Capgemini
RESEARCH INSTITUTE

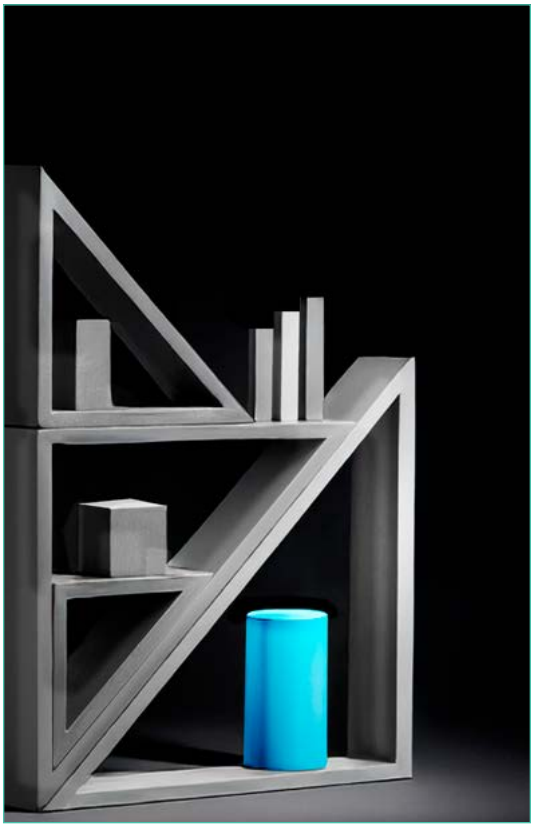
Digital Sovereignty

Balancing Control, Dependencies, and Innovation

Conversations
FOR TOMORROW

N°11 — 2026

Conversations
FOR TOMORROW



Order through structure, balance through design. The cover of this edition reflects digital sovereignty not as isolation, but as an act of careful construction. The open, architectural form, composed of distinct elements held in deliberate tension, mirrors the choices leaders face today: where to anchor control, where to allow interdependence, and how to keep innovation flowing without surrendering agency. It evokes a modular world in which stability comes not from rigidity, but from understanding which connections matter most. Much like the conversations within this edition, the image captures sovereignty as a dynamic equilibrium, balancing control, dependencies, and innovation in an increasingly complex digital landscape.

Foreword

At Capgemini, we believe organizations are best prepared for tomorrow when they draw on a wide range of informed perspectives from business leaders, policymakers, academics, investors, and technology practitioners. Through *Conversations for Tomorrow*, the Capgemini Research Institute brings those voices together to help leaders identify the strategic imperatives shaping business and society. In this eleventh edition, we explore one of the defining questions of our time: how to build digital sovereignty in a world where technology, data, infrastructure, and innovation are deeply interconnected.

This edition examines digital sovereignty as a broad strategic challenge that cuts across multiple layers of the digital landscape.

Among other themes, we explore:

- How organizations can define sovereignty in practical terms, across data, operational, technical, and legal dimensions
- How to balance innovation with control, particularly in cloud, AI, and critical digital infrastructure
- How to reduce dependency without retreating into isolation, by building resilience, portability, and trusted partnerships
- How regulation, geopolitics, and industrial policy are reshaping the technology agenda, especially in Europe
- How leaders can turn sovereignty from a defensive concern into a source of resilience and competitive advantage

As Karine Brunet argues in this edition, the central challenge is not to pursue an illusion of full digital self-sufficiency, but to make clear, affordable, and strategic choices about where control matters most. In a hyper-connected world, no country or organization can be fully sovereign across every layer of the stack. What matters is identifying critical dependencies, understanding the risks they create, and building a pragmatic sovereignty strategy that protects the business without constraining innovation and growth. This idea runs throughout the edition: sovereignty is less about autonomy for its own sake, and more about resilient interdependence, where strategic control, openness, and competitiveness must be held in balance.

We are grateful to the leaders and experts who shared their insights so candidly for this edition. By bringing together voices from enterprise technology, telecommunications, policy, academia, investing, and Capgemini, we hope this journal helps leaders navigate the new tech order with greater clarity and confidence.

