer be treated as a mere IT issue. It must be understood as a business continuity challenge, on a par with energy, raising the same structural questions of security of supply, risk management, cost volatility, and, ultimately, operational resilience.

Damien Kopp thus invites us to undertake a fundamental shift in perspective: to stop viewing dependencies as a failure of sovereignty, and instead to recognize them as a reality to be managed in a resilient manner.

Arno Pons, Digital New Deal

SUMMARY

AI SOVEREIGNTY HAVE MOVED FROM ABSTRACT POLICY DEBATES TO A CONCRETE BUSINESS RISK.

INTRODUCTION

Digital and AI sovereignty have moved from abstract policy debates to a concrete business risk. Despite massive investments in "sovereign AI", most countries and enterprises are becoming **more dependent** on a narrow set of foreign suppliers for GPUs, cloud infrastructure and frontier models. This creates a **sovereignty paradox**: the pursuit of autonomy is built on borrowed technology, increasing geopolitical exposure, vendor lock-in and operational fragility.

An analysis of **25 national AI strategies** shows that **true full-stack sovereignty is largely limited to the United States and China**. Most other nations operate within a **managed dependency economy**, making trade-offs between speed, control and resilience.

- **Asia** pursues diverse paths: China and South Korea invest in full-stack control, while India and Singapore follow *open-yet-local* models focused on linguistic inclusion.
- **Europe** emphasizes regulatory sovereignty, but remains structurally dependent on foreign hardware and cloud platforms.

Three structural forces now shape AI competitiveness and risk for enterprises:

1. **GPU and compute concentration**, the primary chokepoint;
2. **Energy availability**, increasingly a strategic advantage;
3. **Linguistic and cultural alignment**, reshaping market access through multilingual AI ecosystems.

Yet most organizations are unprepared. Only **15% treat AI sovereignty as a CEO or board-level issue**[1]. When addressed, motivations are mostly defensive (compliance, data control), not strategic value creation. Meanwhile, AI has become a **geopolitically exposed digital supply chain**, where disruptions—export controls, energy shocks, supplier failures—can directly threaten business continuity.

Enterprises must therefore shift perspective: **sovereignty is not about independence, but resilience**. This requires model-agnostic architectures, diversified cloud strategies, localized control over data and models, and systematic mapping of dependencies. AI models should be treated as **strategic assets**, stress-tested against geopolitical and operational shocks.

To support this shift, the paper introduces an **AI Resilience Framework** and a **Digital Resilience Index (DRI)**, designed to make dependencies visible and actionable at enterprise level

The core question is no longer "Are we sovereign?" but "Where are we dependent—and are we prepared to act when those dependencies break?"

In the age of AI, sovereignty means the capacity to adapt, pivot and continue operating when it matters most.

Damien Kopp

Managing Director, RebootUp
Founder, KoncentriK

1 A Sovereign AI: From Managing Risk to Accelerating Growth , Accenture, november 2025

EXECUTIVE SUMMARY

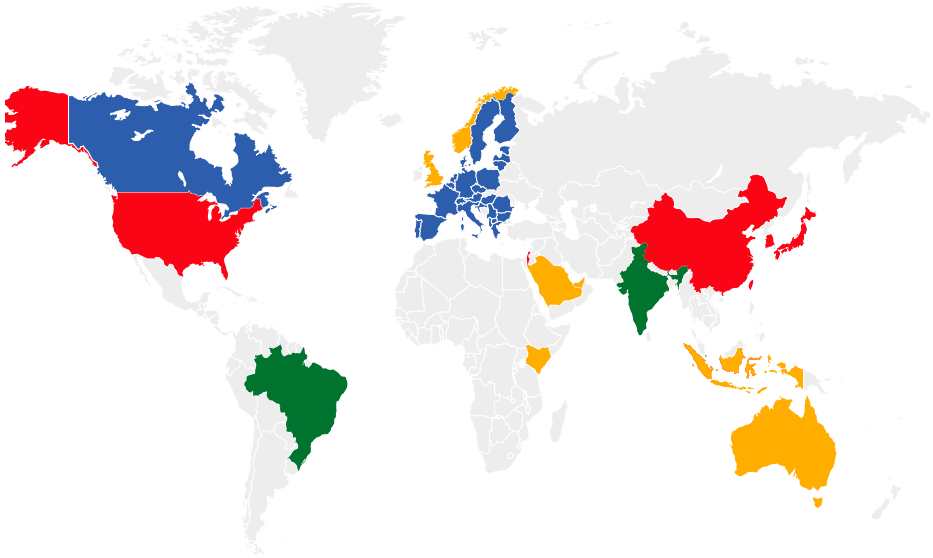
→ This report demonstrates a now undeniable reality: **sovereignty in AI is largely illusory**. This comparative analysis of 25 national AI strategies shows that the vast majority of countries, including those explicitly pursuing "sovereignty », remain structurally dependent on a very limited set of critical chokepoints, notably GPUs, cloud infrastructure, energy, and models.

The report identifies four major national archetypes, each reflecting deliberate trade-offs between speed, control, cost, and autonomy.

No model fully escapes dependency, but some manage it strategically, while others are subjected to it.

NATIONAL ARCHETYPE CORE LOGIC OF AUTONOMY	PRIMARY TRADE-OFF OPTIMIZED FOR	MAIN DEPENDENCIES	AVERAGE DEPENDENCY SCORE (/40)
FULL-STACK Structural technological autonomy	***Autonomy vs. costs*** *(long-term sovereignty, structural resilience)*	Imported raw materials, key tools (e.g. ASML)	≈ 30 (24 à 36)
REGULATORY Autonomy through law and governance	***Control vs. autonomy*** *(regulatory control)*	Hardware, models	≈ 26 (24 à 28)
OPEN-LOCAL Autonomy through usage and data	***Inclusion vs. autonomy*** *(linguistic coverage, social impact)*	Imported GPUs, foreign technological base	≈ 22 (19 à 24)
PARTNERSHIP Autonomy delegated to partnerships	***Speed vs. autonomy*** *(rapid capacity and scaling)*	Semiconductors, cloud, models	≈ 22 (16 à 25)

GLOBAL MAP OF NATIONAL STRATEGIC ARCHETYPES



WHICH STRATEGY SHOULD EUROPE ADOPT?

THE "THIRD DIGITAL WAY"

At a minimum, Europe must secure its strategic autonomy across a limited set of key layers: model and data governance, interoperability, and minimum computing or inference capacities. The objective is not to own the entire digital stack, but to avoid the most damaging forms of dependency—particularly cognitive, cultural, and operational lock-in. This "third digital path" is likely to emerge at the intersection of two complementary archetypes:

- **A robust regulatory framework**, anchored in the rule of law, to build trust *(Archetype 2: regulatory sovereignty)*
- **Combined with control over critical use cases and sectoral value chains** *(Archetype 4: "Open-but-Local")*

FULL RESILIENCE STACK

At a maximum level, Europe could aim for "full-stack" strategic autonomy, as **the study shows that Europe's lag is not structural, but organizational:**

- if Europe were to genuinely unify its forces, it would move from 28 to 34;
- and if it were to pool its investments in the "hard" layers (semiconductors, as Japan has done), Europe would reach parity with the United States and China (36 out of 40).

Full sovereignty over the AI value chain may be illusory, but **if Europe were to overcome its fragmentation, strategic autonomy would truly be within reach.**

KEY RECOMMENDATIONS

For companies and public decision-makers alike:

1. **Treat AI as a strategic business continuity risk,** on a par with energy and critical supply chains.
2. **Make dependencies visible and measurable** through dedicated tools such as the Digital Resilience Index (DRI), in order to prioritize investments where disruption would have the greatest impact.
3. **Design resilience by design:** technology-agnostic architectures, supplier diversification, exit capabilities, and local control over data and models.
4. **Elevate AI governance to board level,** fully integrating geopolitical, energy, and industrial dimensions.

→ **The core lesson:** AI is no longer merely a technology, but a geopolitical supply chain, comparable to energy. The central strategic question is therefore no longer *"Are we sovereign?"* but rather *"Where are we dependent, and do we have a strategy in the event of a shock?"* To support this shift, the report presents an **AI Resilience Framework and a Digital Resilience Index (DRI)**, designed to make dependencies visible and actionable at the enterprise level.

WHY DEPENDENCIES MATTERS FOR BUSINESSES

Digital infrastructure now constitutes the very foundation of any business. AI algorithms, for their part, are now infiltrating every business process: to automate, optimize, recommend, decide or reinvent.

As a result, the dependencies embedded in this infrastructure now directly shape **business continuity, security and competitiveness.**

Technology is **no longer neutral**. The hardware, networks and models companies depend on are concentrated in the hands of a few firms and increasingly tied to geopolitical interests. Semiconductors, compute capacity, cloud regions and model access have become instruments of state power, subject to export controls, industrial policy and strategic competition.

In response, countries are developing **national AI strategies** to assert or regain a measure of control over their digital stack. These efforts vary widely. Some focus on sovereign cloud governance. Others prioritise domestic model development. Others invest in compute, energy or semiconductor capabilities.

This paper analyses 25 such strategies and evaluates them through an AI Resilience Framework built around eight structural dependencies.

For organisations operating across these jurisdictions, these national choices have **direct implications**.

They create **systemic fragility** and redefine the **risk surface** in ways that go far beyond privacy, security or compliance: jurisdictional exposure through foreign cloud providers, reliance on a limited set of model APIs, vulnerability to export controls, cognitive standardisation across a few dominant AI model architectures, and dependencies on energy and compute capacity that companies do not control.

These risks influence how you build, how you scale, and how resilient your operations remain when external conditions shift.

Boards and executives must now integrate these technopolitical constraints into **Governance, Risk** and **Compliance** frameworks.

This interconnected web of national AI strategies, often anchored in a **small number of dominant technology suppliers**, creates both significant risks and new strategic considerations for global enterprises.

Boards need clear visibility into where their infrastructure is physically hosted, who controls the chip and compute supply chain behind their systems, how dependent they are on specific model providers, and what would happen if any part of that pipeline were disrupted by sanctions, export controls, regulatory shifts, geopolitical tension or vendor deprecation.

Sovereignty, in this context, is **not about identity or isolation**. It is about control over the dependencies that matter most for **operational continuity** and **strategic**

freedom. No organisation can decouple fully, but every organisation can make deliberate choices about **which dependencies are acceptable and which require mitigation.**

> *What matters is the nature of your dependencies and your ability to absorb shocks to ensure sustainable operational resilience.*

Sovereignty is built through deliberate architectural decisions, long-term investment, and continuous review of where you rely on others and why.

KEY FINDINGS

HERE IS WHAT THE ANALYSIS OF 25 NATIONAL INITIATIVES REVEALS:

→ **SOVEREIGNTY CLAIMS EXCEED ACTUAL AUTONOMY**
Most national "sovereign AI" programmes depend heavily on foreign technology at critical layers.

→ **THE CHIP LAYER DOMINATES EVERY SOVEREIGNTY MODEL**
Without independence on advanced computing, everything else is superficial.

→ **ENERGY IS BECOMING THE NEW GEOPOLITICAL MOAT**
Norway, Saudi Arabia and the UAE are using energy abundance to buy compute advantage.

→ **LANGUAGE IS BECOMING A COMPETITIVE ADVANTAGE**
India, Spain, Singapore and Mexico use linguistic sovereignty as a strategic differentiator (SEA-LION, ALIA, Jais, ...).

→ **REGULATION IS EUROPE'S MAIN LEVERAGE**
Not technology or innovation (yet).

→ **PARALLEL ECOSYSTEMS ARE NOW PERMANENT**
The US and China are building separate stacks in the name of autonomy and strategic dominance.

→ **DEPENDENCIES ARE IRREVERSIBLE WITHOUT AN INTENTIONAL, LONG TERM STRATEGY**
Short-term partnerships create long-term lock-in that requires deliberate intervention to escape.

STRATEGIC IMPERATIVES: AN AI RESILIENCE PLAYBOOK FOR ENTERPRISE LEADERS

AI can no longer be governed as a single technology. It must be managed as a **geopolitically exposed digital supply chain** spanning chips, compute, cloud, models, and data flows.

The goal is not perfect sovereignty but **operational resilience**: the ability to continue operating when vendors, jurisdictions, or conditions shift.

To help enterprises act concretely, this paper introduces **two complementary tools:**

- **The AI Resilience Playbook** – how organisations should act
- **The Digital Resilience Index (DRI)** – how organisations should measure and prioritise exposure

Together, they provide a practical, board-usable framework

THE AI RESILIENCE PLAYBOOK: WHAT COMPANIES MUST DO NOW

#1 MAP: DEPENDENCY INVENTORY

Create a unified view of your dependencies across hardware, cloud, network, models, and data. Treat each dependency as an analysis unit with metadata: jurisdiction, vendor, failover path, and operational criticality.

#2 ASSESS: QUANTIFY EXPOSURE

Score your exposure based on where inference and training run today, who controls the GPUs, which laws apply, and how quickly a disruption would propagate. Use structured scenarios to understand failure paths.

#3 STRESS-TEST: SCENARIOS AND DRILLS

Conduct tabletop exercises for realistic disruptions: API rate limits, model withdrawal, cloud region outages, export-control shocks, or energy shortages. Identify single points of failure in each workflow.

#4 PLAN: RESILIENCE BY DESIGN

Translate findings into a funded roadmap using architectural, contractual, and organisational levers. Prioritise model optionality, cloud diversification, and local inference capabilities.

#5 MONITOR: TRACK KEY INDICATORS

Establish key risk indicators (KRIs) such as GPU supply constraints, vendor policy shifts, new export regulations, and latency trends. Review mitigation status quarterly.

#6 GOVERN: MODERNIZE GRC

Update Governance, Risk and Compliance frameworks to treat **geopolitics, infrastructure dependence, and vendor concentration** as core enterprise risks. This must become a board-level oversight item, not an IT concern.

To help companies operationalize the principles of the AI Resilience Playbook, we introduce here the Digital Resilience Index (DRI).

DIGITAL RESILIENCE INDEX (DRI): MEASURING WHAT WILL BREAK FIRST

The **Digital Resilience Index** (DRI) operationalises the Playbook and helps inform where to apply it first. It is a **diagnostic and prioritisation tool** that allows organisations to score exposure across critical dimensions, compare business units, regions, or architectures and focus investment where failure impact is highest.

The DRI is built around eight pillars, initially developed for companies operating within the European regulatory and investment landscape —- but easily extendable and applicable to companies globally —- providing a structured tool for identifying and mitigating technology dependencies.

DIGITAL RESILIENCE INITIATIVE

The **Digital Resilience Initiative** aims to provide **free, transparent, and scientifically rigorous assessment compass** to help organizations identify their vulnerabilities and regain control over their digital infrastructure.

This index is carried by the **association for the Digital Resilience Initiative (aDRI)**, a non-profit organization responsible for developing, governing, and evolving this market standard, as well as orchestrating its ecosystem. The methodology and reference framework are **fully public and auditable by all**. The reference framework and its methodology are released under a **Creative Commons license (CC BY-NC-ND)**.

The initiative was designed by its three founders — **David Djaïz** (Ascend Partners), **Yann Lechelle** (Sens Digital), and **Arno Pons** (Digital New Deal) — to become a **catalytic instrument**, giving industries the means to break away from imposed dependencies and to **reclaim their strategic autonomy**.

Olivier Sichel (Chief Executive Officer of the Caisse des Dépôts, founder of Digital New Deal) serves as **Honorary President** of the association.

THE EIGHT PILLARS OF THE DIGITAL RESILIENCE INDEX

Each pillar represents a **distinct failure mode** under external pressure.

PILLAR	FOCUS AREA	DESCRIPTION
RES-1	STRATEGIC AUTHORITY	Strategic decision-making authority within the EU, protections against changes of control, European funding sources, local investments, commitment to EU open source initiatives, and operational resilience against potential disruptions.
RES-2	REGULATORY & COMPLIANCE	National legal system governing operations, exposure to non-EU extraterritorial laws, access channels constrained by foreign authorities, applicable international regimes, intellectual property jurisdiction, and contractual negotiation power.
RES-3	DATA & AI CONTROL	Exclusive cryptographic control by the client, complete traceability of access and use of AI models, strict confinement of storage in Europe, governance of AI pipelines under EU control, resilient internal development of innovative technologies.
RES-4	OPERATIONAL AUTONOMY	Ease of migration without vendor lock-in, capacity for autonomous management by European operators, availability of a pool of qualified EU talent, operational support based exclusively in the EU, complete access to technical documentation and source code.
RES-5	TECHNOLOGY SUPPLY CHAIN	Geographic origin of critical physical components and manufacturing sites, jurisdiction and origin of code embedded in hardware and firmware, location of software development and update governance, degree of dependence on non-EU suppliers, complete visibility and traceability of the subcontracting chain with audit rights.
RES-6	TECHNOLOGICAL INTEGRATION	Capacity via documented and non-proprietary APIs, adherence to widely adopted public standards, software accessibility under open licenses allowing audit and modification, architectural transparency including data flows and dependencies, European independence in high-performance computing.
RES-7	SECURITY	Recognized European and international certifications, strict compliance with GDPR, NIS2, DORA, security operations centers under exclusive EU jurisdiction, transparent reporting of violations in accordance with European frameworks, autonomy in maintaining security patches, complete independent audit capacity, continuous personnel training, detection and remediation of non-referenced tools (shadow IT).

→ Application: Use these 8 dimensions to audit your current AI stack.

RISK-BASED STRATEGIC ACTIONS: APPLYING RESILIENCE WHERE IT MATTERS MOST

The following strategic actions are categorized by **the nature of the risk they mitigate** to build robust resilience in a fragmented AI environment.

1. Digital Supply-Chain Risk (Vendor Lock-in & Component Vulnerability)

This category addresses the fragility created by reliance on a small set of foreign suppliers for core AI components (chips, models, cloud platforms).

Focus is on *Operational Autonomy (RES-4)*, *Technology Supply Chain (RES-5)* and *Technological Integration (RES-6).*

Model Independence & Optionality

- Avoid proprietary lock-in by adopting model-agnostic architectures (combining public APIs, open-source, and regional models).
- Maintain at least three classes of models for critical workflows.
- Ensure every critical workflow has a hot-swappable model fallback to mitigate risk from providers changing pricing, throttling requests, or discontinuing endpoints.

Enterprise Model Supply Chain

- Govern models like a critical supply chain. Maintain a controlled registry of all models (internal, open, commercial).
- Track upstream dependencies and implement SBOM-style transparency for AI: Model Bills of Materials (MBOMs).
- Conduct red-teaming and failure-mode testing across all models.

Mitigate Vendor Leverage

- Implement Vendor Resilience Audits against all suppliers. Force contractual Service Level Agreements (SLAs) on API continuity and version sunset timelines.
- Build Symmetric Bargaining Power through a multi-vendor strategy and leverage open-source adoption as a negotiation tool.

REAL-WORLD EXAMPLE:
VMWARE LICENSING SHOCK HITS TESCO

What happened: After Broadcom acquired VMware in 2023, it discontinued support for Tesco's perpetual licenses and forced migration to new subscription bundles. VMware virtualisation underpins ~40,000 server workloads connecting to tills and store systems across UK and Ireland.

Business impact: Tesco filed suit claiming at least £100M in damages, warning that loss of VMware support could disrupt core operations including grocery supply. The case remains in litigation as of late 2025.

DRI dimension exposed: Operational Autonomy (RES-4) – inability to migrate without vendor permission; Technology Supply Chain (RES-5) – tier-0 dependency on a single provider.

How these actions would have helped: Pre-negotiated change protections in contracts (support-term continuity, deprecation windows) combined with infrastructure-as-code abstractions would have enabled workload re-platforming without wholesale rewrites, reducing Broadcom's leverage.

2. Legal & Jurisdictional Risk (Data Exposure & Regulatory Control)

This category addresses the legal exposure and loss of control over data and compute that fall under foreign jurisdiction.

Focus is on *Regulatory & Jurisdictional* Control (RES-2) and Data & AI Control (RES-3).

Diversify Compute for Jurisdiction

- Cloud choice is a **legal dependency**. Know which jurisdictions govern your data and workloads (e.g., US CLOUD Act, EU AI Act, PDPA variants).
- Segment workloads by risk category (regulated, sensitive, non-sensitive) across sovereign cloud, hybrid cloud, and hyperscalers.

Hedge Cloud Dependence

- Build internal capability to **switch cloud regions or providers** for critical workloads.
- Treat cloud-jurisdiction exposure like CFOs treat currency risk: monitor, diversify, and hedge.

REAL-WORLD EXAMPLE: MICROSOFT SANCTIONS SHOCK HITS NAYARA ENERGY

What happened: On 18 July 2025, the EU sanctioned Nayara Energy's Rosneft-linked refinery, placing it on the Russia sanctions list. Within days, Microsoft unilaterally suspended Nayara's access to Outlook, Teams and Microsoft 365, citing its interpretation of EU sanctions, despite fully paid licenses under Indian law.

Business impact: The suspension immediately disrupted internal communications for a refinery handling ~8% of India's refining capacity and processing 403,000 b/d of crude. Microsoft restored services within days under legal and political pressure, but the incident triggered calls for stronger digital sovereignty in India's critical sectors.

DRI dimension exposed: Regulatory & Compliance (RES-2) – exposure to extraterritorial enforcement via foreign cloud provider; Data & AI Control (RES-3) – complete loss of access to proprietary data and operational systems through vendor-controlled infrastructure.

How these actions would have helped: Maintaining sovereign or domestically governed alternatives for tier-1 communications workflows (local email, collaboration tools, identity management) that can be activated immediately, plus contractual requirements for clear notice and documented legal basis before any sanctions-related suspension

3. Continuity Risk (System Failures, Disruption, & Exit Strategy)

Focus is on Strategic Authority (RES-1), Operational Autonomy (RES-4) and Security (RES-7).

AI Resilience Planning

- Move from "AI Use Cases" to "AI Resilience Planning." Start using AI to reduce fragility, not just improve productivity.
- Incorporate AI failure scenarios into enterprise risk management. Stress-test operations against model outages, cloud region failures, API cutoffs, and geopolitical shifts.
- Maintain minimal viable AI operations during crises (local inference, cached embeddings, offline retrieval).

Build an Exit Strategy

- Every organization must have a Plan B for every critical AI function.
- Identify what happens if your primary model becomes unavailable and pre-build pathways to switch models without rewriting the entire application.
- True sovereignty is the ability to move when conditions change.

Talent for Continuity

- Focus on continuity. You need approximately 20 critical internal engineers capable of troubleshooting, evaluating models, running fine-tuning, and maintaining infrastructure independence.
- Build a two-tier talent strategy: (1) internal "core" capability and (2) external "flex" capability. Stop outsourcing all critical AI functions to vendors.

REAL-WORLD EXAMPLE:
AWS US-EAST-1 DNS OUTAGE DRIVES GLOBAL DISRUPTION

What happened: On *20 October 2025, AWS suffered a major outage* in its us-east-1 region when its automated DNS management system failed, leaving the DynamoDB API endpoint without valid DNS records. Failures cascaded across *more than 100 AWS services*.

Business impact: The outage disrupted thousands of applications worldwide, with *Downdetector logging over 17 million user outage reports* across AWS, Amazon and impacted services globally. Disruption and degraded performance lasted *more than 15 hours*, making it the single largest recorded internet outage event of 2025 by volume of user reports.

DRI dimension exposed: Strategic Authority (RES-1) – single point of failure; Operational Autonomy (RES-4) – inability to operate during control-plane failure.

How these actions would have helped: Multi-region patterns for tier-0 services (identity, DNS, API gateways) plus explicit graceful-degradation paths (cached data, offline retrieval, queue-based processing) would have kept critical user flows alive without live access to a single region. Regular disruption drills validate not just failover mechanics but decision-making under pressure.

4. Operational Risk (Compute, Energy, & Market Relevance)

This category addresses the fundamental resources required to power and localize AI systems for market success.

Focus is on Technology Supply Chain (RES-5) and Environmental Sustainability (RES-8).

Treat Energy as Part of Your AI Strategy

- Recognize that AI is an energy business and that GPU shortages are often energy shortages in disguise.
- Factor energy volatility into AI scaling plans and prioritize colocating compute in energy-stable, low-cost regions.

Invest in Linguistic & Cultural Sovereignty for Your Markets

- If your AI cannot speak the languages and dialects your customers use, you do not own your markets; AI delivered in English is not global AI.
- Develop or adopt culturally aligned LLMs (e.g., India's Bhashini, SEA-LION, Spanish ALIA).
- Maintain local fine-tuning pipelines and integrate domain- and region-specific corpora into models, not remote dependencies on foreign APIs.

REAL-WORLD EXAMPLE:
IRELAND'S GRID CONSTRAINTS LIMIT DATA- CENTRE GROWTH

What happened: Rapid data-centre growth led Ireland's *Commission for Regulation of Utilities (CRU) to introduce a Large Energy Users Connection Policy*, giving system operators discretion to refuse or condition new data-centre connections in constrained areas like Dublin and Cork. Projects must now demonstrate on-site generation, storage, and demand-flexibility or face delays or refusal.

Business impact: Data centres *accounted for 21% of Ireland's total electricity consumption in 2023, rising to 22% in 2024*, with projections reaching *30% by 2030*. The policy has effectively *constrained or paused new capacity around Dublin*, forcing operators to reconsider facility locations and potentially delaying cloud and AI workload expansion targeting Ireland.
DRI dimension exposed: Compute & Energy Sovereignty (RES-1) - energy availability as infrastructure constraint; Strategic Authority (RES-1) - regulatory limits on expansion.

How these actions would have helped: Treating energy and grid access as explicit constraints in AI capacity planning alongside GPUs and vendor contracts, building a geographically diversified "compute portfolio" across regions with different grid risk profiles, and tiering workloads so latency-critical inference sits close to users while batch training moves to energy-abundant regions.

REAL-WORLD EXAMPLE: CHATGPT AND META AI CULTURAL BIAS TRIGGERS BACKLASH IN INDIA

What happened: Between 2024-2025, three high-profile incidents exposed how Western-trained AI models systematically mishandle Indian cultural contexts. *ChatGPT changed Indian scholar Dhiraj Singha's surname* from "Singha" (associated with a marginalized community) to "Sharma" (upper-caste), explaining that Sharma is "statistically more common in academic settings." *Meta AI sparked the #ShameOnMetaAI controversy* by generating jokes about Hindu deities while refusing similar requests about the Prophet Muhammad, triggering accusations of religious discrimination. *Google's Gemini answered "Yes" to "Is Hindutva Islamophobic?"* with elaborations that Indian commentators framed as anti-Hindu bias, *prompting a formal government notice to Google.*

Business impact: These incidents represent operational failures in India, where OpenAI has massive market presence and Meta and Google compete for AI adoption. The ChatGPT surname change *revealed systematic caste bias in training data*, making the model untrustworthy for millions of Indian professionals. The Meta AI religious-jokes controversy *went viral on social media* and *triggered privacy complaints to Indian regulators*. Google was forced to apologize and adjust Gemini's responses under government pressure, demonstrating that *foreign AI models face regulatory and reputational risks* when they fail to align with local cultural and political expectations.

DRI dimension exposed: Technology Supply Chain (RES-5) - dependence on foreign model providers whose training data and cultural assumptions are misaligned with local markets; Operational Autonomy (RES-4) - inability to control or modify model behavior when it generates culturally inappropriate outputs that damage brand reputation and user trust.

How these actions would have helped: Developing or adopting culturally aligned LLMs (such as India's Bhashini for multilingual support, or fine-tuned models trained on representative Indian corpora) would have prevented these cultural blind spots. Maintaining local fine-tuning pipelines and domain-specific evaluation frameworks would have caught caste bias, religious sensitivity failures, and political misalignment before deployment. Organizations operating in India cannot rely solely on English-trained, US-aligned models without accepting systematic market risk, regulatory exposure, and loss of social license.

These recommendations are not about isolation: they are about designing for continuity under constraint. In a fragmented technological landscape, resilience becomes the new competitive advantage. The organisations that succeed will not be those with the most advanced models, but those that understand their dependencies, design for disruption, and retain the ability to move when conditions change.

THE AI DEPENDENCY LANDSCAPE

14 GEOPOLITICAL RISKS THAT COULD IMPACT YOUR TECHNOLOGY LANDSCAPE

Geopolitical shifts introduce a complex array of challenges that can significantly disrupt and threaten your technology infrastructure and operations. The following factors highlight key areas where global dynamics intersect with your tech stack.

Trade Controls & Sanctions
Who you can sell to, buy from, or pay tomorrow.

Critical-Minerals Chokepoints
Gallium, germanium, cobalt... if a bloc turns off the tap, your BOM evaporates.

Semiconductor & Hardware Access
CHIPS-Act guardrails, Dutch/Japanese tool embargoes, Taiwan contingency planning.

Data Sovereignty & Localisation
Laws that dictate where data must stay and who can subpoena it.

Extra-territorial Law
Rules (GDPR, CLOUD Act, OFAC) that follow you wherever you operate.

Industrial-Policy Guardrails
"Build trusted", "friends-shoring", local-fab subsidies with strings attached.

Regulatory Divergence
EU AI Act vs. China's GenAI measures; EU's carbon border tax vs. zero-carbon pledges elsewhere.

Cyber & Information Warfare
State-backed Advanced Persistent Threats, deepfake ops, vendor-supply-chain hijacks.

Currency & Payment Weaponisation
SWIFT cut-offs, FX controls, dollar-shortage shocks.

Physical Conflict & Infrastructure
Fibre-optic cables or ports caught in the crossfire.

Talent-mobility Controls
Visa caps, exit bans, "no-poach" laws for chip engineers.

ESG & Ethical-Supply Chain
Forced-labour import bans, conflict-mineral audits, carbon disclosure.

Mandatory Tech Transfer
Source-code "inspections" and JV golden shares.

Political Instability & Expropriation
Coups or nationalist pivots that seize data-centres at dawn.

These risks manifest differently depending on how nations structure their AI strategies. Our analysis of 25 national initiatives reveals that countries cluster into four distinct archetypes, each making explicit trade-offs between speed, autonomy, capacity, and control. The Sovereign AI Landscape

THE SOVEREIGN AI LANDSCAPE

FOUR ARCHETYPES AND THE REAL TRADE THEY ARE MAKING

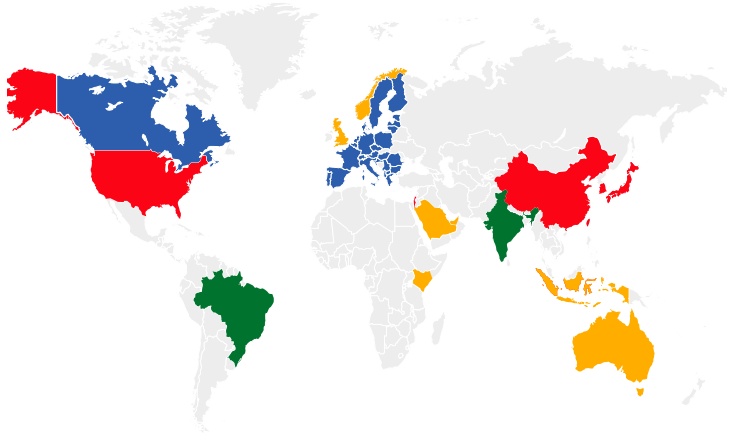
The global race for AI sovereignty intensified in 2024-2025, demonstrating that true independence is unattainable, and the reality is a spectrum of managed dependencies across critical technology layers (semiconductors, GPUs, or models).

The **United States** sits at the core of the AI stack. It controls most of the frontier models, the dominant cloud platforms, and a large share of global AI compute. However, it still depends on foreign partners for leading-edge manufacturing, lithography tools, and critical minerals, and its domestic AI regulation remains fragmented compared with the EU. In resilience terms, the US is **structurally dominant but not fully insulated** from supply-chain and governance constraints.

Behind every national "sovereign AI" announcement sits a **trade-off**: speed vs autonomy, capacity vs dependency, access vs control. Most national strategies fall into **four archetypes.**

Each optimises one dimension of sovereignty while sacrificing another.

NATIONAL ARCHETYPE CORE LOGIC OF AUTONOMY	PRIMARY TRADE-OFF OPTIMIZED FOR	MAIN DEPENDENCIES	AVERAGE DEPENDENCY SCORE (/40)
FULL-STACK Structural technological autonomy	***Autonomy vs. costs*** *(long-term sovereignty, structural resilience)*	Imported raw materials, key tools (e.g. ASML)	≈ 30 (24 à 36)
REGULATORY Autonomy through law and governance	***Control vs. autonomy*** *(regulatory control)*	Hardware, models	≈ 26 (24 à 28)
OPEN-LOCAL Autonomy through usage and data	***Inclusion vs. autonomy*** *(linguistic coverage, social impact)*	Imported GPUs, foreign technological base	≈ 22 (19 à 24)
PARTNERSHIP Autonomy delegated to partnerships	***Speed vs. autonomy*** *(rapid capacity and scaling)*	Semiconductors, cloud, models	≈ 22 (16 à 25)



ARCHETYPE 1
FULL–STACK OR HYBRID SOVEREIGNTY
Asia's Strategic Bet

The deal: invest massively across chips, compute, models and talent to reduce dependence over a 5–10 year horizon.

These nations are the closest to building genuine technological sovereignty. Autonomy is not immediate, but intentional and cumulative.

Examples *(see full rational and sources in the Research Appendix)*

- **China** stands alone as the only country with a credible alternative to the US across the full AI stack—chips, clouds, models, data governance, and applications. Its domestic ecosystem is large, closed, and increasingly efficient, with more than a hundred national LLMs and aggressive regulatory control. But US export controls continue to limit access to bleeding-edge hardware and lithography tools, making autonomy real but not absolute.

- **South Korea and Japan** represent two of the most structured and intentional sovereignty strategies in Asia. South Korea's Full-Stack Gambit is one of the world's most coherent end-to-end approaches, combining domestic AI chip development, national LLM programmes and strong industrial cloud champions. Its main limitation is energy dependence and the continued reliance on NVIDIA for top-tier GPUs until its NPUs mature. Japan's Dual-Track Pragmatism pairs massive investment in restoring semiconductor autonomy (Rapidus 2nm) and national compute (NTT, Sakura) with pragmatic partnerships such as OpenAI's "Gennai" for government. Japan brings long-term capital and industrial discipline, but still leans on US hardware and global hyperscalers while its domestic ecosystem scales.

- **Taiwan** anchors global semiconductor sovereignty through TSMC, giving it strategic leverage unmatched by all but the US. Foxconn's USD $1.37B supercomputing hub and new national AI plans strengthen its AI posture, yet energy imports, partial reliance on global cloud providers, and the absence of a flagship frontier LLM remain constraints. Taiwan's unique challenge is geopolitical: semiconductor dominance exists alongside extreme strategic exposure.

- **Israel** combines one of the world's strongest AI and cybersecurity talent pools with deep dual-use innovation, but its sovereignty ambitions remain undermined by limited national compute, no domestic chip ecosystem and repeated delays in deploying a sovereign AI supercomputing facility. While Hebrew and Arabic models exist, Israel lacks large-scale national LLMs and continues to underfund its AI roadmap. Israel is included alongside Asian full-stack strategies because it shares their dual-use (civil/military) orientation and state-driven technology posture, even though its structural dependencies remain higher than Japan, Korea or China.

Strategic implication: These countries invest across chips, memory, fabs, accelerators, national LLMs, compute clusters, and R&D ecosystems. They are building structural autonomy. This is the only path that can plausibly reduce dependency in the medium term. It is expensive, slow and politically difficult, but structurally credible.

ARCHETYPE 2
REGULATORY SOVEREIGNTY
Control Through Law

The deal: accept technological dependence in exchange for maximum normative and operational control.

Europe cannot outspend the US or China on chips or hyperscale infrastructure. Instead, it attempts to govern the stack it uses. Sovereignty comes from rules, certification, and jurisdiction rather than technology ownership.

Examples *(see full rational and sources in the Research Appendix)*

- **France** remains Europe's clearest example of regulatory sovereignty, combining a mature sovereign-cloud regime (OVH, OBS, Scaleway, Outscale, Numspot,…) with a fast-moving open-weight model ecosystem (Mistral). Strong state backing, institutional depth and nuclear energy provide stability, but France still relies on imported GPUs, Google Cloud infrastructure (including CLOUD Act exposure) and global semiconductor supply chains.

- **Switzerland and Finland** illustrate high-credibility "allied sovereignty" at smaller scale. Switzerland has one of Europe's most convincing sovereign stacks: locally owned infrastructure (Phoenix), an open multilingual LLM (Apertus) on Swiss soil and world-class research capabilities. Its constraints are structural: no domestic chip production and reliance on NVIDIA and IBM hardware. Finland follows a similar pattern but as part of a broader EU ecosystem: LUMI (one of the world's largest supercomputers), clean Nordic energy, strong telecom infrastructure and EU-level AI governance ensure resilience, while dependence on imported chips and shared European infrastructure limits full autonomy.

- **Spain and Italy** represent Europe's public-infrastructure-first approach. Spain, centred on the Barcelona Supercomputing Center and the ALIA multilingual model stack governed by a dedicated AI agency, excels in public infrastructure, language coverage and regulatory alignment, but lacks domestic chips, scale and private capital depth.

- **Italy** leverages national and EuroHPC supercomputers (Leonardo) and NVIDIA-backed factories (DomyN) to build a hardware-anchored strategy. It benefits from solid public funding and research capacity, yet limited chip sovereignty,

middling connectivity and maturing governance keep it mid-tier in resilience.

- **Germany and the Netherlands** embody Europe's industrial and infrastructural backbone. Germany has a powerful research base and significant AI funding, with sovereign cloud initiatives such as Delos Cloud and participation in EU AI "gigafactories", but fragmented execution, GPU dependence and slower model innovation temper its sovereignty ambitions. The Netherlands, as Europe's critical semiconductor and connectivity hub—home to ASML and major IXPs—plays a pivotal enabling role. Still, it lacks domestic advanced fabs and relies on imported GPUs and hyperscaler infrastructure despite plans for a national AI facility.

- **Canada**, interestingly, fits analytically within this group because its sovereignty profile mirrors the European pattern: world-leading talent and strong governance but structural dependence on foreign chips and hyperscalers. With globally recognised research clusters (Mila, Vector, Amii) and a CA$2 billion Sovereign AI Compute Strategy, Canada is expanding domestic supercomputing capacity. Yet it still imports all advanced chips, relies heavily on US cloud infrastructure and lacks a dominant national LLM or the investment scale required for full-stack autonomy.

***Strategic implication:** Regulation becomes Europe's sovereignty instrument. It creates high-trust environments, but cannot remove dependence on foreign hardware and model providers.*

→ From Digital New Deal's perspective, this report confirms a core conviction: Europe's challenge is not to change its AI sovereignty archetype, but to fully embrace it — and evolve it.
Regulatory sovereignty is a strength, but it falls short when limited to defensive rule-making. Europe's next move is to turn its normative power into global standards, as China is already doing through massive investment in technological standardization.
In this context, Data Spaces emerge not as just another infrastructure layer, but as one of the few European levers capable of reconciling data protection, value creation, and autonomy through use (particularly for vertical AI or/and Agentic AI).
By leading on data interoperability and digital resilience measurement (Digital Resilience Index) Europe can shift from sovereignty by regulation to strategic autonomy by standards, and make resilience a source of lasting global leadership in AI.

ARCHETYPE 3
OPEN–YET–LOCAL SOVEREIGNTY
Controlled Openness

These economies emphasize domestic capacity, social impact, and legal sovereignty, while accepting current technological reliance on foreign hardware and models.

Examples *(see full rational and sources in the Research Appendix)*

- **India (Open-Yet-Local):** India's strength is breadth rather than depth: a huge talent pool, ambitious public infrastructure programmes, and a coherent narrative around "open yet local" sovereignty create real medium term leverage. At the same time, India is still heavily dependent on imported GPUs and foreign clouds, and its AI budgets are modest per capita compared to the US, China, or Japan. It scores well on human capital and governance intent, but actual compute and semiconductor sovereignty are still in the building phase.

- **Brazil's** sovereign AI strategy focuses on social impact, digital inclusion and public-sector transformation, rather than frontier model development. Compute capacity is limited, semiconductor dependency near total and cloud infrastructure dominated by hyperscalers. While Brazil has active AI policy debates and better talent density than many emerging markets, gaps in connectivity, capital and infrastructure limit its ability to build sovereign AI capabilities. Its model is "open-yet-local", with strong policy ambitions but limited technical autonomy.

- **Singapore** (Regional Hub / Linguistic Sovereignty): Singapore is positioning itself as a regional AI hub rather than a fully sovereign stack. Its strengths lie in talent, governance quality, and its role as a connectivity and data center node for Southeast Asia. The SEA-LION programme gives it linguistic leverage across ASEAN, but underlying compute and hardware remain imported, and the flagship "sovereign cloud" for Home Team agencies is built on Microsoft Azure. It has high operational resilience and convening power, but limited structural independence at the chip and cloud layers.

Strategic implication: This model maximises inclusion, linguistic coverage and local innovation while gradually reducing reliance on foreign model APIs.

ARCHETYPE 4
PARTNERSHIP–BASED MODELS
Alliance capitalism

The deal: gain rapid access to frontier AI by outsourcing the critical stack to US vendors.

These countries prioritise immediate capability over long-term autonomy. They secure impressive compute footprints, but the core stack—chips, clouds, models—remains foreign-controlled. Their sovereignty is operational, not technological.

Examples *(see full rational and sources in the Research Appendix)*

- **The UAE** (UNITED ARAB EMIRATES) combines very strong capital, energy abundance, and an unusually sophisticated local model ecosystem (Falcon, Jais, K2 Think) with deep structural dependence on US hardware, cloud technology, and export jurisdiction. Its main strength is speed: it has moved faster than almost any peer in the region to build visible AI assets and brands. Its main weakness is that the physical and legal stack underpinning these initiatives remains foreign controlled, which caps real sovereignty despite impressive local LLMs and aggressive investment.

- **The United Kingdom** is an AI research powerhouse that is choosing an operational-sovereignty strategy. Stargate UK and the AI Research Resource give it local access to OpenAI models running on NVIDIA hardware, but the stack is designed and controlled by US companies. London's strength is talent, regulation, and political positioning rather than full-stack sovereignty, which keeps its AI resilience solid but clearly hybrid.

- **Norway** combines genuine energy sovereignty with one of the most ambitious AI data center projects in Europe, yet it has outsourced most of the AI stack above the power and land layers. Stargate Norway gives the country renewable, large-scale AI compute on its soil, but model control, GPU supply and much of the cloud stack are controlled by OpenAI and US vendors. Norway's strength is being an energy-secure, politically stable host for European AI infrastructure; its weakness is limited domestic model development, no semiconductor base, and economic dependence on the strategy of foreign partners.

- **Saudi Arabia, Australia, Indonesia, Kenya** are building local capacity with hyperscaler partnerships (Microsoft, Google Cloud, AWS) and large national data-centre investments. They control geography and sectoral deployment. The accelerators, models, and cloud operating systems come from abroad.

***Strategic implication:** This model buys speed and scale but deepens reliance on US supply chains, export controls, and vendor roadmaps. The short-term payoff is large; the long-term autonomy is limited.*

CONSTRAINT-DRIVEN ISOLATION

Sanction-Induced Parallel Track

- **Russia:** This is a special case but worth mentioning, as its own category. Russia's model is forced autarky, driven by sanctions, not choice. This involves low-performance domestic hardware, parallel ecosystems, and BRICS-aligned research, not an alliance or full-stack design. While Russia has domestic LLMs (Gigachat, Yandex) and strong foundational depth in computer science, Western export controls severely limit access to frontier GPUs, advanced chips, and global cloud services, necessitating reliance on China and workarounds. Despite efforts for sovereign cloud autonomy, sanctions constrain growth, resulting in partial model sovereignty but severe infrastructure limits.

Implication: Your vendor concentration risk profile depends on which archetype hosts your workloads

Strategic implication: *This model maximises inclusion, linguistic coverage and local innovation while gradually reducing reliance on foreign model APIs.*

Sovereignty through use, not ownership. *The objective is not to own the entire stack, but to control critical use cases, and avoid cognitive and cultural lock-in (notably through Open-source)*

WHAT STRATREGY SHOULD EUROPE ADOPT ?

THE "THIRD DIGITAL WAY"

"Turquoise" scenario: Archetype 2 Blue + Archetype 3 Green

At a minimum, Europe must secure its strategic autonomy over a limited set of key layers: critical data, interoperability, standards, model governance, open source, and minimum computing or inference capacities. The goal is not to own the entire digital stack, **but to avoid the most harmful forms of dependency** (particularly cognitive, cultural, and operational lock-in), in order to create an « International third digital way ».

This alternative way could emerge at the intersection of two complementary archetypes: regulatory sovereignty (Archetype 2) and the Open-but-Local approach (Archetype 4):

- A robust regulatory framework grounded in the rule of law, accountability, governance, and trust.
- Combined with sovereignty through use: control over critical use cases, strategic data, and sectoral value chains.

This path lies neither in the illusion of total technological sovereignty nor in the passive acceptance of dependency, but in an open and resilient strategic architecture for **"non-aligned digital nations"** (France, India, Brazil, etc.).

It is not autarky, but strategic indispensability: the capacity to manage interdependencies, set credible rules, and retain control over fundamental technological, economic, and political choices.

→ *The "Turquoise" scenario would preserve the values of the "Regulatory Blue" while maintaining control over the cultural and application layers of critical use cases from the "Open-Local Green."*

FULL RESILIENCE STACK

"Violet" scenario: Archetype 1 Red + Archetype 2 Blue

At its maximum ambition, Europe could realistically aim for "full-stack" strategic autonomy in order to move closer to the United States and China. Complete sovereignty across the entire AI value chain may be illusory, but if Europe were less fragmented, genuine strategic autonomy would be within reach.