Key contributors include:

- Christian Klein, CEO, SAP SE and Aiman Ezzat, CEO, Capgemini
- Lila Tretikov, Partner, Head of AI Strategy, NEA
- Dirk Schrödter, Head of the State Chancellery (CdS) and Minister of Digitalization of the state of Schleswig-Holstein
- Jai Haridas, VP & GM, Regulated and Sovereign Cloud, Google Cloud
- Anu Bradford, Henry L. Moses Professor of Law and International Organization, Columbia University
- Alexander Zwart, Chief Information and Technology Officer, Rabobank
- Kai-Fu Lee, Founder & CEO, 01.AI
- Joakim Reiter, Chief External and Corporate Affairs Officer, Vodafone
- Calista Redmond, VP Global AI Initiatives, NVIDIA
- Sharad Sriwastawa, Co-CEO, Rakuten Mobile and President, Rakuten Symphony
- Jean Coumaros, President & CEO, Bleu, a trusted cloud company in France
- Karine Brunet, Chief Operations and Delivery Officer, Capgemini

Pulling together such a wide range of perspectives was an instructive exercise for us. We hope you enjoy reading this edition as much as we enjoyed putting it together for you.

Fernando Alvarez Tabio
Chief Strategy and Development Officer, Capgemini

Conversations FOR TOMORROW

Contents

Conversations FOR TOMORROW

P.14
THE CEO CORNER

P.16
Christian Klein
CEO
SAP SE

P.16
Aiman Ezzat
CEO
Capgemini

Conversations FOR TOMORROW

P.30
EXECUTIVE CONVERSATIONS WITH…

Conversations FOR TOMORROW

Contents

Executive Summary

The eleventh edition of Conversations for Tomorrow examines digital sovereignty at a decisive inflection point. As geopolitical fragmentation accelerates, AI reshapes the digital value chain, and regulatory expectations harden, leaders can no longer treat sovereignty as a peripheral compliance or infrastructure issue. It has become a strategic discipline, one that directly shapes competitiveness, resilience, innovation, and trust.

Across industries and regions, CXOs are confronting a new reality: technological interdependence is unavoidable, but unmanaged dependence is a growing strategic risk. The question is no longer whether organizations should pursue digital sovereignty, but how to do so pragmatically: securing meaningful control over data, infrastructure, and AI capabilities without forfeiting access to global innovation ecosystems. This edition explores how leading executives are navigating that tension, converging on a shared insight: sovereignty is not about isolation, but about informed choice, layered control, and resilient interdependence.

> **"No country can go it alone, not even a superpower"**
>
> **Anu Bradford,**
> Professor, Columbia University

Sovereignty in a deeply interdependent world

Digital sovereignty is rising in importance as global technology systems become deeply interconnected and increasingly exposed to geopolitical tension. **Anu Bradford**, Henry L. Moses Professor of Law and International Organization at **Columbia University**, highlights the strain that companies feel when it comes to competing legal and political demands: **"International customers and governments are starting to question whether foreign tech providers will obey local laws or the dictates of their home government."** But does that mean every country can go all-in on sovereignty? She's emphatic: **"No country can go it alone, not even a superpower."**

Pragmatic sovereignty is the name of the game

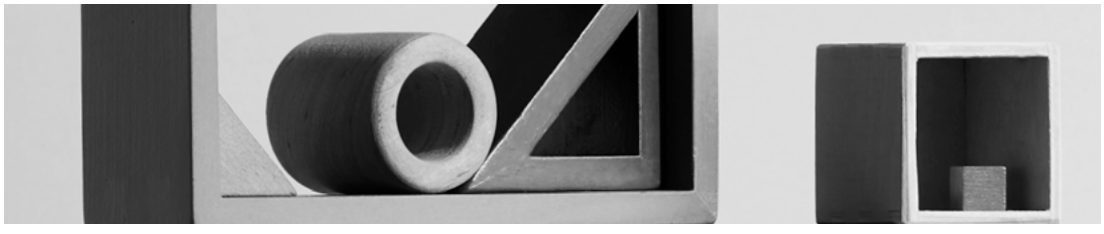
If no country can go it alone, how should companies be approaching sovereignty? A first step is to understand what sovereignty is and isn't. A consistent message across this edition is the danger of treating sovereignty as an absolute or emotionally driven objective.