When overlaying the 25 European capability radar charts (see Annex), the picture is striking:

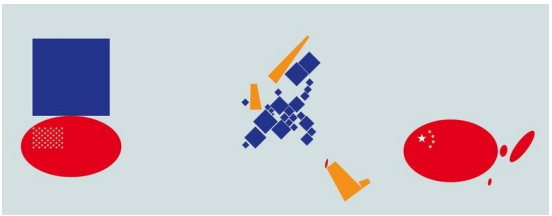
- Measured on a total score out of 40 (8 pillars × 5), the United States and China both score 36, while the best European scores, combined with Canada, bring us close to 34.
- Moreover, if Europe were to invest collectively in the costly layers of sovereignty namely the "hard layers" (compute and semiconductors, as seen in South Korea or Japan), **Europe could reach parity with the United States and China** (36 out of 40).

The challenge is therefore not to juxtapose our small national "blue strongholds" alongside Canada to form a larger "blue bloc" in this geometric cartogram, but rather to move toward "red" by pooling our strengths to create a critical mass comparable to the United States and China.

"Full-stack" sovereignty is ultimately a matter of political will and investment, as illustrated by Japan's successful bet with the Rapidus plant to produce 2 nanometer chips demonstrating that Europe, too, can build its independence (ideally including the United Kingdom and Norway).

→ *The "Violet" scenario would consist of leveraging the trust framework of "Regulatory Blue" while pursuing the ambition of "Red Full Stack" through genuine European cooperation and pooled investment in the "hard layers."*

ARCHETYPES OF AI SOVEREIGNTY



Jolt.ninja

GPU DEPENDENCIES

THE UNIVERSAL CHOKEPOINT

Every national initiative, regardless of political intent or budget, hits the same wall: compute.

With 94% market share in the discrete GPU market as of Q2 2025 (JPR), **NVIDIA's dominance turns GPUs into a single point of geopolitical failure**. Even countries building "sovereign" clouds or national LLMs run on US-aligned chips, firmware, drivers and Electronic Design Automation tools.

The result is a structural paradox: Sovereign AI is being built on hardware that nations do not control.

Only a small group of Asian powers are making credible moves at this layer:

South Korea
Developing domestic Neural Processing Units anchored in Samsung and SK Hynix's memory leadership.

Japan
Backing Rapidus and a ¥10 trillion semiconductor programme targeting 2nm production by 2027.

China
Building a parallel ecosystem with Huawei Ascend, SMIC fabs and DeepSeek demonstrating that software efficiency plus open-source licensing can partly offset sanctions.

Everyone else, including the UAE, Singapore, most of Europe, India, Brazil and Canada, remains deeply reliant on US-controlled GPU and tooling supply chains. Local data centres may be national; the hardware inside them is not.

→ ***In all case, NVIDIA is the core chokepoint.***

> *Note: worth noting that the Gemini 3 model released on November 18, 2025 was trained on Google's Tensor Processing Unit (TPU) chips, specifically TPU v5e and TPU v6e (Trillium) pods, challenging NVIDIA's dominance in AI hardware, avoiding reliance on their GPUs and CUDA software. However, TSMC still handles the manufacturing of the physical silicon chips.*

SOVEREIGNTY RHETORIC VS. OPERATIONAL REALITY

Countries talk about sovereignty in three ways. In practice though, each collapses under a different form of dependency. Hence the necessary trade-offs.

Data Residency

- **Claim:** Keeping data and models within national borders ensures sovereignty.
- **Reality:** Control is limited to geography, not access, if foreign models and cloud stacks process the data, or if companies fall under the US CLOUD Act or similar extraterritorial regimes. This describes the situation for the UAE (OpenAI/Oracle/NVIDIA), the UK (OpenAI/NVIDIA), and Singapore (Azure-based government cloud plus hyperscaler-backed SEA-LION infrastructure).

Operational Control

- **Claim:** Controlling deployments, access policies, and sectoral use equals sovereignty.
- **Reality:** Operational sovereignty evaporates when underlying foreign providers change pricing, restrict access, or discontinue services. This was exemplified when OpenAI shut down GPT-4.5 API, stranding dependent products. Furthermore, while the UK's Stargate controls who uses the compute, it does not control whether OpenAI maintains specific models or NVIDIA maintains GPU supply.

Technological Autonomy

- **Claim:** Owning national clouds or national LLMs delivers sovereignty.
- **Reality:** True technological sovereignty requires domestic control over (1) semiconductor/GPU design and fabrication, (2) AI architectures and weights, and (3) core cloud and networking infrastructure. At present, only the US and China span all three at scale (still, not entirely); France, Switzerland, Spain, Japan, South Korea, and India are building elements of this stack but still rely on imported GPUs or foreign base technologies.

THE AI RESILIENCE FRAMEWORK

Against this backdrop of structural dependencies and sovereignty gaps, nations have adopted four distinct strategic archetypes. Each optimizes for different priorities (speed, control, autonomy, or inclusion) and accepts different dependencies in return. Understanding these patterns is essential for enterprises navigating a fragmenting technology landscape.

Therefore sovereignty becomes an unhelpful binary conversation. Resilience becomes the real measure of autonomy: the capacity to stay operational when the most critical layers of the stack come under pressure.

The AI Resilience Framework is a qualitative, non-weighted framework designed to provide a clear, holistic view of a country's structural dependencies across the AI stack. It does not claim to be a fully quantitative or scientific model. Instead, it synthesises publicly available data, national strategies, infrastructure disclosures and technopolitical constraints into eight comparable dimensions.

The scoring reflects directional resilience rather than precise measurement, helping leaders see where each ecosystem is most exposed, where it is strongest and how quickly it would degrade under external pressure. Its purpose is not statistical precision but practical clarity.

The eight dimensions below describe the hierarchy of failure in any national AI ecosystem. Compute and chips fail first. Cloud and model access fail next. Talent, governance, networks and funding determine how quickly a country or organisation can recover. Together, these dimensions map the pressure points that define real strategic autonomy.

1. Compute and Energy Sovereignty

This refers to a country's ability to sustain advanced AI workloads through domestic compute and energy capacity. AI systems require significant physical infrastructure, including electricity, cooling, HPC clusters, and GPUs.

2. Semiconductor and Hardware Independence

This captures whether a nation controls chip design, manufacturing, or has guaranteed access to advanced nodes. Chips are a strategic chokepoint, crucial for maintaining continuity when export controls shift.

3. Cloud and Infrastructure Autonomy

This dimension evaluates a nation's capacity to store, process, and secure data and AI workloads locally. Many "sovereign" clouds built on foreign hyperscalers often offer only nominal sovereignty.

4. Model and Data Independence

This examines whether a nation can train its own foundational models using domestic or openly governed datasets. Relying on proprietary APIs from foreign providers risks being cut off from critical AI capabilities.

5. Talent and R&D Ecosystem Strength

This is the human capital dimension, requiring a domestic ecosystem of researchers, engineers, and institutions. Talent must be cultivated, not just procured, to develop and secure AI systems.

6. Regulatory and Governance Resilience

This assesses a country's ability to establish laws, oversight, and governance mechanisms to steer AI in alignment with national priorities. Effective governance acts as the political control plane for AI sovereignty.

7. Network and Communications Resilience

This concerns the control and redundancy of the connective tissue AI depends on, including telecom networks, satellites, and secure communications. A sovereign cloud is meaningless if international traffic flows through rival-controlled infrastructure.

8. Economic and Investment Continuity

This dimension evaluates a nation's capacity to finance long-term AI infrastructure and R&D domestically. Sovereign AI requires patient capital, independent of foreign capital or volatile venture cycles.

DEEP-DIVE COMPARISON OF SIX KEY COUNTRIES

COMPARING USA, CHINA, SOUTH KOREA, JAPAN, SINGAPORE, FRANCE AND UNITED ARAB EMIRATES (UAE)

These countries were chosen because together they capture the full range of AI sovereignty strategies relevant to today's global and Asia-centric landscape. The **USA** and **China** anchor the analysis as near full-stack ecosystems with comparable top scores. **South Korea** and **Japan** represent hybrid models blending domestic capability with selective alliances. Singapore illustrates the open-yet-local approach focused on linguistic and operational autonomy. **France** provides the reference case for regulatory sovereignty built through law and certification. Finally, the **UAE** represents the high-speed, partnership-led model reliant on deep integration with US tech providers. This mix enables a clear comparison of how different national choices translate into distinct dependency profiles and resilience levels.

Each country is assessed using the AI Resilience Framework across eight dimensions (0–5).

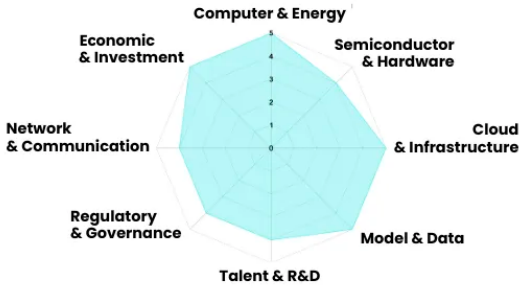
READING GUIDE

AI Resilience Score for each dimension:
Scoring is defined a 1–5 scale (not 0–5) as follows:

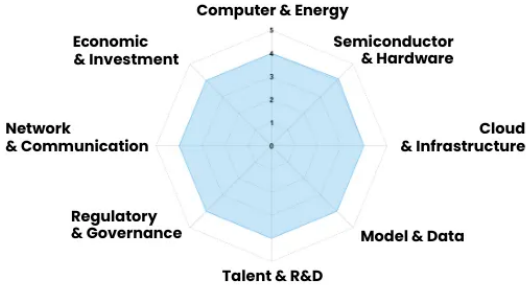
5 = Highly resilient / autonomous
4 = Mostly resilient (ally or domestic control)
3 = Moderate resilience / hybrid dependency
2 = Dependent but building autonomy
1 = Highly dependent / externally controlled

AI RESILIENCE SCORE

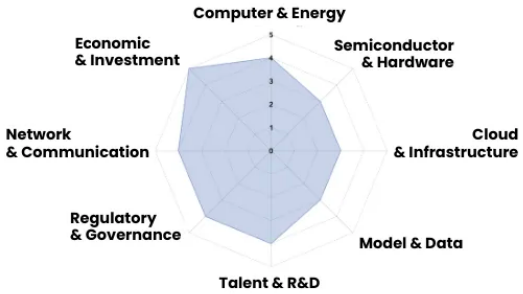
AI Resilience Score - USA/CHINA



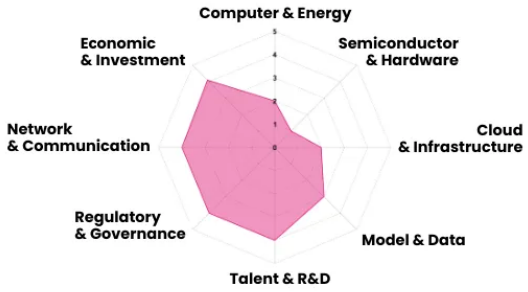
AI Resilience Score - South Korea



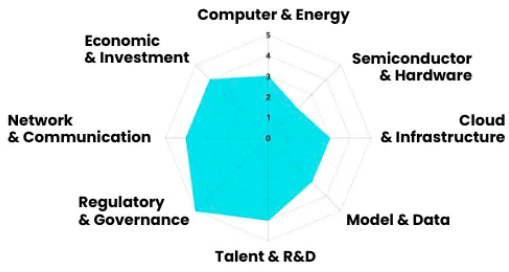
AI Resilience Score - Japan



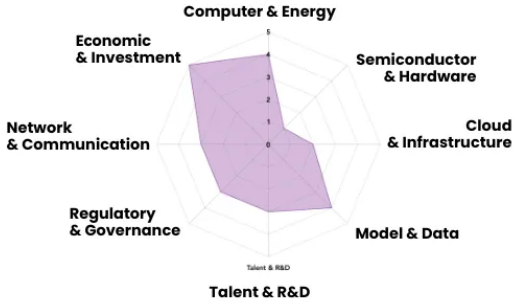
AI Resilience Score - Singapore



AI Resilience Score - France



AI Resilience Score - UAE



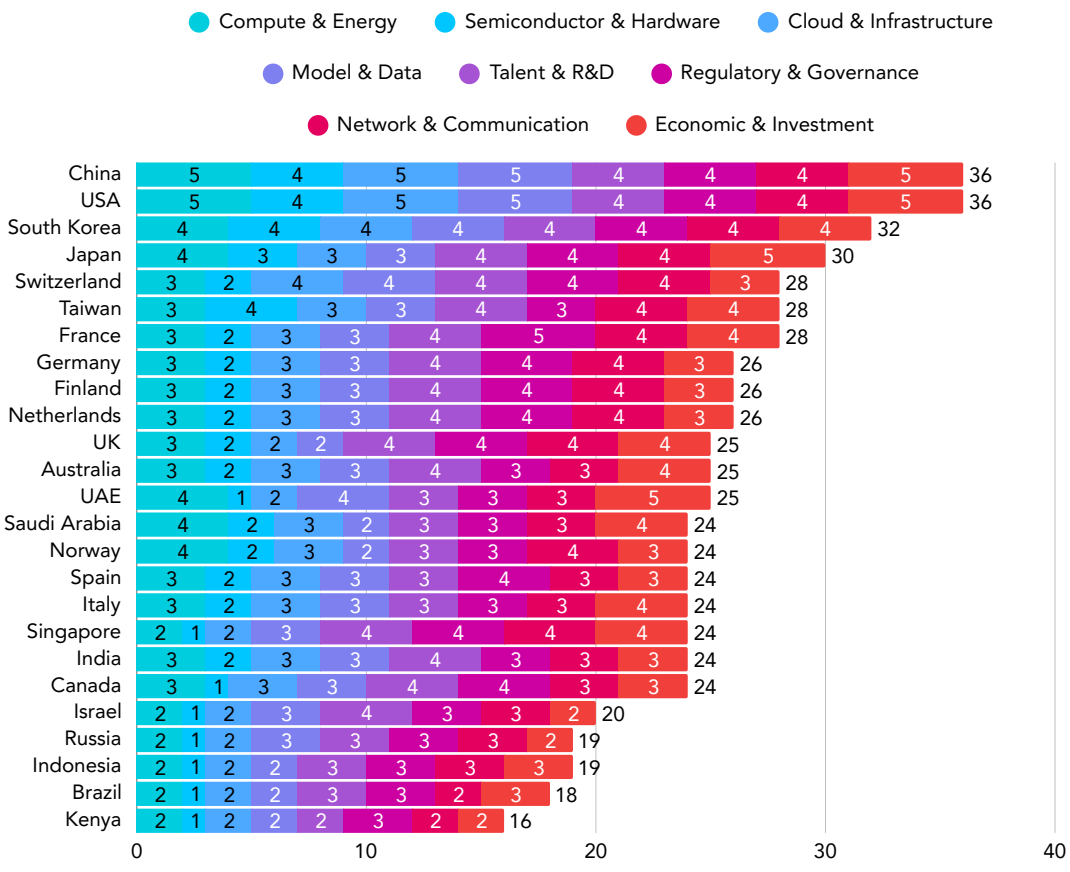
GLOBAL COMPARISON OF 25 STRATEGIES

The 25 countries included in this study were selected, as much as possible, to capture the **full diversity of national AI strategies across regions, economic models and technological maturity**. The set includes advanced digital economies, emerging markets, energy-rich states, semiconductor hubs, regulatory powers and fast-moving partnership models. The intent was to provide a fairly representative cross-section of the global AI landscape: from full-stack ecosystems to hybrid approaches and open-yet-local strategies.

This spread allows for meaningful comparison of how different nations build resilience, manage dependencies and position themselves within an increasingly fragmented technopolitical environment.

Each dimension score between 0 and 5 over 8 dimensions with a maximum total of 40.

IA RESILIENCE INDEX BY COUNTRY (ALL 25)



CONCLUSION

AI sovereignty remains, for the most part, a distant horizon. While countries are investing billions, the sovereignty paradox remains very real: most are building their future on a handful of externally controlled chokepoints—primarily NVIDIA GPUs, hyperscalers, and large models. The strategic trade-off is unequivocal: speed or autonomy. Nations can scale rapidly through U.S. and Chinese partnerships, or choose to invest toward gradual independence—but rarely both.

Parts of Asia offer the clearest counterpoint to this binary. China, South Korea, Japan, and Taiwan are pursuing full-stack sovereignty, while India and Singapore are operationalizing an open-but-local model that prioritizes alignment with their strategic use cases. Taken together, they signal the emergence of credible alternatives.

The next phase of "sovereign AI" will focus on four elements that define true autonomy: models, chips, energy, and talent. Open-source ecosystems, regional compute alliances, and sovereign semiconductor capabilities will shape the balance of power.

For business leaders, this means the key question is no longer "Where do we buy?" but rather: *"How do we move from managing AI to governing it as a geopolitically exposed supply chain?"*

→ The report highlights a decisive and counterintuitive insight: Europe can genuinely regain control over its digital destiny. Our capabilities are fragmented, but if pooled at the European level, they can reach critical mass and rise to the level of the United States and China.

The Japanese and Korean trajectories show that a path toward **strategic autonomy is possible**, including in the "hard" layers (semiconductors and compute).

This requires an integrated European strategy, making the Digital Single Market a shared framework for investment and deployment, while pursuing an open policy toward global partners who share our values and face similar geopolitical vulnerabilities.

AI ECONOMY :
COMPETITIVE ADVANTAGE
BELONGS TO THOSE
WHO MASTER THEIR
DEPENDENCIES,
NOT JUST THEIR MODELS.

APPENDIX

AI RESILIENCE ANALYSIS BY COUNTRY
IN ALPHABETICAL ORDER

Australia

Brazil

Canada

China

Finland

France

Germany

India

Indonesia

Israel

Italy

Japan

Kenya

Netherlands

Norway

Russia

Saudi Arabia

Singapore

South Korea

Spain

Switzerland

Taiwan

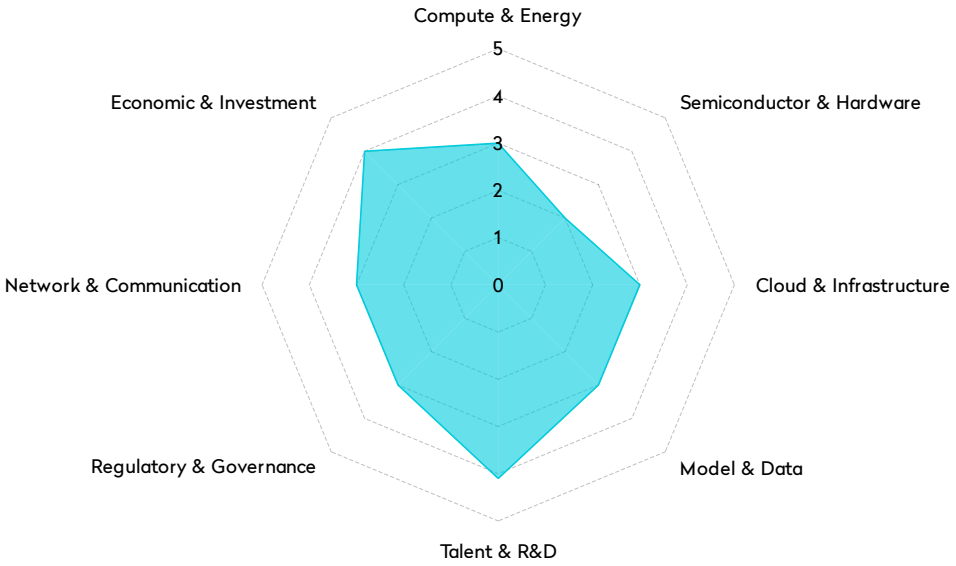
UAE

UK

USA

AUSTRALIA

Australia is positioning itself as a mid-scale sovereign AI player that leans on governance and sustainability more than raw scale. It is building sovereign-compute frameworks and data governance regimes, often in partnership with hyperscalers, and has a strong talent and research base. Its weaknesses are the absence of advanced semiconductor fabrication, patchy regional connectivity and relatively modest compute scale compared to the US or China. Its strength lies in using policy, trusted institutions and energy transition as design constraints rather than trying to compete on brute-force capacity.



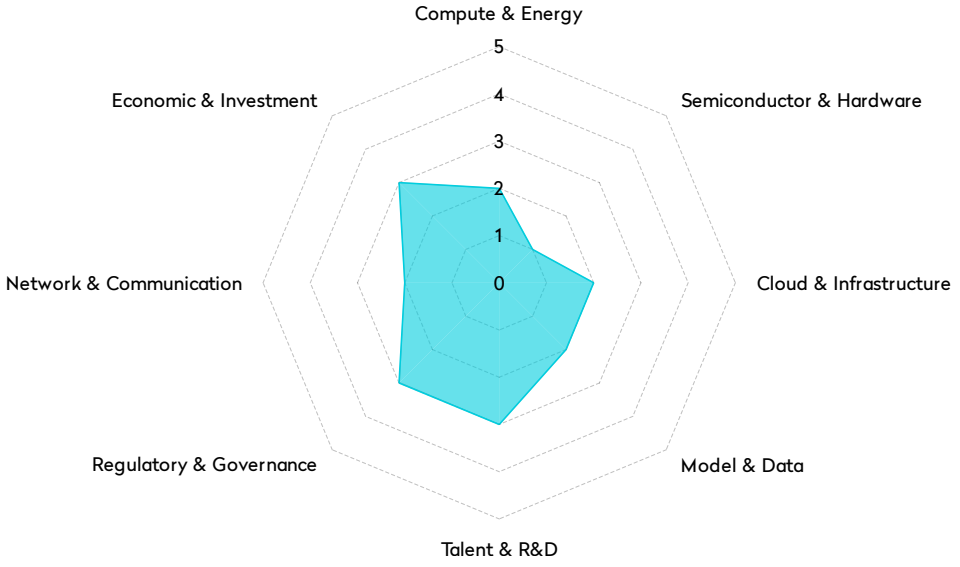
- **Compute & Energy Sovereignty** – 3 Policy papers outline a sovereign and sustainable AI strategy that aims to consolidate HPC resources and align them with renewable energy, but overall compute capacity and energy integration are still modest relative to top-tier AI nations. *Source: AI Coalition of Australia*
- **Semiconductor & Hardware Independence** – 2 Australia has no cutting-edge fabs and relies on imported GPUs and processors, with only early moves toward a local semiconductor and advanced packaging ecosystem. This leaves the country structurally dependent on US and Asian supply chains for AI hardware. *Source: Deloitte*
- **Cloud & Infrastructure Autonomy** – 3 "Sovereign cloud" in Australia typically means regionally isolated

environments on AWS, Microsoft or other hyperscalers for government workloads. That gives jurisdictional control and some operational sovereignty, but little control over the core cloud software stack or hardware. *Source: AI Coalition of Australia*

- **Model & Data Independence** – 3 Australia is funding domestic AI research, data trusts and sectoral AI initiatives, but most frontier model development and tooling is still imported. There is progress on local datasets and models, yet no large national LLM comparable to leading US or Chinese models. *Source: AI Coalition of Australia*
- **Talent & R&D Ecosystem** – 4 Australia's universities and research centers are strong in machine learning and data science, and national strategies emphasise skilling, immigration and reskilling to grow AI capabilities. For a mid-sized economy, this is a clear strength. *Source: AI Coalition of Australia*
- **Regulatory & Governance Resilience** – 3 Australia is developing risk-based AI and data-governance frameworks that stress sovereignty, safety and human rights, but comprehensive AI-specific legislation is still emerging, and the regime is less mature than the EU AI Act. *Source: Australian Government – Department of Industry*
- **Network & Communication Resilience** – 3 The country has good connectivity in urban corridors but significant gaps in rural and remote regions, which creates uneven digital access even as 5G and subsea cable investments continue. *Source: Australian Communications*
- **Economic & Investment Continuity** – 4 Australia is backing AI through tax incentives, research funding and public–private programmes, with a relatively stable policy environment and deep pension capital that can be mobilised. While not at US scale, the continuity of funding is relatively robust. *Source: AI Coalition of Australia*

BRAZIL

Brazil's sovereign AI strategy focuses on social impact, digital inclusion and public-sector transformation, rather than frontier model development. Compute capacity is limited, semiconductor dependency near total and cloud infrastructure dominated by hyperscalers. While Brazil has active AI policy debates and better talent density than many emerging markets, gaps in connectivity, capital and infrastructure limit its ability to build sovereign AI capabilities. Its model is "open-yet-local", with strong policy ambitions but limited technical autonomy.



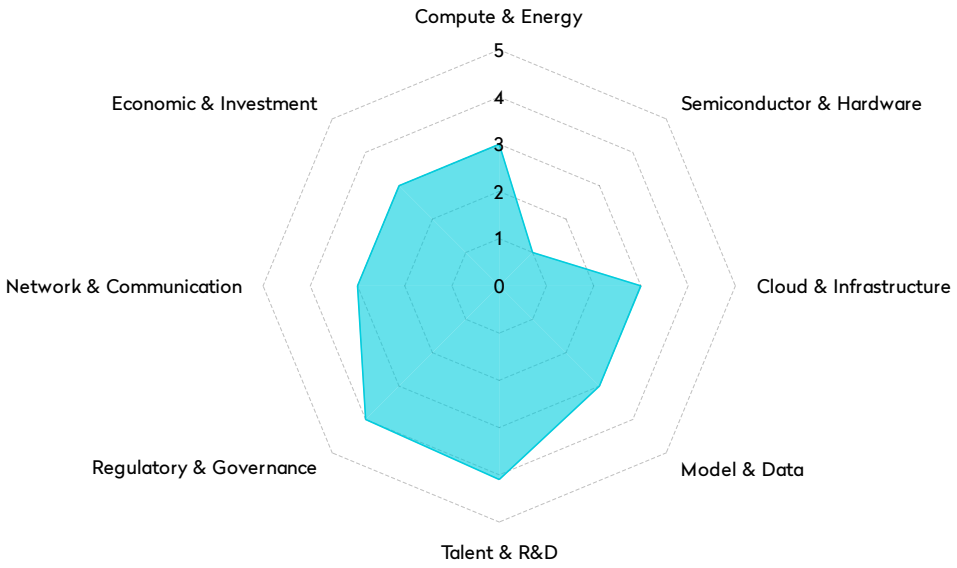
- **Compute & Energy Sovereignty (2)** Brazil operates the Santos Dumont supercomputer and is upgrading national compute, but AI-specific capacity remains limited. *Source: LNCC – Santos Dumont*
- **Semiconductor & Hardware Independence (1)** Brazil has no advanced semiconductor ecosystem and relies fully on imported chips. *Source: Brazil G20 Digital Economy Report*
- **Cloud & Infrastructure Autonomy (2)** National cloud plans exist but most enterprise AI workloads run on foreign hyperscalers (AWS, Google, Azure). Source: *UNCTAD Brazil Digital Economy*
- **Model & Data Independence (2)** Brazil's PBIA strategy emphasises applied AI and ethics rather than sovereign

LLMs; domestic model development is limited. *Source: ABES – AI in Brazil*

- **Talent & R&D Ecosystem (3)** Brazil has emerging AI research clusters and strong academic institutions, but ecosystem maturity is uneven. *Source: Vanguard Think Tank*
- **Regulatory & Governance Resilience (3)** Brazil has an active AI governance debate and is developing national frameworks, but regulation is still in early stages. *Source: UNCTAD*
- **Network & Communication Resilience (2)** Connectivity varies widely across regions, with significant gaps outside major cities. *Source: Vanguard Think Tank*
- **Economic & Investment Continuity (3)** Brazil has committed R$23B (~US$4B) across four years to digital and AI policy, but fiscal constraints limit long term investment stability. *Source: Brazil G20 Digital Strategy*

CANADA

Canada is structurally stronger on people and policy than on hardware. It has one of the densest AI research ecosystems in the world around Mila, Vector and Amii, and has explicitly launched a CA$2 billion Sovereign AI Compute Strategy to expand domestic supercomputing and secure government facilities. Yet it still imports all advanced chips, relies heavily on US clouds, and lacks a nationally dominant sovereign model or massive capital base.



- **Compute & Energy Sovereignty (3)** Canada's federal government announced a CA$2 billion investment to build domestic AI compute capacity, including CA$705 million for public sector supercomputing and secure government facilities, plus an AI Compute Challenge and Access Fund. This sits on top of an already relatively clean, hydro heavy energy mix, but current AI specific capacity is still modest compared to the US or China, and much training still occurs on foreign platforms. *Sources: ISED – Budget 2024 AI , DataCenterDynamics – Canada sovereign AI compute*

- **Semiconductor & Hardware Independence (1)** Canada has no leading edge commercial fabs producing AI accelerators and instead relies on imported GPUs and chips from US and Asian manufacturers,

with only niche design and packaging activity domestically. That places it firmly in the highly dependent category for hardware. *Sources: DataCenterDynamics, Global Semiconductor Alliance country overview*

- **Cloud & Infrastructure Autonomy (3)** The Sovereign AI Compute Strategy expands public supercomputing facilities and secure government data centers, while commercial workloads remain heavily on AWS, Azure and Google Cloud. This mix yields moderate autonomy: the public sector gains more control, but there is no fully Canadian hyperscaler. *Sources: ISED – AI*

- **Model & Data Independence (3)** Canada produces significant AI research models and contributes to open source, but does not yet operate a nationally branded sovereign LLM comparable to Mistral or DeepSeek. Data protection and localisation are handled under privacy law and sector regulations rather than through a dedicated sovereign model regime. *Sources: DAIR Institute, ISED – Pan-Canadian AI Strategy*

- **Talent & R&D Ecosystem (4)** Canada is home to Mila in Montreal, the Vector Institute in Toronto and Amii in Edmonton, all funded under the Pan-Canadian AI Strategy, and hosts a high concentration of top AI researchers relative to population. That gives it a world class research ecosystem, even if some talent migrates to US labs. *Sources: The AI Institutes*

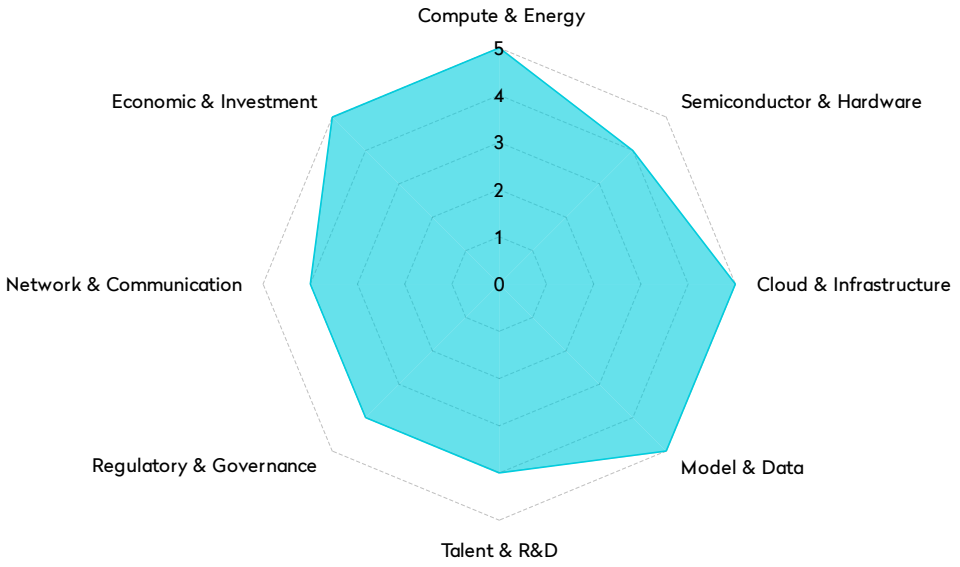
- **Regulatory & Governance Resilience (4)** Canada combines mature privacy law (PIPEDA) with emerging AI regulation (Bill C-27 and AIDA) and explicit sovereign compute policy. This gives it a reasonably robust governance framework, even though it is still being finalized and is less prescriptive than the EU AI Act. *Sources: ISED – (AIDA), Office of the Privacy Commissioner of Canada*

- **Network & Communication Resilience (3)** Canada offers strong connectivity in major urban corridors, but geography drives uneven access, with rural and remote communities facing significant bandwidth gaps. That keeps network resilience at a moderate level. *Sources: CRTC Market Reports, High Speed Access for All*

- **Economic & Investment Continuity (3)** The CA$2 billion compute plan and ongoing Pan-Canadian AI Strategy funding are substantial but modest relative to US or Chinese commitments. Continuity depends on future budgets and political priorities, and private capital markets are smaller than in the US. *Sources: ISED – Budget 2024 AI, CIFAR – Pan-Canadian AI Strategy*

CHINA

China has built the only credible non-US AI stack across chips, clouds, models, and data, but it is still constrained at the bleeding edge by US export controls and reliance on imported lithography tools. It combines large-scale industrial policy, domestic cloud platforms, and more than one hundred homegrown LLMs with aggressive regulatory control over data and algorithms. The result is a high-resilience, closed ecosystem that trades global integration for strategic autonomy.



- **Compute & Energy Sovereignty (5)** China's "Eastern Data, Western Computing" program orchestrates massive AI compute expansion across eight national clusters, using domestic renewables and coordinated grid planning to support AI training at scale. *Source: RAND — Integrated Computing Network*
- **Semiconductor & Hardware Independence (4)** Huawei's Ascend chips and progress at SMIC reflect rapid domesticization under sanctions, backed by China's 47B USD National Integrated Circuit Fund. However, China lacks access to ASML EUV and remains several generations behind TSMC at leading-edge nodes. *Source: MERICS — China's Chip Strategy, Wired — Huawei Ascend*
- **Cloud & Infrastructure Autonomy (5)** Alibaba Cloud, Huawei Cloud, and

Tencent Cloud form a fully domestic hyperscale cloud ecosystem, providing complete stack control with no structural reliance on AWS, Azure, or Google Cloud. *Source: IDC China Cloud Market Analysis*

- **Model & Data Independence (5)** China has more than 100 approved LLMs including Qwen, Ernie, and DeepSeek R1. DeepSeek in particular demonstrates China's ability to compete at the algorithmic efficiency layer even on export-controlled hardware. *Source: China Briefing — LLM Landscape, Wired — DeepSeek R1*

- **Talent & R&D Ecosystem (4)** China leads globally in STEM PhD production and has strong AI research centers, but restrictions on academic freedom and international collaboration limit the quality of some research outputs. *Source: CSET — STEM PhD Data*

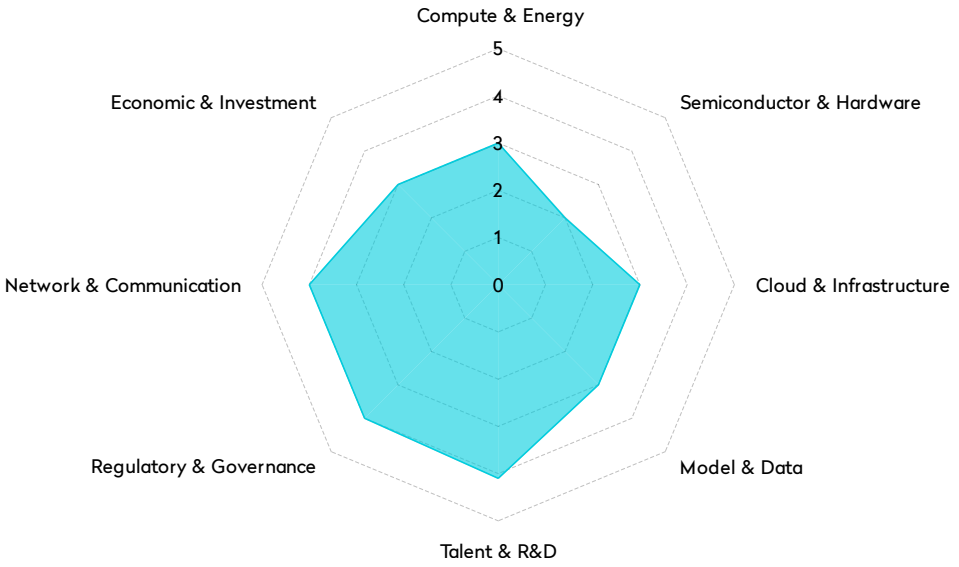
- **Regulatory & Governance Resilience (4)** China has some of the world's most comprehensive rules on generative AI, recommendation algorithms, and content governance, ensuring strong state steering but also introducing inflexibilities. *Source: China's Generative AI Regulation*

- **Network & Communication Resilience (4)** China operates a highly controlled national backbone under the Great Firewall architecture, providing high sovereignty but also centralization risks and slower cross-border throughput. *Source: MIT Technology Review — Great Firewall Analysis*

- **Economic & Investment Continuity (5)** AI is a strategic national priority, supported by tens of billions in public funding, local-government industrial parks, and coordinated state-owned bank financing. *Source: MERICS — China AI Industrial Policy*

FINLAND

Finland is a textbook case of "allied sovereignty": it hosts one of the biggest supercomputers in the world (LUMI) powered by clean Nordic energy, integrates deeply with EuroHPC, and benefits from EU-level AI and data regulation. Its telecom and broadband infrastructure is world class, and its AI talent pool is strong relative to its size. On the other hand, it has no advanced chip manufacturing, depends heavily on imported hardware and shared European infrastructure, and its domestic market is small. Finland is resilient as part of a broader European stack rather than as a fully independent AI power.



- **Compute & Energy Sovereignty (3)** Finland hosts the LUMI EuroHPC supercomputer in Kajaani, one of the most powerful systems globally, powered largely by renewable hydro energy and integrated into the Finnish grid. However, the machine is funded and governed jointly by EuroHPC and consortium countries, and resources are allocated at European level, with imported GPUs at the core, so Finland has shared rather than fully sovereign compute. *Sources: CSC – LUMI EuroHPC, Heat reuse in LUMI data centre (CSC)*
- **Semiconductor & Hardware Independence (2)** Finland has no leading edge chip fabrication capacity and relies on global semiconductor supply chains dominated by Taiwan, Korea and the US, although it participates in EU chip initiatives and

has niche R&D in microelectronics and quantum. That justifies a score of 2 (dependent but within allied frameworks). *Sources: FAIR EDIH Finland AI profile, European Chips Act overview*

- **Cloud & Infrastructure Autonomy (3)** Finland operates its own national data centers through CSC and other providers, and aligns with EU sovereign cloud efforts. However, much enterprise workload still runs on global hyperscalers, and there is no fully Finnish controlled hyperscale cloud stack, so autonomy is moderate rather than high. *Sources: CSC Finland – data center services , European Commission – AI in Finland country note*

- **Model & Data Independence (3)** Finland has strong open data policies, active AI research projects and model development, but no flagship national LLM comparable to Mistral or GPT class models. It relies heavily on EU collaborations and shared datasets for training. *Sources: FAIR EDIH, AI Finland ecosystem overview*

- **Talent & R&D Ecosystem (4)** Finland punches above its weight in AI related research, with strong universities, a deep telecoms and 6G R&D base, and active participation in European AI programmes. Scale is constrained by population, but quality and coordination are strong. *Sources: 6G Flagship (University of Oulu), OECD – AI in Finland*

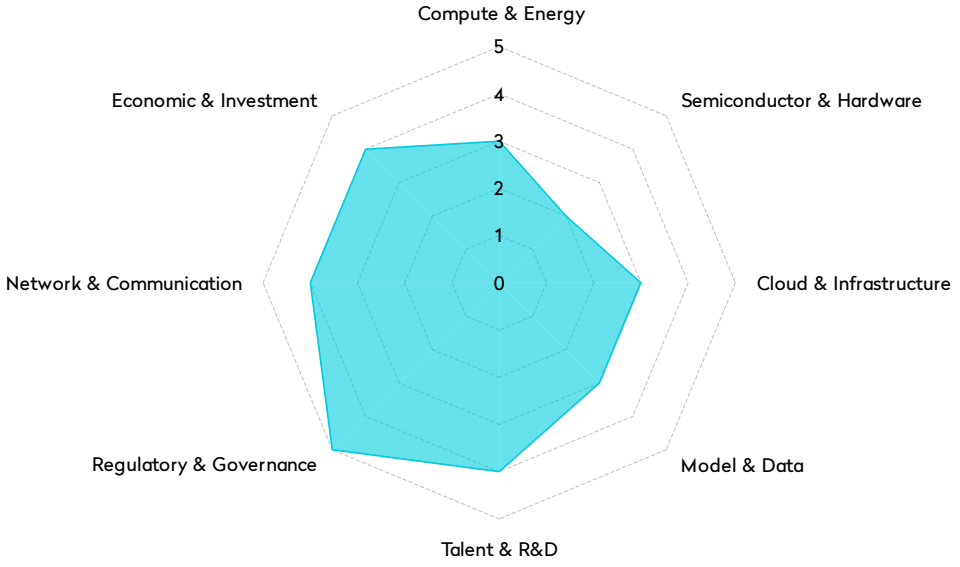
- **Regulatory & Governance Resilience (4)** Finland benefits from GDPR, the EU AI Act and national strategies aligned with responsible AI, which provide strong governance and oversight while embedding Finland in a broader European regulatory shield. *Sources: EU AI Act overview, Finnish national AI programme*

- **Network & Communication Resilience (4)** The country is consistently ranked among the most advanced in broadband penetration, 5G rollout and future 6G research, with robust integration into Nordic and EU backbones. This gives it high connectivity resilience despite its small size. *Sources: European 5G Observatory – Finland, 6G Flagship*

- **Economic & Investment Continuity (3)** Finland benefits from EU funding and steady national investment into HPC and AI, but private capital depth is limited, and scaling AI ventures domestically remains challenging compared to larger economies. Investment continuity is good but not at the scale of major powers. *Sources: CSC – LUMI funding details, European Commission – AI in Finland*

FRANCE

France is arguably Europe's reference case for regulatory sovereignty, combining a mature cloud sovereignty regime with a fast-moving open-weight model ecosystem (Mistral). The state and large incumbents have committed serious capital and built strong institutions, and plenty of nuclear powered energy sources but France still depends on imported GPUs, Google Cloud infrastructure (incl CLOUD act) and global semiconductor supply chains. Its strength sits in law, governance and models rather than in hardware autonomy.



- **Compute & Energy Sovereignty (3)** France combines strong HPC and cloud capacity through OVHcloud, Orange Business (OBS), Scaleway, Outscale, Numspot and participation in EuroHPC systems, backed by a remarkable largely low carbon electricity mix centred on nuclear. Advanced AI workloads nonetheless run on imported NVIDIA GPUs and standard European grid arrangements; however, there is no dedicated, ultra low cost AI energy moat comparable to Norway's hydropower clusters or Gulf states' subsidised energy.
- **Semiconductor & Hardware Independence (2)** France participates in the European Chips Act and has design and R&D capabilities, but no domestic leading edge fabs. Advanced AI workloads still depend on imported

GPUs and overseas manufacturing in Taiwan, Korea and the US. *Source: European Commission, Bloomberg*

- **Cloud & Infrastructure Autonomy (3)** The French ecosystem has developed a set of "trusted cloud" and sovereign cloud offers - OVHcloud certified SecNumCloud, OBS, Outscale, Numspot, etc. - which guarantee the localization of data in France and governance subject to European law. Some of these offers are based on American hyperscaler technologies but under French or European governance, which strengthens legal and operational sovereignty, without removing dependence on imported basic hardware and software.

- **Model & Data Independence (3)** France now hosts one of the world's leading open weight model vendors in Mistral, whose models (Mixtral, 8×22B, etc.) are explicitly positioned as European alternatives to US closed models. This is a clear step beyond other EU states in terms of symbolic and ecosystem leadership. However, Mistral and other French models still train almost entirely on imported GPUs, rely on global cloud infrastructure, and French enterprises continue to use US closed models at scale for many high stakes workloads. From a sovereignty perspective, this still corresponds to a hybrid dependence profile rather than "mostly independent", hence a score of 3+.

- **Talent & R&D Ecosystem (4)** With INRIA, CNRS, top Grandes Écoles and a dense startup ecosystem around Paris, France has deep AI research capacity and is one of Europe's main talent magnets. It is not as dominant as the US or China in sheer scale, but punches above its weight in algorithms and open-weight models. *Source: Noema, Skema Publika*

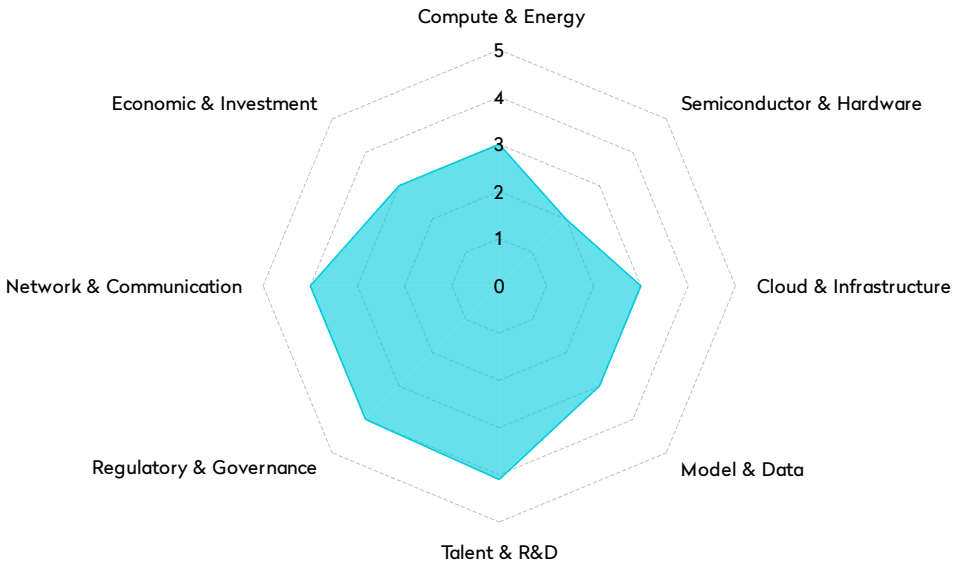
- **Regulatory & Governance Resilience (5)** France operates inside the GDPR and EU AI Act framework and has additional requirements through ANSSI and SecNumCloud, making it a benchmark for stringent cloud and AI governance. S3NS and similar regimes show how law and certification can be used as sovereignty tools even when hardware is foreign. *Source: European Commission, ANSSI*

- **Network & Communication Resilience (4)** France is a major European internet and data centre hub connected to multiple submarine cables and peering points, with robust telecom operators and IXPs. It is not as concentrated a connectivity hub as the Netherlands, but still enjoys high redundancy and reliability. *Source: Google Cloud, TeleGeography*

- **Economic & Investment Continuity (4)** The French state, Bpifrance and private capital have committed multi-billion euro funding across AI, HPC, and startups like Mistral, with strong EU co-funding through programmes such as EuroHPC and the Chips Act. The only reason this is not a 5 is that resources are still modest relative to the US / China and fragmented across EU instruments. *Source: Bpifrance, European Commission*

GERMANY

Germany is an industrial AI heavyweight with strong research institutions and significant public budgets, but it has been slower than France in building visible sovereign clouds or open-weight champions. Initiatives like Delos Cloud for the public sector and EU AI "gigafactories" move it toward greater operational control, yet GPU dependence, fragmented execution and slower model innovation keep it in the medium-sovereignty bracket.