Joakim Reiter, Chief External and Corporate Affairs Officer at **Vodafone**, warns: **"The challenge is that this debate has not always started from the right question: what are we actually trying to achieve?"** He emphasizes realism: **"You will never be 100% sovereign, just as you will never be 100% secure."**

> **"The challenge is that this debate has not always started from the right question: what are we actually trying to achieve?"**
>
> **Joakim Reiter,**
> Chief External and Corporate Affairs Officer at Vodafone

> **"Digital sovereignty is the ability to exercise choice, control, and governance across data, operational, technical, and legal layers, while staying connected to the best global technology. It's certainly not about isolation or excluding global partners"**
>
> **Christian Klein,**
> CEO of SAP

Christian Klein, CEO of **SAP**, offers a straightforward definition: **"Digital sovereignty is the ability to exercise choice, control, and governance across data, operational, technical, and legal layers, while staying connected to the best global technology. It's certainly not about isolation or excluding global partners."**



> **The same architectural choice can be both a strength and a vulnerability, depending on the scenario"**
>
> **Alexander Zwart,**
> Chief Information and Technology Officer, Rabobank

Aiman Ezzat, CEO of **Capgemini**, argues for pragmatism: **"What is both realistic and desirable is 'strategic autonomy': the ability to choose and manage our dependencies to protect European interests. That means identifying which parts of the digital value chain are truly critical – and designing for resilient interdependence rather than complete independence."**

Alexander Zwart, CITO of **Rabobank, translates that principle into an operational test. "The same architectural choice can be both a strength and a vulnerability, depending on the scenario,"** he observes.

Jai Haridas, VP & GM of Sovereign Cloud at **Google Cloud**, also cautions against what he terms **"emotional sovereignty": "Decisions driven by fear or emotion rather than a careful, use-case-by-use-case risk analysis tend to over-constrain organizations, push them into overly restrictive solutions, and unnecessarily compromise innovation."**

> **Decisions driven by fear or emotion rather than a careful, use-case-by-use-case risk analysis tend to over-constrain organizations, push them into overly restrictive solutions, and unnecessarily compromise innovation"**
>
> **Jai Haridas,**
> VP & GM of Sovereign Cloud at Google Cloud

AI sovereignty: Models, values, and the power of choice

Artificial intelligence is rapidly becoming a key part of the digital sovereignty debate. Beyond infrastructure and data, sovereignty increasingly hinges on who controls AI models, how they are trained, and whose values they embed. As AI systems move closer to core decision making and economic value creation, concerns about cultural alignment, competitive dependence, and long-term autonomy are intensifying. **Kai-Fu Lee**, Founder & CEO of **01.AI** – an AI company developing open-source products – and Chairman of **Sinovation Ventures** in China, frames AI sovereignty fundamentally

> **Sovereignty means having control over the technologies themselves"**
>
> **Kai-Fu Lee,**
> Founder & CEO of 01.AI,
> Chairman of Sinovation Ventures

as control at the model level: **"Sovereignty means having control over the technologies themselves."** He argues that for most countries, sovereignty does not require building frontier models from scratch, but rather adapting existing ones: **"The practical alternative, and I think the right one for almost all countries outside the US and China, is to take a leading open-source model and continue training it for the country's specific language, values, and regulations."**

> **Invest locally, engage globally"**
>
> **Calista Redmond,**
> VP Global AI Initiatives, NVIDIA

As AI moves from generating content to taking action, sovereignty must extend to the full workflow. As **Calista Redmond,** VP Global AI Initiatives, **NVIDIA** puts it: **"The governance challenge is shifting from content quality to action quality."** She frames the objective as **"invest locally, engage globally."** But organizations need to move fast. As **Jai Haridas**, VP & GM of Sovereign Cloud at **Google Cloud**, points out: **"Six months in AI is like seven dog years."**

Evaluating sovereign cloud without false trade-offs

For CXOs selecting sovereign cloud solutions, the stakes are high and the misconceptions widespread. Too many organizations assume that sovereignty necessarily limits their ability to innovate, or that migrating to sovereign environments demands costly re-architecture. Neither assumption is inevitable.

Jai Haridas, VP & GM of Sovereign Cloud at **Google Cloud**, challenges executives to reject the false choice: **"The question is not whether to pursue sovereignty, but how to do so without sacrificing competitive position and innovation capacity."** He urges CXOs to evaluate vendors on their ability to balance sovereignty, security, and innovation simultaneously, and to scrutinize lock-in beyond technology, including through licensing mechanisms.