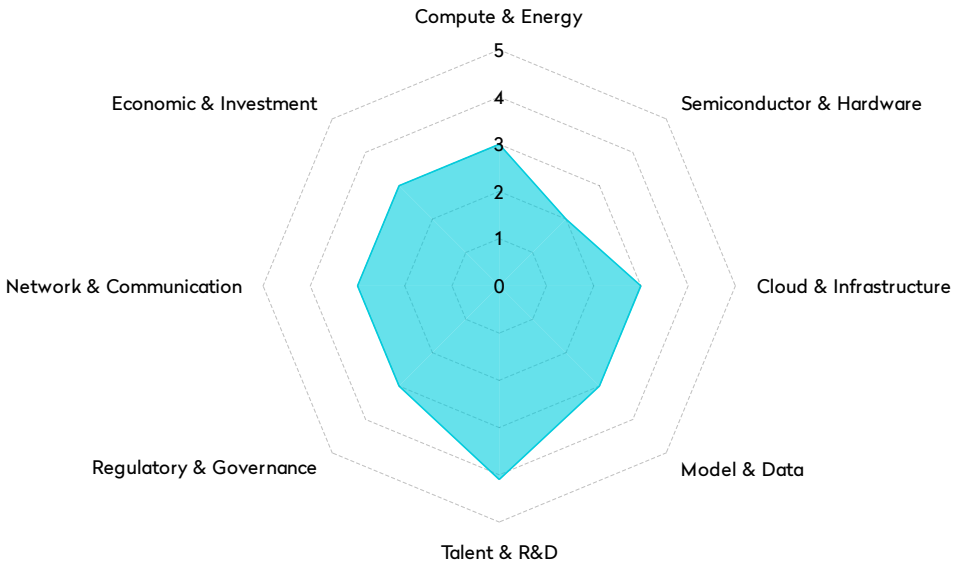
- **Compute & Energy Sovereignty (3)** Germany participates in EuroHPC and operates large national HPC systems for science and industry, while also hosting major hyperscaler data centres. Energy is relatively secure but high cost and part of an integrated EU grid, with no special AI energy moat comparable to Norway or parts of the Gulf. Source: EuroHPC, *Reuters*
- **Semiconductor & Hardware Independence (2)** Germany is a major automotive and industrial electronics base and has attracted Intel foundry investments under the EU Chips Act, but still lacks domestic leading edge AI chip manufacturing and relies heavily on TSMC, Samsung and US GPU vendors. *Source: European Commission, Intel*
- **Cloud & Infrastructure Autonomy (3)** The Delos Cloud joint venture

with SAP and Arvato is designed as a sovereign cloud for the German public sector, yet it uses hyperscaler technology and imported hardware. Broader German cloud use is split between domestic providers and US hyperscalers, resulting in a hybrid, medium-autonomy posture. *Source: Delos Cloud, American German Institute*

- **Model & Data Independence (3)** Germany excels in applied and industrial AI but lacks a flagship general purpose LLM equivalent to Mistral or LLaMA. Several research projects and sectoral models exist, and the country benefits from EU-level open data and AI programmes, yet most frontier models used in production remain foreign. *Source: American German Institute, European Commission*
- **Talent & R&D Ecosystem (4)** With institutions such as the Max Planck Society, Fraunhofer, and strong university clusters, Germany has one of Europe's deepest R&D ecosystems, particularly in robotics, manufacturing and industrial AI. It is behind the US and China on volume but remains a global research centre. *Source: American German Institute, MVProMedia*
- **Regulatory & Governance Resilience (4)** Germany is tightly integrated into GDPR and the EU AI Act process and has its own updated national AI strategy emphasising safety, industrial strength and public sector use. Its governance strength lies primarily in alignment with EU-level regulation rather than bespoke German AI law. *Source: European Commission, Federal Government of Germany*
- **Network & Communication Resilience (4)** Germany is one of Europe's main internet transit and data centre hubs, with strong telecom operators and dense cross-border connectivity. While there are ongoing debates about rural broadband, the backbone for AI workloads is robust. *Source: American German Institute, TeleGeography*
- **Economic & Investment Continuity (3)** The federal government earmarked around €5.5 billion for AI and participates in multiple EU funding schemes, but experts frequently note lagging commercialization, complex bureaucracy and slower startup scaling compared with the US or UK. *Source: Reuters, European Commission*

INDIA

India's strength is breadth rather than depth: a huge talent pool, ambitious public infrastructure programmes, and a coherent narrative around "open yet local" sovereignty create real medium term leverage. At the same time, India is still heavily dependent on imported GPUs and foreign clouds, and its AI budgets are modest per capita compared to the US, China, or Japan. It scores well on human capital and governance intent, but actual compute and semiconductor sovereignty are still in the building phase.



- **Compute & Energy Sovereignty (3)** The IndiaAI Mission targets large scale public compute and has already moved from an initial 10,000 GPU goal to around 38,000 GPUs offered at roughly 65 per hour through a subsidised national platform, which is a substantial step toward sovereign capacity. However, the underlying hardware is imported and constrained by US export controls, and grid bottlenecks remain, especially for high density AI data centers. *Source: CyberMedia IndiaAI analysis, Press Information Bureau on IndiaAI*
- **Semiconductor & Hardware Independence (2)** India has announced multiple semiconductor fab projects and incentive schemes, but it still lacks operational advanced node fabs and depends on imported GPUs and ASICs for AI workloads. Foundational chip

sovereignty remains aspirational. *Source: India Semiconductor Mission overview, Express Computer on IndiaAI and chips*

- **Cloud & Infrastructure Autonomy (3)** India combines public sector data centers and domestic cloud providers with heavy reliance on global hyperscalers like AWS, Azure, and Google Cloud. IndiaAI Compute and certain sovereign cloud projects add resilience, but most workloads still run on foreign technology stacks under foreign jurisdictions. *Source: Neysa on IndiaAI Compute, Atlantic Council on India's digital public infrastructure*

- **Model & Data Independence (3)** India emphasises open source and linguistic sovereignty through initiatives such as the Bhashini platform for 22 Indian languages and emerging Indic LLMs. The DPDP rules aim to require local storage and processing for AI models that use Indian data. However, India still leans on foreign foundation models and hardware, so model independence is partial. *Source: Bhashini mission, Tech Policy Press on DPDP and AI*

- **Talent & R&D Ecosystem (4)** India has a very large base of software engineers and data scientists, strong CS programmes, and global IT service champions. It is one of the few countries that can supply AI talent both domestically and to the rest of the world. The main challenge is retaining top researchers and moving from services to product and platform innovation. *Source: Red Hat on India's AI talent, Atlantic Council on India's digital ecosystem*

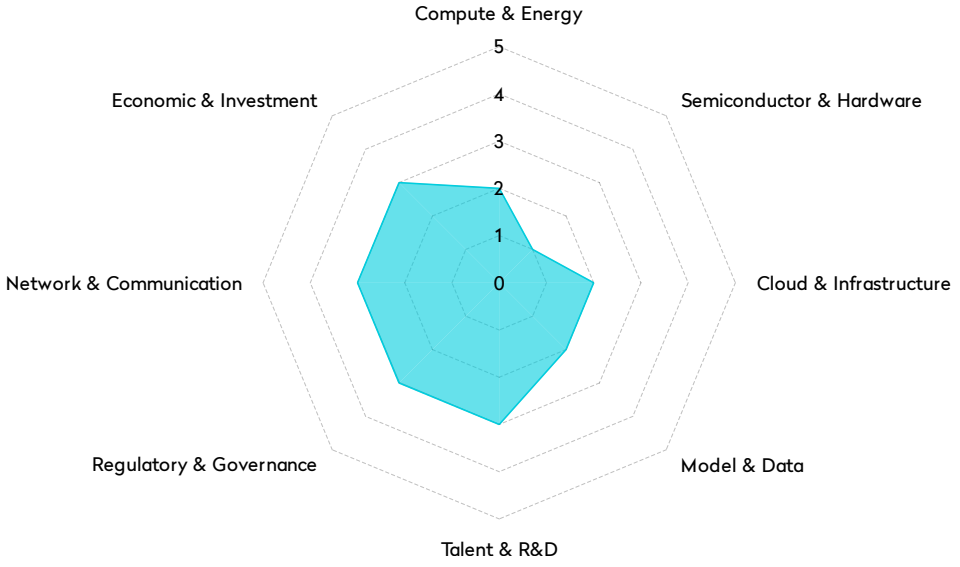
- **Regulatory & Governance Resilience (3)** The DPDP Act, sectoral guidelines, and forthcoming AI rules show an increasing focus on data protection and AI risk, but the framework is still evolving and less detailed than the EU AI Act or some national regimes. India is balancing innovation, openness, and strategic autonomy rather than maximising any single dimension. *Source: Economic Times explainer on DPDP, Tech Policy Press on India AI governance*

- **Network & Communication Resilience (3)** India has strong fibre and mobile coverage in major urban areas, extensive 4G and expanding 5G, but connectivity is still uneven across rural regions, which constrains nationwide AI deployment and edge intelligence. *Source: Oxford University Press on India's digital divide, TRAI statistics via government portals*

- **Economic & Investment Continuity (3)** The IndiaAI Mission is backed by funding of about 10,372 crore (approximately 1.2 billion US dollars) plus ongoing DPI investment. This is meaningful, but small compared to the hundreds of billions in planned US or Chinese AI and chip programmes, and it is vulnerable to future fiscal reprioritisation. *Source: Press Information Bureau, Atlantic Council*

INDONESIA

Indonesia is in the early stages of an AI sovereignty journey, anchored in a national AI roadmap that explicitly targets foreign investment and future sovereign-AI capacity. Hyperscalers currently provide most compute and cloud capability, while the country explores a sovereign-AI fund and partnerships with firms such as Microsoft and NVIDIA. Its strengths are demographic scale, political focus and growing talent initiatives; its weaknesses are full dependence on imported chips, foreign-owned cloud, and nascent model development.



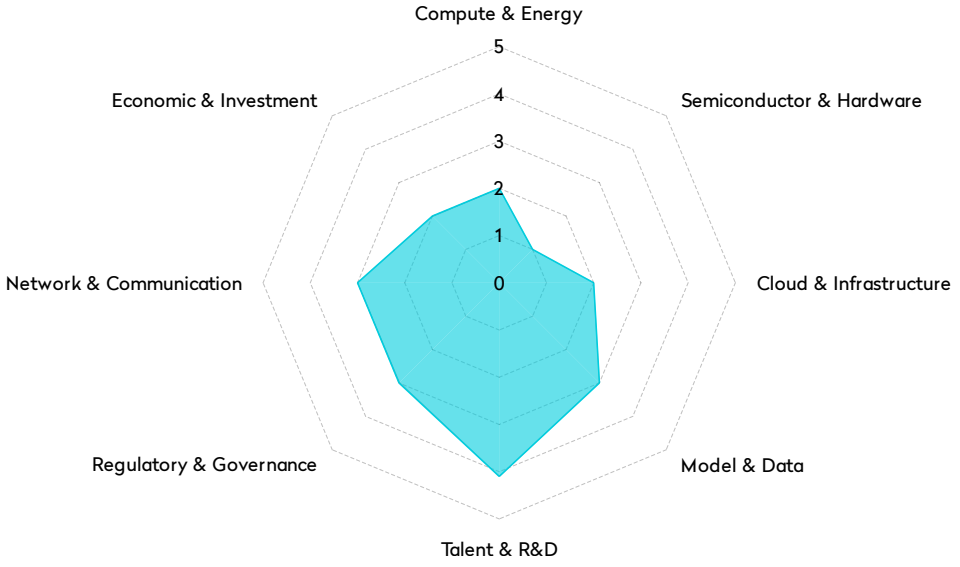
- **Compute & Energy Sovereignty** – 2 Today, AI workloads rely heavily on foreign hyperscalers, and while Indonesia is expanding data centers and exploring AI-specific infrastructure, it does not yet operate large sovereign AI clusters integrated with its own energy system. *Source: White & Case*
- **Semiconductor & Hardware Independence** – 1 Indonesia has no domestic semiconductor fabs and is fully reliant on imported chips and GPUs from the US, China, Taiwan and others, even as it positions itself as an investment destination for AI infrastructure. *Source: White & Case*
- **Cloud & Infrastructure Autonomy** – 2 The country's AI roadmap focuses on attracting cloud investments and establishing a sovereign AI fund by 2027–2029, but current cloud capacity is dominated by foreign hyperscalers,

with limited local control over the software stack. *Source: White & Case*

- **Model & Data Independence** – 2 Indonesia's AI strategy highlights domestic use cases and public services, yet indigenous frontier models and large-scale datasets remain limited; it instead relies on collaborations with players such as Huawei and GoTo for applied AI. *Source: UN ESCAP*
- **Talent & R&D Ecosystem** – 3 Public–private partnerships and education initiatives are ramping up AI skills development, but research capacity and advanced AI expertise still lag behind regional leaders like Singapore and South Korea. *Source: UN ESCAP*
- **Regulatory & Governance Resilience –** 3 Indonesia is aligning its AI policies with ASEAN's principles of inclusivity and ethics and has issued strategic documents outlining governance directions, yet detailed AI-specific regulation and assurance mechanisms are still in formation. *Source: UN ESCAP*
- **Network & Communication Resilience** – 3 Connectivity is improving through submarine cables and mobile expansion, but the archipelago still faces uneven coverage and latency issues outside major urban centers, which constrains AI deployment in more remote regions. *Source: UN ESCAP*
- **Economic & Investment Continuity –** 3 Microsoft has announced around 1.7 billion dollars of AI and cloud investment and NVIDIA has signalled hundreds of millions more, while the government is designing a sovereign AI fund; however, the funding base is still forming and heavily reliant on foreign capital. *Source: White & Case*

ISRAEL

Israel is a global leader in AI talent, cybersecurity and dual-use innovation, but its sovereign AI ambitions remain constrained by limited domestic compute, reliance on imported chips, and repeated delays in deploying a national AI supercomputing facility. While Hebrew and Arabic language models exist and defence-driven applied AI remains strong, the country lacks large sovereign LLMs and consistently underfunds its own AI roadmap. Israel's greatest strength is human capital; its greatest weakness is strategic under-investment and infrastructure dependency.



- **Compute & Energy Sovereignty (2)** Israel planned a Nebius-backed sovereign AI supercomputer, but the project has been delayed and current sovereign compute capacity remains modest. The country also faces energy constraints and no hyperscale domestic GPU clusters. *Source: EU Reporter*
- **Semiconductor & Hardware Independence (1)** Israel has chip design expertise (Intel, Mobileye), but no domestic cutting-edge fabrication and remains fully dependent on imported GPUs and processors. *Source: Israel Innovation Authority*
- **Cloud & Infrastructure Autonomy (2)** Israel hosts some national data centres, but most AI workloads run on AWS, Microsoft Azure or Google Cloud. Sovereign cloud ambitions have advanced slowly. *Source: Israel Tech Insider*

- **Model & Data Independence (3)** Israel has Hebrew and Arabic models and strong defence AI capabilities. However, it lacks a large-scale sovereign LLM at parity with frontier systems. *Source: AI Israel*

- **Talent & R&D Ecosystem (4)** Israel ranks among the world's top AI innovation hubs, with deep cybersecurity and military-tech integration such as Unit 8200 and strong academic institutions. *Source: Israel Innovation Authority*

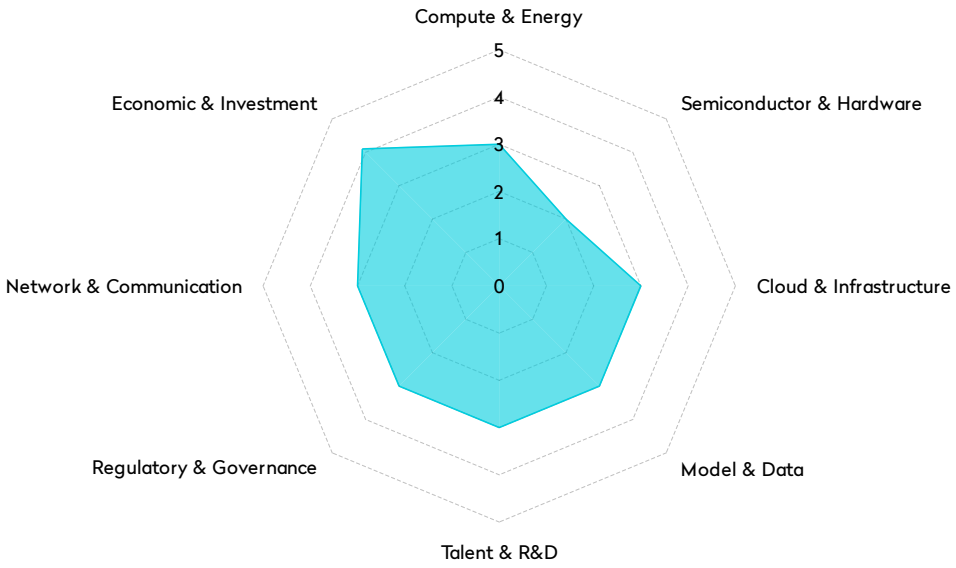
- **Regulatory & Governance Resilience (3)** Israel has an AI national programme, but implementation lags strategy documents and regulatory clarity remains evolving. *Source: Israel Desks*

- **Network & Communication Resilience (3)** Israel has strong telecom infrastructure but faces geopolitical and security vulnerabilities that reduce resilience. *Source: EU Reporter*

- **Economic & Investment Continuity (2)** Israel announced a NIS 25B AI strategy, but only ~20 percent has been funded, and budget instability has slowed progress. *Source: Israel Tech Insider*

ITALY

Italy's AI sovereignty strategy is infrastructure-centric: it leverages national and EuroHPC supercomputers such as Leonardo and partners with NVIDIA for the DomyN AI factory, while working on domestic models and applications. It has decent public funding and a respectable research base, but limited chip autonomy, middling connectivity and still-maturing AI governance keep it in the mid-resilience band.



- **Compute & Energy Sovereignty (3)** CINECA operates Leonardo, one of Europe's top supercomputers, and Italy is building an AI factory with NVIDIA Grace Blackwell hardware to support national AI workloads. Energy is relatively stable but not uniquely sovereign or low cost compared with Norway or the Gulf. *Source: CINECA, NVIDIA*

- **Semiconductor & Hardware Independence (2)** Italy has no advanced semiconductor fabs and relies entirely on imported GPUs and processors, although it participates in EU Chips Act initiatives and European semiconductor supply chain projects. *Source: European Commission, NVIDIA*

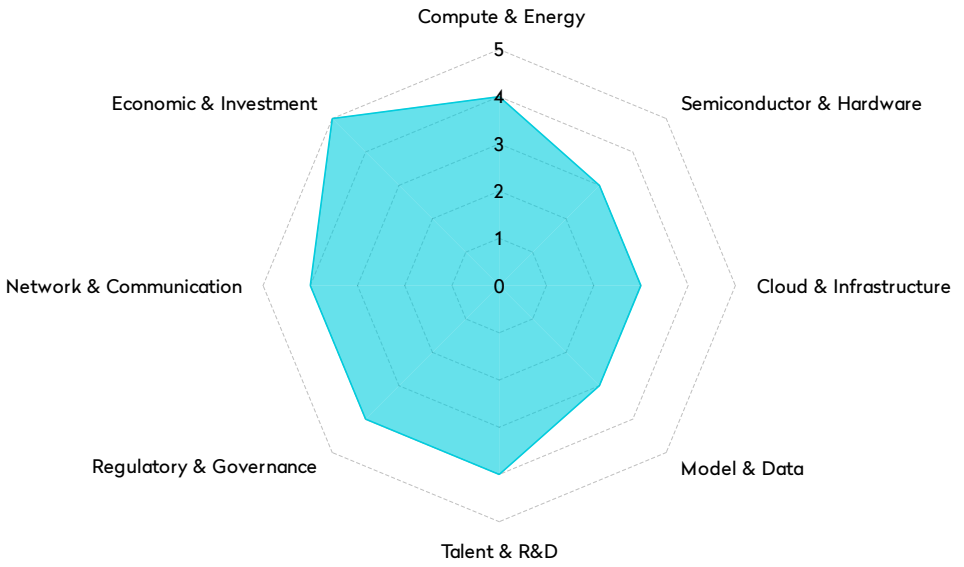
- **Cloud & Infrastructure Autonomy (3)** National HPC centres, EuroHPC participation and regional providers give Italy some autonomous

infrastructure, but most AI workloads still sit on foreign hardware and commercial cloud services. DomyN and CINECA improve control over the infrastructure layer without changing chip dependence. *Source: CINECA, EuroHPC*

- **Model & Data Independence (3)** Italy is backing domestic models within EuroHPC and national projects and experimenting with Italian language and sectoral LLMs, yet there is no flagship Italian model comparable to Mistral or LLaMA. Italy remains mostly a user and adapter of foreign foundation models. *Source: Italian AI Programme, NVIDIA*
- **Talent & R&D Ecosystem (3)** Italian universities and research centres have solid but not top tier global AI footprints. The talent base in AI and data science is growing, but brain drain and limited scale compared with France or Germany keep this at a mid-level score. *Source: AGID, European Commission*
- **Regulatory & Governance Resilience (3)** Italy aligns with GDPR and the EU AI Act and has a national AI strategy, but governance frameworks are still being operationalised. There is less evidence of the kind of sophisticated cloud sovereignty regimes seen in France. *Source: AGID, European Commission*
- **Network & Communication Resilience (3)** Italy is reasonably well connected through European backbones and submarine cables, but is not a primary IX or data hub on the scale of the Netherlands or Germany. Connectivity is adequate rather than strategically dominant. *Source: TeleGeography, CINECA*
- **Economic & Investment Continuity (4)** Public investments of several billion euros in HPC and AI, plus EU funding, give Italy a reasonably strong and durable capital base. While not at French or German scale, the commitments around Leonardo and DomyN indicate sustained support. *Source: NVIDIA, Italian Government*

JAPAN

Japan is pursuing a dual-track AI sovereignty strategy: massive state-led investment to restore semiconductor autonomy (via Rapidus 2 nm fabrication) and large-scale national compute through NTT and Sakura, combined with a pragmatic partnership model using OpenAI's "Gennai" for government. Japan's strength is its long-term commitment, scale of funding and industrial R&D maturity. Its weaknesses remain reliance on US chips until Rapidus matures and a cloud ecosystem that still leans on global hyperscalers.