Within Europe, the cloud landscape is evolving. Local regulations and a desire of some organizations to work with local providers are causing shifts in the market. **Jean Coumaros**, President & CEO of **Bleu**, a trusted cloud provider in France, frames the executive challenge clearly: **"At least a dozen countries have extraterritorial laws that can compel cloud providers to hand over customer data to a foreign government."**

> **At least a dozen countries have extraterritorial laws that can compel cloud providers to hand over customer data to a foreign government"**
>
> **Jean Coumaros,**
> President & CEO of Bleu

Toward ownership, partnerships, and resilient interdependence

At the infrastructure layer, sovereignty increasingly hinges on transparency, openness, and ownership.
Dirk Schrödter, Head of the State Chancellery and Minister of Digitalization of **Schleswig-Holstein**, argues that substituting one proprietary dependency for another is not enough: **"Open source is the key to digital sovereignty."**
From the CEO and investor perspective, sovereignty is increasingly about **choice, trust, and balance** – not withdrawal from global ecosystems.

> **Open source is the key to digital sovereignty"**
>
> **Dirk Schrödter**,
> Head of the State Chancellery and Minister of Digitalization of Schleswig-Holstein

Karine Brunet, Chief Operations and Delivery Officer at **Capgemini**, underscores the strategic shift underway: **"Sovereignty now means balancing strategic self-reliance with intelligent partnerships."**

> **Sovereignty now means balancing strategic self-reliance with intelligent partnerships"**
>
> **Karine Brunet,**
> Chief Operations and Delivery Officer at Capgemini

Aiman Ezzat, CEO of **Capgemini**, concludes: **"Ultimately, it is the freedom – and the capability – to choose your dependencies."**
Yet sovereignty is not only a concern for nations and organizations. As **Lila Tretikov**, Partner and Head of AI Strategy at **NEA**, argues: **"Amid all the talk of sovereign nations, sovereign AI and sovereign infrastructure, we should not lose sight of the most important sovereign entity: the human being."**

> **Ultimately, digital sovereignty is the freedom – and the capability – to choose your dependencies"**
>
> **Aiman Ezzat,**
> CEO of Capgemini

Across these conversations, a clear executive agenda is emerging. Digital sovereignty is no longer a binary choice between control and innovation, but a continuous set of strategic decisions. Leaders must now make explicit choices about which digital assets and capabilities are truly critical, where dependence is acceptable, or even advantageous, and how quickly those choices must evolve as technology and geopolitics shift.

"Amid all the talk of sovereign nations, sovereign AI and sovereign infrastructure, we should not lose sight of the most important sovereign entity: the human being"

Lila Tretikov,
Partner and Head of AI Strategy at NEA

This edition of Conversations for Tomorrow brings together the voices of leaders who view digital sovereignty not as a constraint, but as a strategic capability – one that enables choice, resilience, trust, and sustained innovation in an interdependent world.

Christian Klein

CEO, SAP SE

The CEO Corner

in discussion with

Aiman Ezzat

CEO, Capgemini

Christian Klein
CEO, SAP SE

Christian Klein is Chief Executive Officer and chairman of the Executive Board of SAP SE. In his role, Klein holds the overall responsibility for the corporate strategic direction, management, and performance of SAP SE.

Klein started his career at SAP SE in 1999 as a student. After holding various positions across the company, including Chief Financial Officer of SAP SuccessFactors and SAP's Chief Controlling Officer, he was appointed Chief Operating Officer of SAP SE in 2016, a role in which he continued until 2021. On October 11, 2019, he was named Co-CEO of SAP SE together with Jennifer Morgan, before being appointed the sole CEO on April 20, 2020. Klein holds a diploma in International Business Administration from the University of Cooperative Education in Mannheim, Germany.

Aiman Ezzat
CEO, Capgemini

With more than 20 years' experience at Capgemini, Aiman Ezzat has a deep knowledge of the Group's main businesses. He has worked in many countries, notably the UK and the US, where he lived for more than 15 years.

Aiman was appointed CEO in May 2020. Prior to that, from 2018 to 2020, he served as the Group's COO and, from 2012 to 2018, as CFO. Aiman is also on the Board of Directors of Air Liquide and is a member of the Business Council and the European Round Table (ERT) for Industry. Aiman is a Knight of the Legion of Honor.

A common European definition

How do you define digital sovereignty? To what extent is the lack of a common definition hampering progress?

> **Digital sovereignty is the ability to exercise choice, control, and governance across data, operational, technical, and legal layers"**
>
> Christian Klein

— **Christian:** For me, digital sovereignty starts with a simple reality: AI is reshaping enterprise software and the way companies run their core operations. SAP sits right at the heart of that change.

This is central to our vision for the Autonomous Enterprise. We see a future where AI handles operational tasks autonomously, empowering people to focus on what they do best: solving complex problems and driving innovation.

Ultimately, digital sovereignty is the ability to exercise choice, control, and governance across data, operational, technical, and legal layers, while staying connected to the best global technology. It's certainly not about isolation or excluding global partners. Europe must remain open to innovation and international cooperation.

Having a common definition of digital sovereignty across Europe is essential. Currently, that's not the case, and this lack of alignment creates uncertainty for public authorities, regulated industries, and technology providers. It directly undermines the adoption of cloud, AI, and mission-critical digital services.

A single, harmonized EU-wide approach to sovereign cloud would reduce fragmentation, strengthen the single market, and enable providers to scale more efficiently. And in the end, that means better outcomes for European organizations and citizens.

— **Aiman:** Digital sovereignty, as I see it, is a country or region's ability to master key digital technologies and the laws that govern them, so it can independently assess, decide, and act in the digital realm – without having its structural choices dictated by a third party.

The concept spans multiple dimensions: data sovereignty, operational sovereignty, technical sovereignty, and legal sovereignty. Ultimately, it is the freedom – and the capability – to choose your dependencies. For large organizations, the goal is not full autonomy; it is to understand and manage technological dependencies, moving from dependence to resilient interdependence.

> **Ultimately, digital sovereignty is the freedom – and the capability – to choose your dependencies"**
>
> Aiman Ezzat

When governments and businesses use "digital sovereignty" to mean different things, the debate loses focus and nuance – making it harder to build consensus and take collective action.

When the CEOs of Europe's largest organizations ask you about digital sovereignty, which risks are they trying to mitigate – and has that changed in the past 12–18 months?

— **Christian:** When I talk with CEOs, the conversation almost always comes back to a few core risks. Over the past 18 months, those risks have only become more urgent.

The first is business continuity. If something goes wrong, it isn't the infrastructure itself that is exposed, but rather core processes such as supply chains, logistics, finance, and public services.

> **Digital sovereignty has shifted from a technical topic to becoming a central pillar of Europe's economic security agenda"**
>
> Christian Klein

The second is the broader environment. Geopolitical tension, rising cyberthreats, and increasingly complex regulation are putting a lot of pressure on organizations. Staying secure, compliant, and trusted are top priorities for every company. That means digital dependencies now translate directly into strategic vulnerabilities.

As AI moves into critical decision-making, leaders are asking new questions: Who controls the data? Who governs the models? And how transparent and accountable are the decisions those systems make?

This is why digital sovereignty has shifted from a technical topic to becoming a central pillar of Europe's economic security agenda. And in a volatile environment, SAP helps organizations manage exactly that complexity.

— Aiman: When European CEOs raise digital sovereignty, the underlying goal is to reduce critical reliance on non-European technologies. The risks they want to mitigate are clear: dependence on a single foreign cloud or software provider; extraterritorial legal exposure (for example, foreign authorities gaining access to sensitive data); and cybersecurity vulnerabilities across critical digital supply chains. Ultimately, they worry that heavy reliance on foreign-owned platforms can erode control over data and operations – or expose them to the consequences of external decisions beyond their influence.

The conversation is now shifting. Where it used to focus on autonomy in specific domains (such as data or cloud), the most frequent question I hear today is: "Can we strengthen our digital sovereignty without losing competitiveness?" CEOs want assurance that they can reduce critical dependencies and protect operations while still accessing best-in-class technology and competing globally. In other words, the central challenge is to balance sovereignty with agility and innovation.

"The central challenge is to balance sovereignty with agility and innovation"

Aiman Ezzat

How important is the enterprise software layer in achieving digital sovereignty?