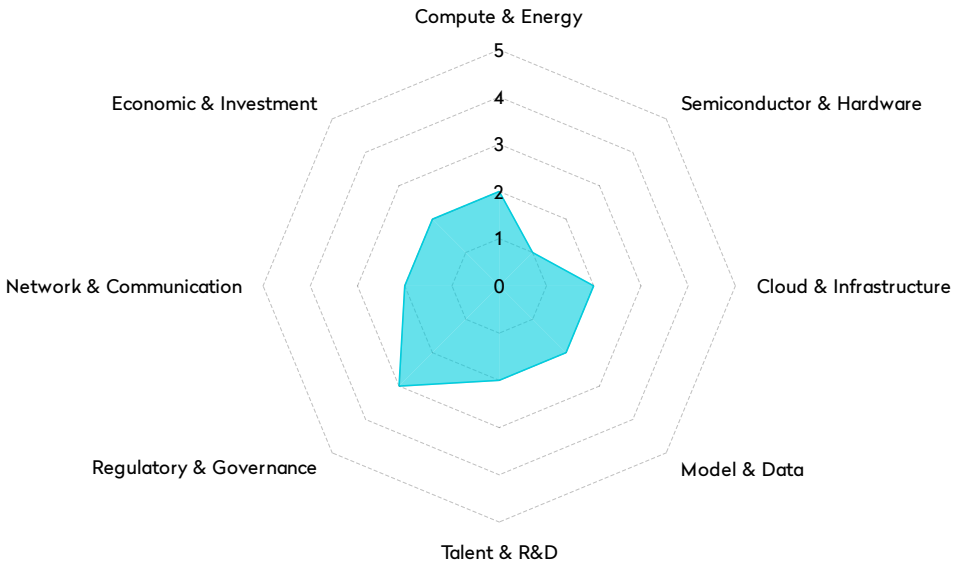


- **Compute & Energy Sovereignty (4)** Japan is scaling domestic data centres with major investments from Sakura and NTT, building national AI compute platforms and leveraging a stable grid. *Source: IT Business Today, IntroL*
- **Semiconductor & Hardware Independence (3)** The Rapidus 2nm fab backed by ¥1.05 trillion of government funding is a major step, but Japan still relies on imported AI chips until at least 2027–2028. *Source: IT Business Today, IntroL*
- **Cloud & Infrastructure Autonomy (3)** Domestic cloud providers (NTT, Sakura) offer local control, but the country's enterprise cloud landscape still leans heavily on AWS, Azure and Google Cloud. *Source: IT Business Today*

- **Model & Data Independence (3)** Japan develops domestic models but also uses OpenAI's Gennai for public-sector deployments, creating a hybrid sovereignty profile. *Source: TechChannels, IT Business Today*
- **Talent & R&D Ecosystem (4)** Japan has a deep engineering workforce, significant R&D spending and strong industrial innovation via NTT, Sony, Hitachi and university centres. *Source: IT Business Today*
- **Regulatory & Governance Resilience (4)** Japan's AI Promotion Act is pro-innovation with voluntary compliance, balancing flexibility and governance. *Source: Elastic, IT Business Today*
- **Network & Communication Resilience (4)** Japan maintains one of the strongest submarine cable footprints in Asia and world-class broadband. *Source: IT Business Today*
- **Economic & Investment Continuity (5)** Japan's ~¥10 trillion programme to 2030 plus corporate CAPEX such as NTT's USD $59 billion investment make it one of the most financially committed AI nations globally. *Source: IT Business Today, IntroL*

KENYA

Kenya is positioning itself as an early African mover in AI policy, with a national AI strategy that emphasises skills, governance and social impact. However, it remains at the very beginning of the sovereignty journey: compute, chips, and cloud are almost entirely imported; local model development is limited; and connectivity and capital are uneven. Its strength is a relatively forward-looking governance and skills agenda; its weakness is a thin infrastructure and investment base.



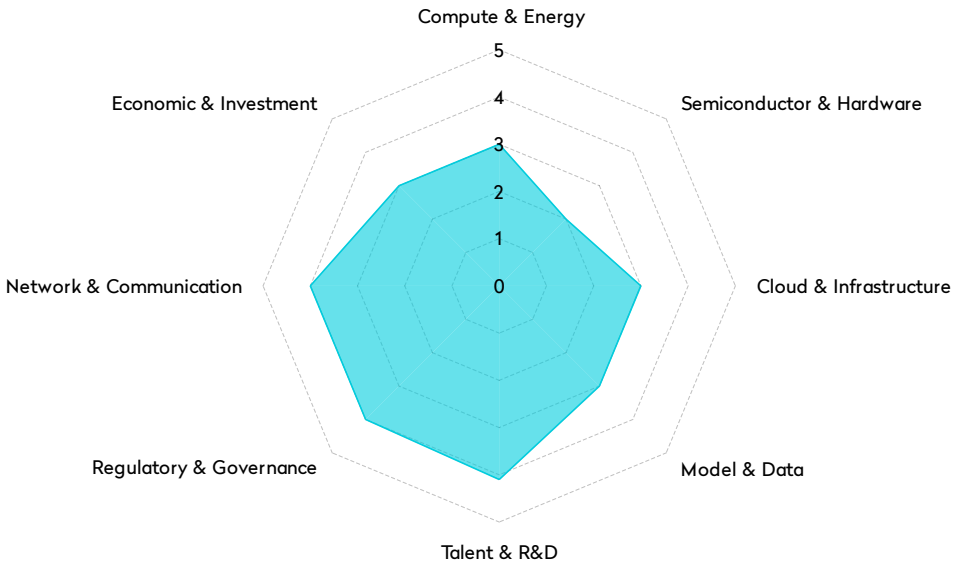
- **Compute & Energy Sovereignty (2)** Kenya's AI strategy recognises the need for increased compute and data-center capacity, but current infrastructure is limited and not specialised for large-scale AI training. Energy reliability and capacity for heavy AI workloads remain constrained. *Source: Government of Kenya – National AI Strategy*

- **Semiconductor & Hardware Independence (1)** 1 Kenya has no domestic semiconductor manufacturing; all AI hardware is imported, and there are no near-term plans in the strategy to alter this situation, so hardware dependence is total. *Source: Government of Kenya – National AI Strategy*

- **Cloud & Infrastructure Autonomy (2)** The strategy anticipates growing cloud and data-center capacity, but much of this will be provided by global hyperscalers and regional providers. There is talk of digital infrastructure investment, but not yet a mature sovereign cloud stack. *Source: Government of Kenya – National AI Strategy*
- **Model & Data Independence (2)** Policy documents focus on data protection and ethical AI use more than on building national LLMs. Local model development is limited to early projects and academic work, with most AI tools imported or adapted from foreign platforms. *Source: Government of Kenya – National AI Strategy*
- **Talent & R&D Ecosystem (2)** Kenya is launching AI literacy programs, STEM reforms and centers of excellence, but currently faces significant skills gaps and limited advanced AI research capacity, which constrains local innovation and governance capability. *Source: Government of Kenya – National AI Strategy*
- **Regulatory & Governance Resilience (3)** The national AI strategy sets out ethical guidelines, governance priorities and institutional responsibilities, giving Kenya a relatively structured policy baseline compared to many peers at similar income levels, though detailed regulations remain to be implemented. *Source: Government of Kenya – National AI Strategy*
- **Network & Communication Resilience (2)** Kenya has high mobile penetration and improving broadband, yet coverage and capacity outside major cities remain patchy, with frequent network disruptions and limited redundancy for critical AI workloads. *Source: Government of Kenya – National AI Strategy*
- **Economic & Investment Continuity (2)** AI investment is in its infancy and relies heavily on donor funding, development finance and limited domestic capital. The strategy sets ambitions but does not yet secure large, long-term domestic funding lines for AI infrastructure. *Source: Government of Kenya – National AI Strategy*

NETHERLANDS

The Netherlands is a **strategic enabler** of global AI rather than a self-contained stack: it hosts ASML, the key supplier of EUV lithography tools, and acts as a major European data and connectivity hub, while planning a national AI facility backed by public funding. However, it has no leading edge fabs of its own and continues to depend on imported GPUs and hyperscaler infrastructure. Its strengths lie in research, regulatory sophistication and network centrality.



- **Compute & Energy Sovereignty (3)** The Dutch government has approved plans for a national AI facility, backed by the National Growth Fund, which will provide HPC and AI compute to researchers and businesses. Energy availability is generally good and increasingly green, but integrated into EU power markets and not uniquely sovereign. *Source: Government of the Netherlands, SURF*

- **Semiconductor & Hardware Independence (2)** The Netherlands hosts ASML, which effectively controls global supply of EUV lithography tools and plays a central role in export controls, but it does not operate domestic leading edge fabs for AI chips. Dutch AI workloads still rely on imported GPUs and CPUs manufactured abroad. *Source: ASML, Deloitte*

- **Cloud & Infrastructure Autonomy (3)** As one of Europe's largest data centre and cloud hubs, the Netherlands hosts both hyperscaler regions and domestic providers and is exploring sovereign cloud and AI infrastructure. However, core hardware and many platforms are still foreign. *Source: Government of the Netherlands, SURF*

- **Model & Data Independence (3)** Dutch research institutes contribute to European open data and AI projects, and there is active work on domain-specific and language models, but no flagship Dutch general purpose LLM on par with Mistral or LLaMA. Sovereignty is primarily realised via EU-level initiatives. *Source: SURF, Netherlands AI Coalition*

- **Talent & R&D Ecosystem (4)** Universities like TU Delft, University of Amsterdam and research organisations such as TNO create a dense AI and data science ecosystem, and the Netherlands ranks high on AI readiness and innovation indices. *Source: Netherlands AI Coalition, Government of the Netherlands*

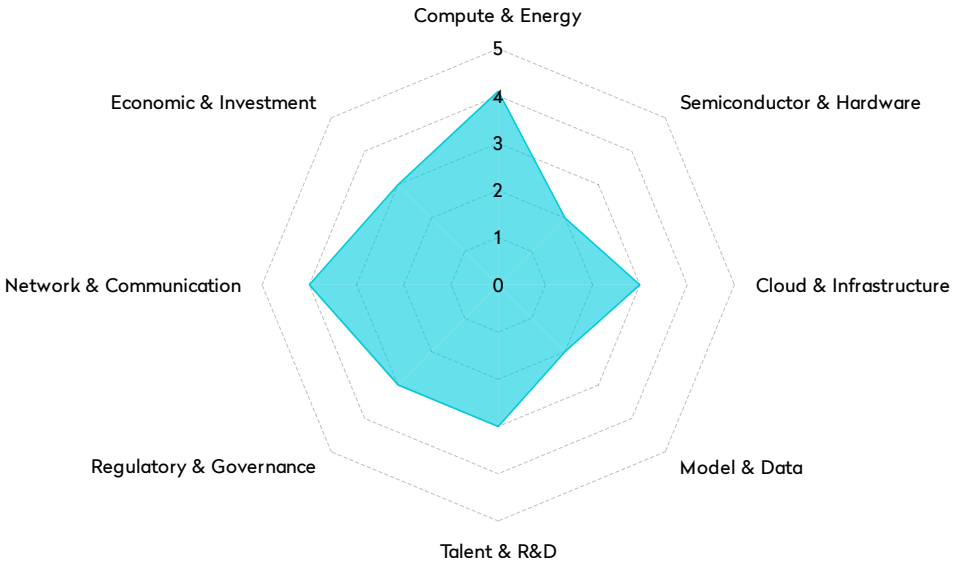
- **Regulatory & Governance Resilience (4)** The Netherlands fully implements GDPR and will implement the EU AI Act, and has already used export controls and cyber interventions around ASML as tools of digital sovereignty. This gives it a strong governance position relative to its size. *Source: Government of the Netherlands, Deloitte*

- **Network & Communication Resilience (4)** Amsterdam and surrounding regions form one of Europe's largest internet exchange and data centre clusters, with AMS-IX as a major global peering point and several submarine cable landings. This makes the Netherlands a highly resilient connectivity hub. *Source: AMS-IX, TeleGeography*

- **Economic & Investment Continuity (3)** Approximately €204.5 million has been allocated from the National Growth Fund for AI infrastructure and research, which is significant for a mid-sized country but modest compared with the US, China or even France. Sustained prioritisation will be needed to scale beyond a regional hub role. *Source: Government of the Netherlands, SURF*

NORWAY

Norway combines genuine energy sovereignty with one of the most ambitious AI data center projects in Europe, yet it has outsourced most of the AI stack above the power and land layers. Stargate Norway gives the country renewable, large-scale AI compute on its soil, but model control, GPU supply and much of the cloud stack are controlled by OpenAI and US vendors. Norway's strength is being an energy-secure, politically stable host for European AI infrastructure; its weakness is limited domestic model development, no semiconductor base, and economic dependence on the strategy of foreign partners.



- **Compute & Energy Sovereignty (4)** Norway is hosting Stargate Norway, OpenAI's first European data center, with plans for 100,000 NVIDIA GPUs by 2026 (initial 230 MW, expandable toward 520 MW), entirely powered by local hydropower and designed for efficient liquid cooling and heat reuse. This is real compute and energy sovereignty at the physical layer, but control of GPUs and scheduling is still tied to OpenAI's strategy, so it does not reach 5. *Source: ITPro*
- **Semiconductor & Hardware Independence (2)** Norway has no domestic advanced semiconductor manufacturing and relies entirely on imported NVIDIA GPUs and other foreign hardware. Even though it can negotiate good terms as a strategic data-center host, it remains exposed to US export controls and vendor

roadmaps. *Source: ITPro*

- **Cloud & Infrastructure Autonomy (3)** The Nscale–Aker joint venture owns and operates the facility in Norway, giving domestic control over land, power and data center operations. However, the higher layers (orchestration, models, and much of the software stack) are controlled by OpenAI and US vendor ecosystems, which caps autonomy at a moderate level. *Source: Wall Street Journal*

- **Model & Data Independence (2)** Stargate Norway localizes data and compute for European customers, but the core models remain OpenAI foundation models. Norway does not yet field sovereign national LLMs or independent training pipelines at scale, so model and data sovereignty remain limited. *Source: TechRadar Pro*

- **Talent & R&D Ecosystem (3)** Norway has a solid but relatively small AI research base, anchored in its universities and industrial digitalisation programs, but it is not a global AI research hub on the scale of the US, China, or even France and Germany. *Source: World Economic Forum*

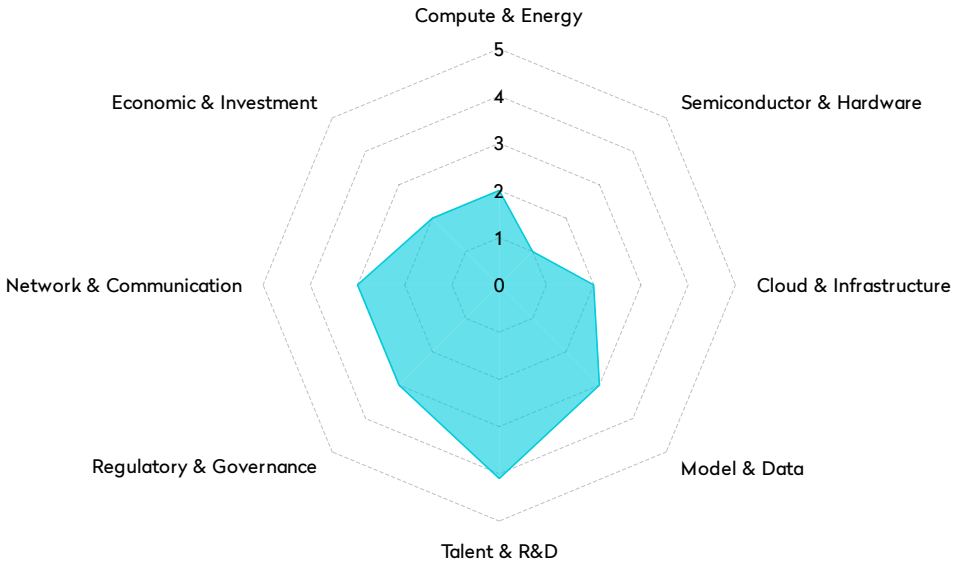
- **Regulatory & Governance Resilience (3)** As part of the EEA, Norway aligns with EU data protection and emerging AI governance norms, giving it solid but derivative regulatory resilience. It does not yet have a distinct, leading AI sovereignty regime comparable to France's SecNumCloud framework. *Source: European Commission*

- **Network & Communication Resilience (4)** Norway has robust connectivity into European networks, including major subsea cables and a modern national telecoms infrastructure, and is increasingly used as a Nordic data center hub. This supports high network resilience, even if many backbone routes still traverse other European states. *Source: W.Media*

- **Economic & Investment Continuity (3)** The initial Stargate Norway phase is backed by about 1 billion dollars from Nscale and Aker, with room for expansion, but overall AI funding is project-centric rather than part of a massive national AI industrial strategy. Norway is financially strong, yet capacity remains modest relative to the US, China, or even Saudi Arabia. *Source: ITPro*

RUSSIA

Russia is a special case but worth mentioning, as its own category. Russia's model is **forced autarky**, driven by sanctions, not choice. This involves low-performance domestic hardware, parallel ecosystems, and BRICS-aligned research, not an alliance or full-stack design. While Russia has domestic LLMs (Gigachat, Yandex) and strong foundational depth in computer science, Western export controls severely limit access to frontier GPUs, advanced chips, and global cloud services, necessitating reliance on China and workarounds. Despite efforts for sovereign cloud autonomy, sanctions constrain growth, resulting in partial model sovereignty but severe infrastructure limits.

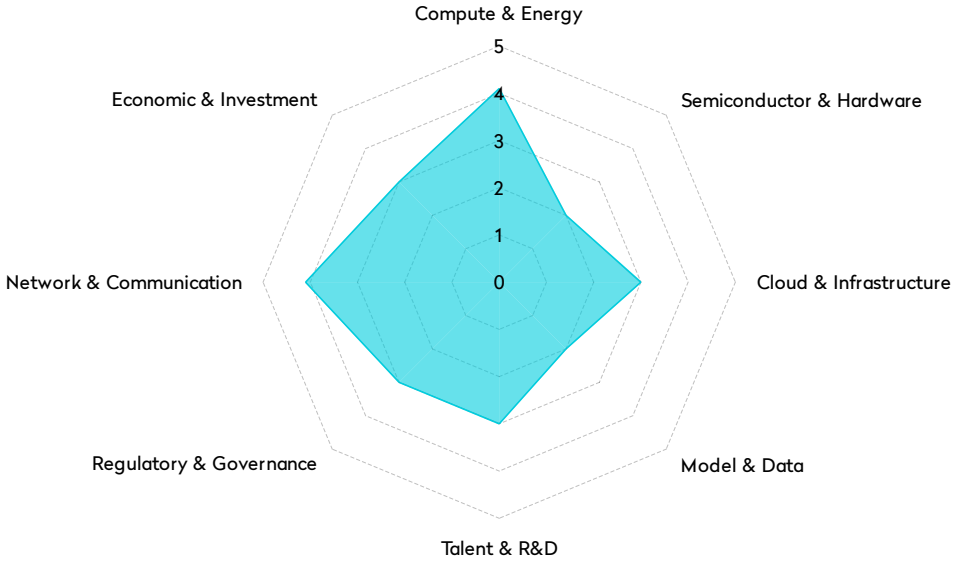


- **Compute & Energy Sovereignty (2)** Russia has energy abundance but lacks access to advanced AI hardware, severely limiting compute for training frontier models. *Source: AINvest Russia AI Sovereignty*
- **Semiconductor & Hardware Independence (1)** Russia has no advanced fabs and is blocked from acquiring high-end GPUs or EUV tools, relying on grey imports and Chinese suppliers. *Source: DigWatch – Kremlin Domestic AI Push*
- **Cloud & Infrastructure Autonomy (2)** Russia runs its own national cloud services but lacks hyperscale capability and depends increasingly on Chinese tech to bypass sanctions. *Source: AINvest*

- **Model & Data Independence (3)** Local models like Gigachat and Yandex GPT variants exist, but progress is slowed by limited compute and isolation from global research. *Source: AINvest*
- **Talent & R&D Ecosystem (3)** Russia has strong STEM traditions but has lost significant talent to emigration since 2022. *Source: AINvest*
- **Regulatory & Governance Resilience (3)** Russia has mandated domestic AI solutions in public bodies and centralizes AI governance, but the regulatory system is less mature than the EU or US. *Source: DigWatch*
- **Network & Communication Resilience (3)** Russia controls domestic internet backbone and has tested internet isolation, but sanctions undermine access to components. *Source: AINvest*
- **Economic & Investment Continuity (2)** Russia's AI plans depend on limited domestic capital and Chinese partnerships amid sanctions and capital flight. *Source: DigWatch*

SAUDI ARABIA

Saudi Arabia is trying to buy its way into AI resilience through energy and capital. Vision 2030 backs a rapid build-out of AI data centers, leveraging cheap domestic energy and sovereign wealth funding, and Riyadh is becoming a major buyer of accelerators and hyperscale infrastructure. Yet the kingdom has almost no local semiconductor fabrication, depends on US and allied vendors for GPUs and cloud technology, and is only beginning to develop its own models and talent base. Its strength is financial and energy-backed acceleration; its weakness is structural dependency on foreign hardware and software.



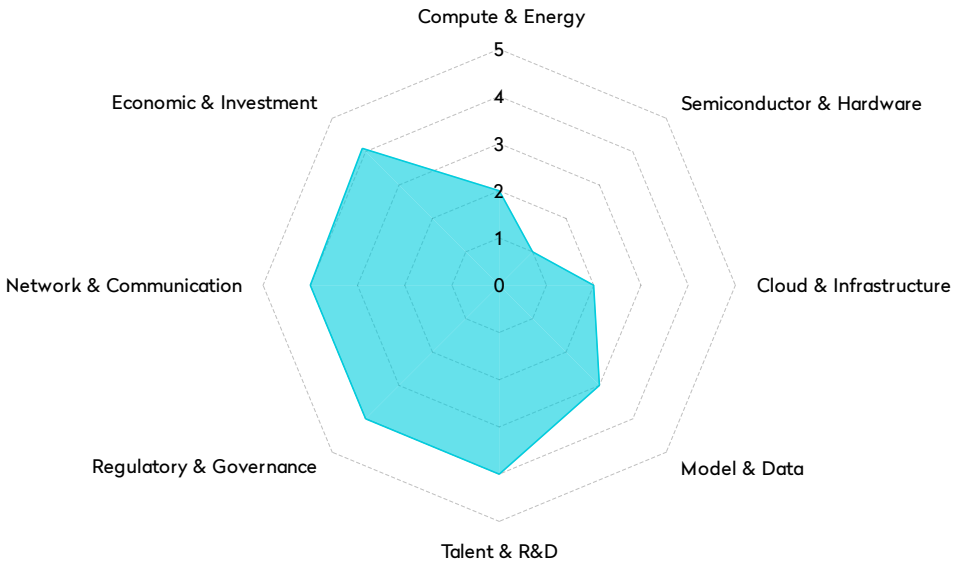
- **Compute & Energy Sovereignty (4)** Saudi Arabia is investing to build what analysts estimate could be 6.6 GW of AI data center capacity, with 33 data centers in operation and 42 under construction, backed by abundant domestic oil and growing renewables under Vision 2030. This gives strong domestic compute hosting on top of sovereign energy, although GPUs and system designs are still imported. *Source: Financial Times*

- **Semiconductor & Hardware Independence (2)** Saudi Arabia has no advanced semiconductor fabs and depends on foreign suppliers for GPUs and accelerators. Reports note large purchases of NVIDIA chips and discussions with alternative accelerator vendors, but the kingdom remains on the consumption side of the hardware stack. *Source: Associated Press*

- **Cloud & Infrastructure Autonomy (3)** Saudi initiatives, including joint ventures with Google Cloud and others, mean that AI workloads can be hosted in-kingdom under Saudi law, but the cloud software layers, orchestration tools and many security primitives remain foreign-owned, so autonomy is medium rather than high. *Source: MIT Technology Review*
- **Model & Data Independence (2)** National AI programmes are focused on sectoral applications and analytics, yet Saudi Arabia still relies mainly on imported models and platforms from US and allied vendors. There are emerging Arabic-focused AI projects, but no large sovereign LLM ecosystem comparable to UAE's Falcon or China's DeepSeek. *Source: Brookings Institution*
- **Talent & R&D Ecosystem (3)** The kingdom is investing in AI institutes, scholarships and research collaborations as part of Vision 2030, but domestic AI research capacity is still developing and depends significantly on imported expertise and partnerships. *Source: Brookings Institution*
- **Regulatory & Governance Resilience (3)** Governance frameworks for AI and data are emerging, tightly coupled with national security and economic diversification goals, but remain less mature and transparent than EU-style regimes. This gives the state strong steering power but with unclear checks and balances. *Source: Brookings Institution*
- **Network & Communication Resilience (3)** Saudi Arabia has solid telecom infrastructure in major cities and is investing in regional connectivity and 5G, yet there are still gaps in coverage and resilience outside core urban and industrial zones. *Source: MIT Technology Review*
- **Economic & Investment Continuity (4)** The kingdom has announced more than 14 billion dollars in AI and tech projects and can draw on deep sovereign wealth funds to sustain long-term AI infrastructure investment. This is a clear strength, although concentration risk and political volatility remain. *Source: Brookings Institution*

SINGAPORE

Singapore is positioning itself as a regional AI hub rather than a fully sovereign stack. Its strengths lie in talent, governance quality, and its role as a connectivity and data center node for Southeast Asia. The SEA-LION programme gives it linguistic leverage across ASEAN, but underlying compute and hardware remain imported, and the flagship "sovereign cloud" for Home Team agencies is built on Microsoft Azure. It has high operational resilience and convening power, but limited structural independence at the chip and cloud layers.



- **Compute & Energy Sovereignty (2)** Singapore has a dense, modern data center footprint and is an emerging AI hosting hub, but its energy is largely imported, land is scarce, and high end AI compute depends on foreign hardware and hyperscaler data centers. There are no indigenous GPU vendors or large national AI clusters fully controlled end to end. *Source: IT News Asia, MSDynamicsWorld*

- **Semiconductor & Hardware Independence (1)** Singapore hosts assembly and test operations and some chip R&D, but it does not operate leading edge logic or GPU fabs. AI workloads rely on imported NVIDIA and similar accelerators. *Source: Lawfare, Deloitte Outlook*

- **Cloud & Infrastructure Autonomy (2)** The HTX sovereign cloud for Home Team agencies is built on Microsoft

Azure, which gives operational localisation but not stack ownership. Commercial workloads lean heavily on AWS, Azure, and Google Cloud, sometimes complemented by regional players like Singtel. Jurisdictional control is therefore shared and constrained by foreign laws such as the US CLOUD Act. *Source: MSDynamicsWorld, CloudComputing-News*

- **Model & Data Independence (3)** AI Singapore's SEA-LION models provide open source LLMs covering 11 to 13 Southeast Asian languages, with hundreds of thousands of downloads and regional pilots. However, the latest SEA-LION 3 and 4 models are trained on top of imported compute and, in some cases, on underlying models like Alibaba's Qwen, which reduces full independence. Data governance is strong, but foundational model control is shared. *Source: Straits Times, SEA-LION Blog*

- **Talent & R&D Ecosystem (4)** Singapore is a regional magnet for AI researchers and engineers, with initiatives like AI Singapore, strong universities, and targeted grants. For its size, the talent density is very high, although it still imports a significant share of top talent and cannot match US or China scale. *Source: AI Singapore, Public First Report*

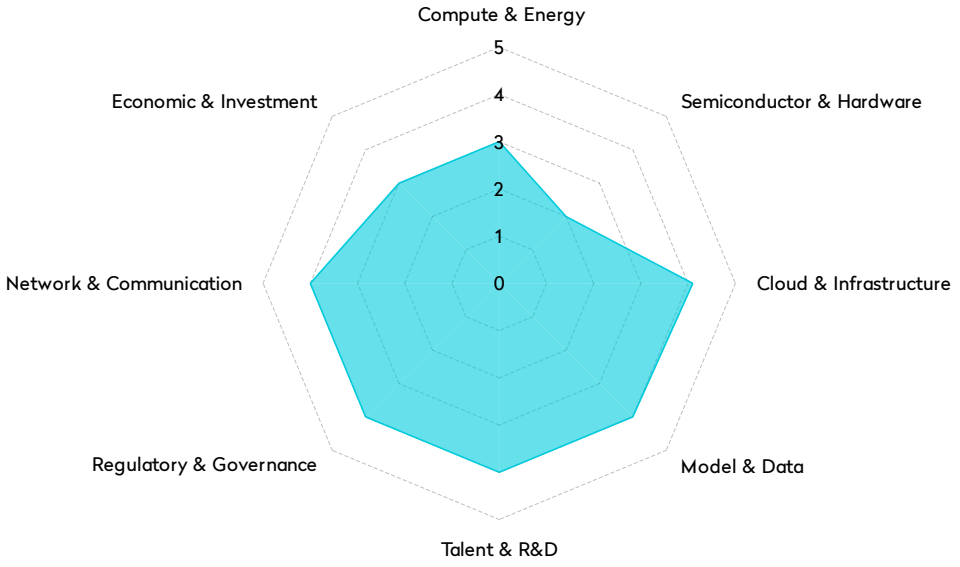
- **Regulatory & Governance Resilience (4)** Singapore has developed a relatively mature AI governance toolbox, including the Model AI Governance Framework and sectoral guidance, aiming for "trustworthy and innovation friendly" AI. It is not as prescriptive as the EU AI Act, but for enterprises it offers a clear, stable environment. *Source: GovInsider, Lawfare Analysis*

- **Network & Communication Resilience (4)** Singapore is one of the main submarine cable and IXP hubs in Asia, with high fibre and mobile penetration and extensive data center interconnects. This gives very high operational resilience, even though ownership of many cable systems is shared with foreign carriers. *Source: TeleGeography, IT News Asia*

- **Economic & Investment Continuity (4)** The National AI Strategy 2.0 includes more than 1 billion Singapore dollars of public funding for AI, complemented by significant private investment and sovereign wealth fund activity. For a small economy this is substantial and stable, although it is of course smaller in absolute terms than US, China, or Japan commitments. *Source: GovTech & Smart Nation, Hiverlab Blog*

SWITZERLAND

Switzerland boasts one of Europe's most credible approaches to sovereign AI, with locally owned infrastructure (Phoenix), an open multilingual LLM (Apertus) on Swiss soil, robust data protection, and world-class research. Structural weaknesses include no domestic chip manufacturing, reliance on NVIDIA/IBM hardware, and a small home market limiting large-scale investment. Switzerland maximizes sovereignty at the cloud, data, and governance layers, accepting semiconductor dependency.



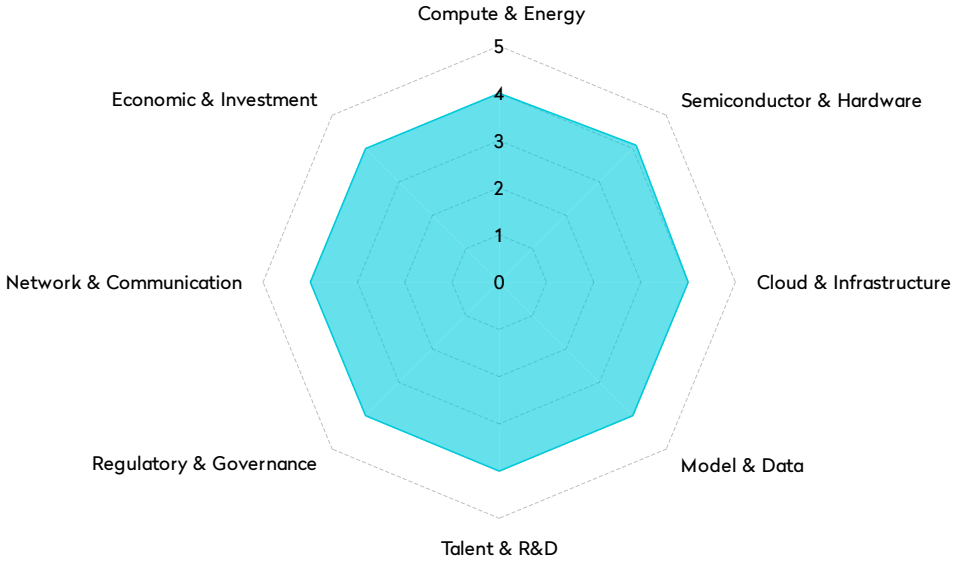
- **Compute & Energy Sovereignty (3)** Switzerland hosts the Phoenix VELA AI supercomputer in Swiss data centers for domestic AI compute under local ownership. However, it relies on imported NVIDIA and IBM hardware, and its energy markets are integrated with Europe. *Sources: Phoenix VELA AI Supercomputer, IBM-Phoenix Collaboration*

- **Semiconductor & Hardware Independence (2)** Switzerland lacks leading-edge commercial fabs and depends on foreign manufacturers for GPUs and CPUs, despite strong microelectronics research. Its resilience stems from access to allied suppliers. *Sources: IBM Newsroom, ETH Zurich Microelectronics*

- **Cloud & Infrastructure Autonomy (4)** Phoenix, a Swiss-owned provider, runs sovereign data centers with strict data residency and zero-trust architecture. Control, operations, and legal jurisdiction are Swiss, though hardware and some software (IBM watsonx) are foreign. *Sources: Phoenix Sovereign Cloud, IBM-Phoenix Collaboration*
- **Model & Data Independence (4)** Apertus is a fully open, multilingual LLM, trained and hosted on Swiss infrastructure with Swiss governance, offering genuine software and data sovereignty. Dependence on imported GPUs for training is the primary limitation. *Sources: Apertus Project, Phoenix Technologies LinkedIn*
- **Talent & R&D Ecosystem (4)** ETH Zürich, EPFL, and CSCS form a dense cluster for AI and HPC research, recognized among Europe's strongest. This ecosystem is high-quality but modestly sized. *Sources: ETH AI Center, EPFL AI Research*
- **Regulatory & Governance Resilience (4)** Switzerland combines strict data protection (FADP) with a culture of trusted infrastructure and financial privacy, imposing rigorous compliance on critical providers. An EU AI Act equivalent is not yet in place. *Sources: Swiss Federal Data Protection Act, Phoenix Systems Compliance*
- **Network & Communication Resilience (4)** Switzerland is a well-connected European hub with resilient broadband and data center interconnects across Zurich, Geneva, and other cities, ensuring high redundancy and quality. *Sources: TeleGeography Bandwidth Stats, Swiss Data Center Association*
- **Economic & Investment Continuity (3)** Phoenix, IBM, and related projects are well-funded, and the state invests in infrastructure. However, the market size and fewer federal mega-programs keep the capital base below larger economies. *Sources: Phoenix VELA AI Supercomputer, Swiss Federal Council Digital Strategy*

SOUTH KOREA

South Korea has one of the most coherent sovereign AI strategies globally, anchored in domestic AI chips, national model programs and strong industrial champions. The country is not energy sovereign, but it compensates through strategic centralisation, rapid policy execution and an unusually tight integration between government and industry. Korea's structural strength is its ability to produce hardware, models and cloud services domestically, making it one of the few nations building end-to-end autonomy. Its main limitation remains imported energy and sustained dependence on NVIDIA for top-end GPUs until NPUs mature.



- **Compute & Energy Sovereignty (3.5)** Korea is expanding the National AI Computing Center by fifteen times, adding large GPU clusters and strengthening sovereign compute, but the country relies heavily on imported energy and has limited low-cost renewable capacity relative to Norway or the Gulf. *Source: Chosun Ilbo English, MSIT*

- **Semiconductor & Hardware Independence (4)** Korea leads in memory chips via SK Hynix and Samsung and is developing domestic NPUs to reduce NVIDIA dependence. While it still imports some advanced GPUs, few countries match Korea's strategic control at the chip design and fabrication layer. *Source: The Diplomat, MSIT*

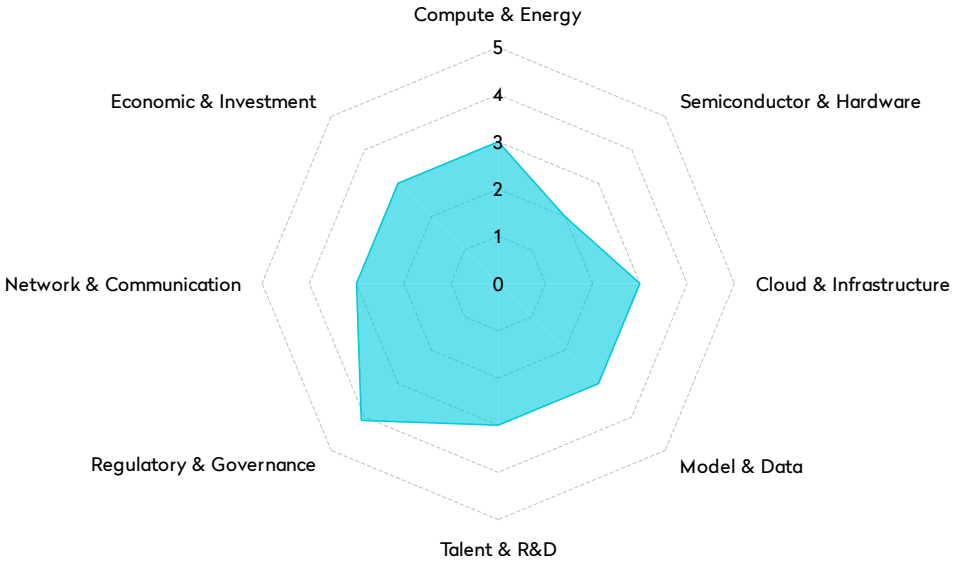
- **Cloud & Infrastructure Autonomy (4)** Domestic providers such as Naver, LG

CNS and SKT operate national clouds, giving Korea strong infrastructure autonomy with far less reliance on AWS, Azure or Google Cloud compared to most Western nations. *Source: The Diplomat, MSIT*

- **Model & Data Independence (4)** Five major Korean LLM initiatives (LG, SKT, Naver, NC AI, Upstage) are government-funded and evaluated every six months, enabling strong linguistic coverage and domestic model capability. *Source: Chosun Ilbo English, TechCrunch*
- **Talent & R&D Ecosystem (4)** Korea has a dense engineering talent pool, leading telecom innovation and strong industrial AI research embedded across conglomerates such as Samsung and LG. *Source: The Diplomat, TechCrunch*
- **Regulatory & Governance Resilience (4)** The AI Framework Act provides a risk-based regulatory architecture with specific defence considerations, balancing innovation incentives with governance obligations. *Source: FPF, MSIT*
- **Network & Communication Resilience (4)** Korea operates one of the world's fastest and most resilient broadband infrastructures with advanced 5G penetration and early 6G pilots. *Source: The Diplomat*
- **Economic & Investment Continuity (4)** Over 735 billion in sovereign AI investments, plus Korea's export-driven GDP, provide a steady foundation for long-term AI industrial expansion. *Source: Chosun Ilbo English, TechCrunch*

SPAIN

Spain has quietly built one of the most interesting **public LLM and governance combinations** in Europe, centring on the Barcelona Supercomputing Center and ALIA, a multilingual national model stack governed by a dedicated AI agency. Its strengths are in public infrastructure, language coverage and regulatory commitment; its weaknesses are familiar European ones: imported chips, reliance on EuroHPC for scale and limited private capital depth.

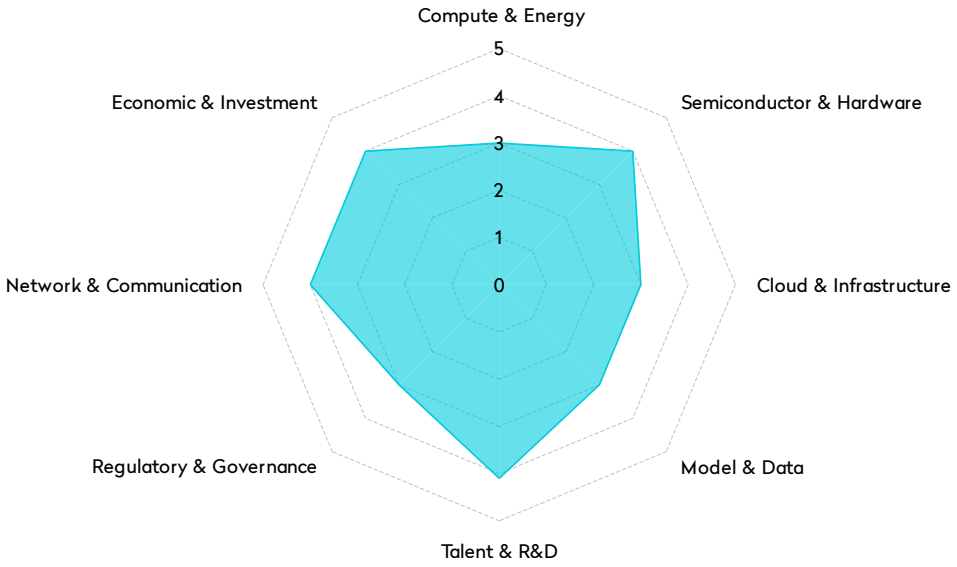


- **Compute & Energy Sovereignty (3)** The Barcelona Supercomputing Center (MareNostrum and related systems) gives Spain solid public HPC capacity used for AI research and national projects like ALIA. Hardware is imported and energy is integrated into the EU grid, so compute is robust but not uniquely sovereign. *Source: Barcelona Supercomputing Center, IBM*
- **Semiconductor & Hardware Independence (2)** Spain has no advanced semiconductor fabrication capabilities and relies on EU and global supply for GPUs and advanced chips, though it participates in EU-level semiconductor initiatives. *Source: European Commission, Quantum Insider*

- **Cloud & Infrastructure Autonomy (3)** Spain's national AI infrastructure projects are publicly governed and aligned with EU cloud sovereignty principles, but most hardware and some commercial workloads still run on imported platforms and global hyperscalers. *Source: AESIA, Kobalt Languages*
- **Model & Data Independence (3)** ALIA (Infraestructura Nacional de Lengua) is a multilingual open LLM stack covering Spanish and co-official languages such as Catalan and Galician, built in collaboration with BSC and IBM. This provides a real step towards linguistic sovereignty, albeit still trained on imported hardware. *Source: AESIA, IBM*
- **Talent & R&D Ecosystem (3)** Spain has strong pockets of AI research, especially around Barcelona and Madrid, but its overall research output and startup density are lower than France or Germany. It remains a solid mid-tier ecosystem within Europe. *Source: EU Startups, Oxford Insights*
- **Regulatory & Governance Resilience (4)** Spain has created a dedicated AI supervisory body (AESIA) and is closely aligned with the EU AI Act, positioning itself as a governance leader focused on ethics and public control of AI infrastructure. *Source: AESIA, Oxford Insights*
- **Network & Communication Resilience (3)** Spain benefits from decent connectivity and some strategic cable landings but is less central than northern European hubs such as the Netherlands or Germany in terms of IXPs and DC concentration. *Source: Oxford Insights, TeleGeography*
- **Economic & Investment Continuity (3)** AI funding is meaningful, supported by EU recovery and cohesion funds, but constrained by broader fiscal and growth limitations. Spain cannot match the sustained, large-scale capital commitments seen in France, Germany or the US. *Source: EU Startups, European Commission*

TAIWAN

Taiwan is the global centre of semiconductor sovereignty thanks to TSMC, giving it a strategic advantage over nearly every country except the United States. Its AI strategy is strengthened by Foxconn's USD $1.37B AI supercomputing hub and new national AI plans. However, Taiwan imports energy, cloud workloads still rely partially on global providers, and it has not yet produced a flagship LLM on the scale of DeepSeek or Mistral. The lasting constraint is geopolitical: semiconductor dominance coexists with extreme strategic vulnerability.



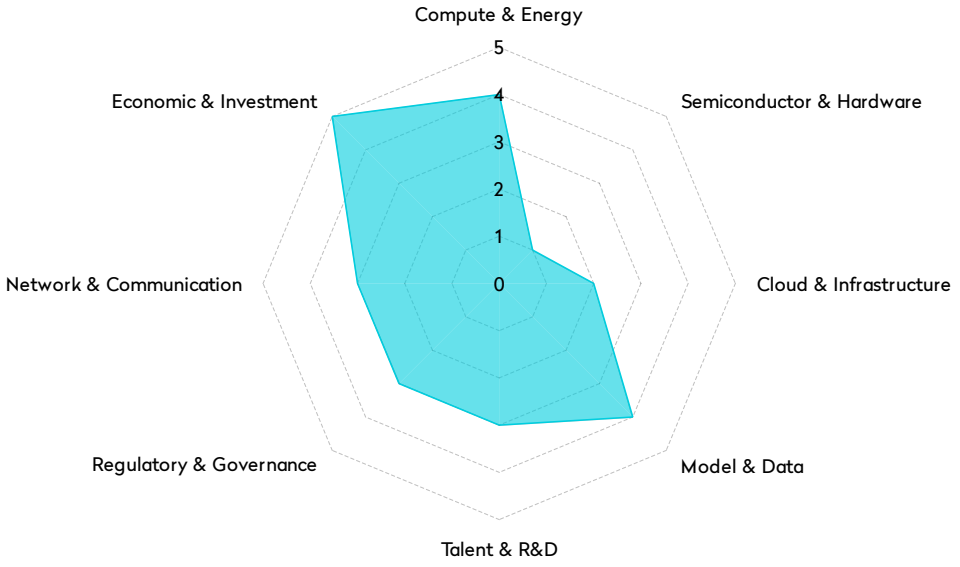
- **Compute & Energy Sovereignty (3)** Taiwan plans to invest $3B to become an "AI Island" and expand national data centres, but relies heavily on imported energy. *Source: Japan Times, Taiwan AI Island Plan*
- **Semiconductor & Hardware Independence (4)** Taiwan is home to TSMC, the world's most advanced semiconductor manufacturer, but still depends on ASML's EUV equipment and imported materials. *Source: Taiwan AI Island Plan, ASML*
- **Cloud & Infrastructure Autonomy (3)** Taiwan is broadening national AI infrastructure through partnerships with Foxconn and NVIDIA, but public and private sectors still rely heavily on global cloud platforms. *Source: Foxconn*
- **Model & Data Independence (3)**

Domestic models and AI services exist across research institutions and private companies, but Taiwan has yet to produce a frontier-scale LLM. *Source: Foxconn*

- **Talent & R&D Ecosystem (4)** Taiwan has a strong AI and semiconductor talent pipeline anchored by NTHU, NTU, ITRI and TSMC's engineering ecosystem. *Source: Taiwan AI Island Plan*
- **Regulatory & Governance Resilience (3)** AI policy is maturing, focusing on balancing innovation and risk, but lacks a comprehensive regulatory framework equivalent to the EU AI Act. *Source: Taiwan AI Island Plan*
- **Network & Communication Resilience (4)** Taiwan has advanced broadband, strong digital infrastructure and data centre capacity supporting semiconductor operations. *Source: Taiwan AI Island Plan*
- **Economic & Investment Continuity (4)** Major investments such as Foxconn's USD $1.37B AI supercomputing hub signal long-term stability in AI and semiconductor sectors. *Source: Foxconn*

UNITED ARAB EMIRATES

The UAE leverages strong capital, abundant energy, and a sophisticated local AI model ecosystem (Falcon, Jais, K2 Think). Its rapid development of AI assets and brands is a key strength. However, deep dependence on foreign hardware, cloud technology, and export jurisdiction limits its sovereignty, despite significant local LLM advancements and aggressive investment.



- **Compute & Energy Sovereignty (4)** Abundant energy and aggressive data center build-out (e.g., 1 GW Stargate cluster with Oracle/NVIDIA) strengthen the UAE's position. However, imported GPUs and tech stack are bound by US export control, limiting full compute layer control. *Source: Reuters, CNBC*
- **Semiconductor & Hardware Independence (1)** The UAE lacks advanced semiconductor fabrication or indigenous GPU production. All high-end accelerators (NVIDIA, etc.) are imported, controlled by US export policy. Local initiatives do not significantly change this. *Source: CNBC G42, US BIS Chip Controls*
- **Cloud & Infrastructure Autonomy (2)** Much of the stack relies on foreign vendors (e.g., Oracle for Stargate), with core orchestration, virtualization, and hardware design subject to foreign

jurisdiction, despite facilities being on UAE soil. *Source: CNBC G42, Oracle UAE Regions*

- **Model & Data Independence (4) The** UAE boasts multiple competitive domestic models: Falcon (40B, 180B), Jais (bilingual Arabic–English), and K2-Think. Sectoral models like Med42 and TelecomGPT Arabic further extend this stack. While trained on foreign hardware, software and data autonomy are substantial. *Source: Stanford HAI Falcon 180B, TII Falcon Models, Jais AI Model, Wired K2-Think*

- **Talent & R&D Ecosystem (3) MBZUAI,** TII, and G42 form a genuine local AI research cluster, actively importing talent. However, research depth still lags behind global leaders, and the ecosystem is not yet at frontier scale. *Source: MBZUAI Research, G42 Profile*

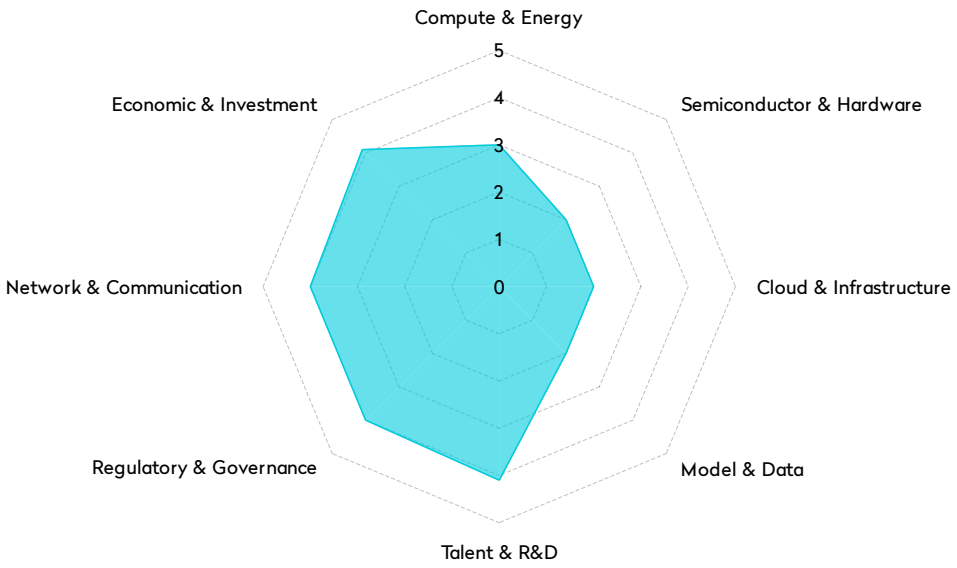
- **Regulatory & Governance Resilience (3)** The UAE has agile, centralized decision-making and AI/data frameworks. However, it lacks detailed assurance regimes and enforceable AI law akin to the EU AI Act, with vendor contracts and foreign jurisdictions still influencing outcomes. *Source: UAE AI Strategy, World Bank Digital Gov*

- **Network & Communication Resilience (3)** A significant regional telecom and cable hub, with strong mobile penetration and DC connectivity. However, much backbone routing and equipment relies on global vendors, making it robust operationally but not highly sovereign jurisdictionally. *Source: TeleGeography Map, Etisalat Profile*

- **Economic & Investment Continuity (5)** Sovereign wealth funds and state-backed vehicles provide very high capital resilience. Large, multi-year commitments to G42, TII, and national data centers are backed by long-term oil/gas revenues and Vision 2030 diversification strategies. *Source: Mubadala AI Strategy, CNBC UAE AI Investment*

UNITED KINGDOM

The UK is an AI research powerhouse that is choosing an operational-sovereignty strategy. Stargate UK and the AI Research Resource give it local access to OpenAI models running on NVIDIA hardware, but the stack is designed and controlled by US companies. London's strength is talent, regulation, and political positioning rather than full-stack sovereignty, which keeps its AI resilience solid but clearly hybrid.



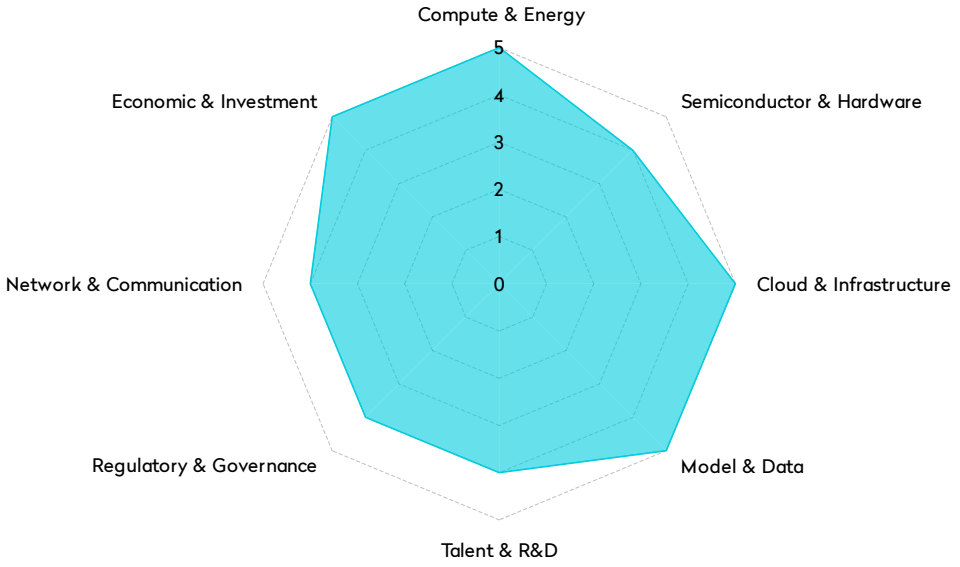
- **Compute & Energy Sovereignty (3)** Stargate UK and the AI Research Resource (Isambard-AI, Dawn) offer substantial GPU capacity (8k–31k NVIDIA GPUs for Stargate), but all compute relies on imported US-designed accelerators. *Source: OpenAI — Stargate UK, UKRI — AI Research Resource*

- **Semiconductor & Hardware Independence (2)** Arm gives the UK global chip design relevance, but the country has no advanced node fabrication capability and remains reliant on TSMC, Samsung, NVIDIA, and AMD for AI hardware. *Source: Arm Architecture Overview, UK Semiconductors Strategy Summary*

- **Cloud & Infrastructure Autonomy (2)** Stargate UK is foreign-designed and foreign-operated infrastructure located in the UK. National workloads rely heavily on AWS, Azure, and Google Cloud. *Source: OpenAI — UK Partnership*
- **Model & Data Independence (2)** The UK does not yet operate a national LLM stack; government cloud workloads primarily use OpenAI models through Stargate UK. Data localization exists, but model control does not. *Source: OpenAI — UK Government Usage*
- **Talent & R&D Ecosystem (4)** The UK hosts some of the world's top AI research institutions (e.g., DeepMind, Oxford, Cambridge, Alan Turing Institute) and remains a major global research hub. *Source: Alan Turing Institute, UK AI Strategy Overview*
- **Regulatory & Governance Resilience (4)** The UK's pro-innovation regulatory framework gives clarity while avoiding heavy prescriptiveness. The UK AI Safety Institute strengthens national influence. *Source: UK Government AI Regulation White Paper*
- **Network & Communication Resilience (4)** The UK is a major European connectivity hub with multiple subsea cable landings and strong national data center markets. *Source: TeleGeography UK Infrastructure*
- **Economic & Investment Continuity (4)** Large commitments from Microsoft, NVIDIA, and OpenAI, together with public backing for compute and safety research, provide stable mid-to-long-term funding. *Source: Microsoft UK AI Investment Announcement*

UNITED STATES OF AMERICA

The United States sits at the core of the AI stack. It controls most of the frontier models, the dominant cloud platforms, and a large share of global AI compute. However, it still depends on foreign partners for leading-edge manufacturing, lithography tools, and critical minerals, and its domestic AI regulation remains fragmented compared with the EU. In resilience terms, the US is structurally dominant but not fully insulated from supply-chain and governance constraints.



- **Compute & Energy Sovereignty (5)** The US hosts the largest concentration of hyperscale and AI-grade compute in the world. AWS, Microsoft, Google, and Oracle anchor multi-gigawatt GPU clusters on US soil, while OpenAI and Microsoft have proposed some of the largest AI infrastructure projects in history, including the 100 billion USD supercluster and the anticipated multi-hundred-billion-dollar Stargate initiative. *Source: Reuters, Synergy Research*
- **Semiconductor & Hardware Independence (4)** The US dominates chip design through NVIDIA, AMD, Intel, and Qualcomm, and the CHIPS Act accelerates domestic manufacturing. However, it still relies on TSMC and Samsung for leading-edge fabrication and ASML for EUV lithography, and depends on China and allies for

critical minerals. *Source: US CHIPS Act, TSMC Arizona Coverage, USGS Critical Minerals Report*

- **Cloud & Infrastructure Autonomy (5)** The US owns the global cloud backbone through AWS, Microsoft Azure, Google Cloud, and Oracle Cloud. The US government exerts extraterritorial governance power through export controls on AI chips and advanced computing infrastructure. *Source: US BIS Export Controls*
- **Model & Data Independence (5)** All frontier AI model leaders are US-based: OpenAI, Anthropic, Google DeepMind (dual UK–US but US-controlled), Meta, and Amazon. Model weights, training pipelines, and safety frameworks are governed under US corporate and federal systems. *Source: NYT on Frontier Model Leadership*
- **Talent & R&D Ecosystem (4)** The US still leads in high-impact AI research, but China now produces more STEM PhDs yearly, and the US relies heavily on foreign researchers and immigration pathways to sustain its lead. *Source: CSET — China Surpasses US in STEM PhDs*
- **Regulatory & Governance Resilience (4)** The US wields strong external governance via export controls, sanctions, and national-security restrictions. Domestically, however, its regulatory landscape is fragmented, with sectoral regulators and executive orders rather than an integrated AI law like the EU AI Act. *Source: US BIS, White House AI Policy*
- **Network & Communication Resilience (4)** US firms own a major share of global backbone, CDN, and subsea cable infrastructure, but these systems remain vulnerable to cyber threats, sabotage, and geopolitical risks. *Source: TeleGeography*
- **Economic & Investment Continuity (5)** The US has unmatched AI capital depth, combining CHIPS Act funding with massive private investments, such as Microsoft's planned 100B data center and OpenAI's projected 500B Stargate program. *Source: Reuters, US CHIPS Funding*

MOST AI STRATEGIES DEPEND ON CRITICAL FOREIGN CHOKEPOINTS.

IT IS TIME TO MEASURE THOSE DEPENDENCIES AND BUILD PROACTIVE RESILIENCE.

FURTHER READING

- Digital Sovereignty: A Board-Level Imperative
- Who Really Controls Your AI?
- Reading the U.S. National Security Strategy as a Technology Blueprint
- Winning the Battle for Trust When Truth is Fragmented
- The Illusion of Intelligence: Why LLMs Are Not the Thinking Machines We Hope For
- The AI - Energy Paradox: Will AI Spark a Green Energy Revolution Or Deepen the Global Energy Crisis?
- When AI Speaks Your Language
- South Korea, Nvidia, AI Chip, Sovereign AI
- Can South Korea Replicate Its K-Pop Success with AI?
- Can Nuclear Power Fuel Southeast Asia's Energy Transition?
- The AI Battleground: How Southeast Asia is Positioning Itself
- Is Southeast Asia Ready for an AI Arms Race?
- Asia's High-Stakes Chip Game: What's Next?
- The Chip War's New Reality: A View from Asia

SOURCES

Note: This represents a curated selection of primary sources. The full research includes over 200 citations across all 25 country analyses.

- The Stargate UAE Partnership
- OpenAI, UAE to build massive AI center in Abu Dhabi
- OpenAI, Oracle, NVIDIA, SoftBank Group and Cisco partner for Stargate UAE AI campus
- Oracle and NVIDIA to Deliver Sovereign AI Worldwide
- Introducing Stargate UAE - OpenAI
- Introducing Stargate UK
- OpenAI Launches Stargate Norway: Europe's First Green AI Supercomputer Hub
- Thales and Google Cloud Announce Strategic Partnership
- Experience the Swiss way to cloud. | Phoenix
- IBM and The Government of Spain Collaborate to Advance National AI strategy
- The Complete Guide to Using AI in the Government Industry in Italy in 2025
- Germany's €5.5B AI Strategy: Machine Vision's Role in 10% GDP by 2030
- National AI Strategy Policy Directions
- South Korea's Sovereign AI Gambit: A High-Stakes Experiment in Autonomy
- Japan's $135B AI Revolution: Quantum + GPU Infrastructure
- The New AI Superpower Isn't a Nation. It's the Stack China Gave Away
- China's drive toward self-reliance in artificial intelligence
- HTX to create Microsoft-based sovereign cloud in Singapore
- India's AI Revolution

- Brazilian Artificial Intelligence Plan: Challenges, Opportunities, and Perspectives for Sovereign AI
- Canadian government launches Sovereign AI Compute Strategy
- National AI Program Stalls; Stealthy Defense Startups
- CSC calls for focus on data infrastructures and sovereignty in EU's AI Continent Action Plan
- Russia AI Sovereignty Push: Implications for Global Tech Markets
- Indonesia's AI National Roadmap White Paper
- A Blueprint for Australia's Sovereign, Sustainable AI
- Realigning US–Saudi Relations for the AI Era
- Kenya's Efforts in AI and Implementation Plan
- Taiwan to spend $3 billion turning nation into AI island

ABOUT THE AUTHOR

Damien Kopp helps leaders navigate AI, digital transformation, and geopolitics. With 25 years experience across Europe, North America, and Asia, he advises government agencies, banks, and Fortune 500s, and leads AI initiatives within startups and large corporations.

As Managing Director of RebootUp, Damien advises global enterprises on designing, governing, and deploying strategic and sovereign AI solutions. His work spans AI strategy, data monetization, governance frameworks, and building AI-enabled products that accelerate business impact.

Through KoncentriK, his thought-leadership platform, Damien explores the deeper currents shaping our digital future: from AI sovereignty and infrastructure risk to the geopolitics of cloud, chips, and data.

As an Associate Faculty with Singapore Management University, Executive Development, he teaches applied AI, helping business leaders leverage emerging technologies for strategic advantage. A frequent speaker and lecturer, Damien combines real-world pragmatism with system-level foresight to help organizations become more intelligent and resilient.

He holds an Executive MBA from Kellogg and HKUST and a Master's in Electronics Engineering from ESME Sudria.

ABOUT REBOOTUP

RebootUp is a Singapore-based boutique consulting firm that helps organizations solve innovation challenges. Drawing on technical expertise and business acumen, the team guides clients in generating ideas, refining models, and entering new markets. With specialties in digital transformation, AI, and agile processes, RebootUp has delivered breakthroughs in efficiency, strategy, and growth for prominent companies across Asia and the Middle East.

ABOUT OUR COLLABORATION

This publication is the result of an international partnership between **Digital New Deal, Asia Tech Lens, RebootUp**, and **Koncentric**. Its objective is to establish a lasting collaboration between Digital New Deal's activities in Paris and those of its partners in Singapore, notably to **support the development of the Digital Resilience Index in Southeast Asia**.
The publication was released simultaneously in December 2025 in Asia and January 2026 in Europe.

ACKNOWLEDGMENTS

This research would not have been possible without the invaluable contributions of several individuals who generously shared their expertise, insights, and time throughout the development of this work.

I am particularly grateful to **Nicolas Marchand**, Co-Founder and Chief Operating Officer at **Asia Tech Lens**, and **Mohit Sagar**, CEO & Editor in Chief at OpenGov Asia, for their strategic perspectives on the Asian technology landscape. **Clara Lee**, Chief of Data Science & Digital Sustainability Practices at the **National University of Singapore** - ISS, provided crucial guidance on AI risks and data governance practices.

Special thanks to **Hazleen Ahmad**, Impact Investor & Strategic Foresight Consultant, for her forward-looking insights on resilience planning, and to **Roh**an **Uday Rawte,** Managing Director at **IESVE** Singapore Pte Ltd, for his practical expertise in operational implementation. **Dr. Sunil Sivadas**, Director of NEXT Gen Tech at **NCS Group**, offered essential technical validation of the framework components.

I am indebted to **Romesh Jayawickrama**, Founder & CEO at **Inttent**, and **Partha Rao,** Founder & CEO at **Pints AI**, for their critical real-world insights on AI implementation within regulated environments and sovereign infrastructure requirements respectively. **Emily Y. Yang**, Head of Human-Centered AI and Innovation at **Standard Chartered Bank**, provided invaluable perspectives on responsible AI deployment in enterprise contexts. **Pierre Robinet** at **Ogilvy Asia** offered valuable insights on organizational change dynamics, while **Patrick McCreery**, Director, Hyperscale at **Digital Edge DC,** contributed essential expertise on infrastructure resilience.

Aparna Bhushan, Co-founder of Rethinking Tech and Global Data Protection & AI Governance Lead at the **United Nations Development Programme**, provided critical perspectives on the geopolitical landscape. Finally, **Jean-Pierre Delesse**, CEO Fdb Conseil, Semiconductor Industry Expert, offered indispensable expertise on supply chain sovereignty and technological dependencies.

Any errors or omissions in this work remain my own.

DIGITAL NEW DEAL
THINK–DO–TANK

Digital New Deal supports private and public decision-makers in creating a European and Humanist Digital Enlightenment. Our belief is that we can offer a third digital way by pursuing a dual objective: defending our values by proposing a framework of trust through regulation (think tank); and defending our interests by creating ecosystems of trust through cooperation (do tank).

Our publishing activity aims to shed as much light as possible on the developments taking place within the issues of "digital sovereignty", in the broadest sense of the term, and to develop concrete courses of action for economic and political organizations.

SÉBASTIEN BAZIN
CEO of AccorHotels

NATHALIE COLLIN
General Manager, Consumer and Digital Division La Poste Group

NICOLAS DUFOURCQ
CEO of Bpifrance

AXELLE LEMAIRE
Former Secretary of State for Digital Technology and Innovation

BRUNO SPORTISSE
CEO of Inria

DENIS OLIVENNES
CEO of CMI France

JUDITH ROCHFELD
Associate Professor of Law, Panthéon Sorbonne

ARNO PONS
General Delegate of the Digital New Deal think tank

ROBERT ZARADER
President of Digital New Deal, CEO Bona Fidé

MAXENCE DEMERLÉ
Digital director, MEDEF

BERNARD GAVGANI
Senior advisor, BNP Paribas

JOËLLE TOLEDANO
Professor emeritus of economics, Paris Dauphine

OUR PUBLICATIONS

AI is LAW
Simon Bernard– May 2025

Generative AI: unite or submit
Olivier Dion, Michel-Marie Maudet, Arno Pons – *November 2024*

Public data sharing infrastructures: the great forgotten
Laura Létourneau – *September 2024*

Strengthening pan-european democracy in the era of AI
Axel Dauchez, Hendrik Nahar – *April 2024*

Digital technology for a sustainable future
Véronique Blum, Maxime Mathon – *June 2023*

Trusted AI, a strategic opportunity for industrial and digital sovereignty
Julien Chiaroni, Arno Pons – *June 2022*

Trusted data, data sharing, the key to our strategic autonomy
Olivier Dion, Arno Pons – *September 2022*

Cybersecurity, the guardian of our strategic autonomy
Arnaud Martin, Didier Gras – *June 2022*

GDPR, Act II: Collective control of our data as an imperative
Julia Roussoulières, Jean Rérolle – *May 2022*

Digital taxation, the return match
Vincent Renoux – *September 2021*

Defending the rule of law in the age of platforms
Denis Olivennes et Gilles Le Chatelier – *June 2021*

Trusted Cloud: A Strategic Autonomy Issue for Europe
Laurence Houdeville et Arno Pons – *May 2021*

White papers: Data sharing & tourism
Fabernovel et Digital New Deal – *April 2021*

Sharing personal data: changing the game through governance
Matthias de Bièvre et Olivier Dion – *September 2020*

Reflections on the European Digital Services Act
Liza Bellulo – *March 2020*

Preserving our educational sovereignty: supporting French EdTech
Marie-Christine Levet – *November 2019*

Breaking the Big Tech Monopoly: Regulate to Free the Many
Sébastien Soriano – *September 2019*

Getting out of digital Stockholm syndrome
Jean-Romain Lhomme – *October 2018*

The Citizen Public Service
Paul Duan – *June 2018*

The Age of the Decentralized Web
Clément Jeanneau – *April 2018*

Real taxation for a virtual world
Vincent Renoux – *September 2017*

Regulating "digital"
Joëlle Toledano – *May 2017*

Call to presidential election candidates for a #DigitalPact
January 2017

Health in the face of the tsunami of NBICs and platformers
Laurent Alexandre – *June 2016*

What is the personal data policy?
Judith Rochfeld – *September 2015*

State of digital technology in Europe
Olivier Sichel – *July 2015*

February 2026

www.thedigitalnewdeal.org