— Christian: When we talk about digital sovereignty, the enterprise software layer is absolutely critical, because it's where everything comes to life. AI agents can look impressive, but without real industry and process knowledge, real data, and real business context, they're basically just demos. No foundation model delivers that on its own. SAP does.

True digital sovereignty requires control across the entire stack: infrastructure, platforms, applications, and AI. And the enterprise software layer is where these elements come together. It's where business processes run, where data is structured, and where decisions are made.

That's why enterprise software isn't just another part of the stack. It's the layer that connects infrastructure, data, and AI into trusted, end-to-end systems. It's what makes sovereignty real and practical for organizations.

Ultimately, this is what enables the Autonomous Enterprise – where AI is not just an add-on, but embedded into end-to-end business processes, driving decisions, adapting in real time, and operating within clearly governed and sovereign frameworks.

— Aiman: The enterprise software layer is often underappreciated. Cloud infrastructure and chips are essential, but software is the connective tissue across the digital value chain – it is what links data, processes, and decision-making end to end.
Strengthening this layer is therefore a priority for sovereignty. Open source can bring transparency and flexibility, but it is not a silver bullet for either sovereignty or security. What matters is that software choices – especially for core business functions and data management – preserve control: the ability to switch, to audit, and to operate. For Europe, that means pushing interoperability and portability to avoid lock-in, and ensuring critical software can run in a sovereign environment (for example, security-verified, hosted in Europe, with encryption keys controlled locally). In short, the enterprise software layer is as strategic to sovereignty as cloud and semiconductors.

> **"The enterprise software layer is as strategic to sovereignty as cloud and semiconductors"**
>
> Aiman Ezzat

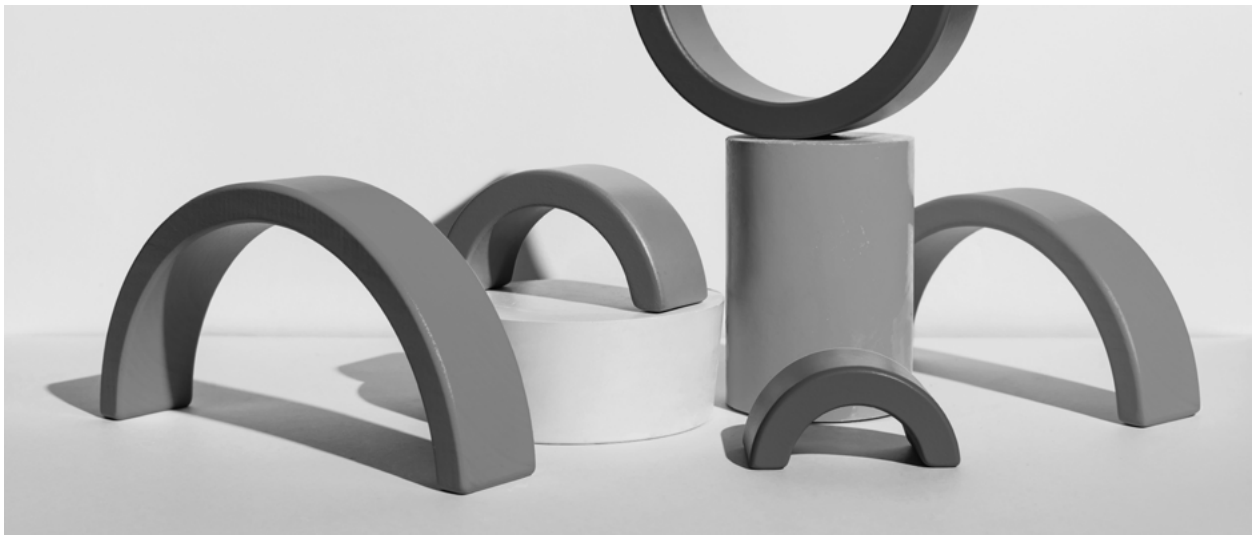
End-to-end sovereignty?

Do you believe true end-to-end European digital sovereignty is achievable? And perhaps more importantly, is it desirable?

— Christian: Yes, European digital sovereignty is achievable, as long as we define sovereignty in a practical way. It isn't about shutting ourselves off or insisting everything needs to be built in Europe. For me, it's really about having the ability to act, and making sure that critical data is governed under European control, oversight, and decision rights.

Europe can still use the best global technologies while ensuring that data stays here, is managed under European jurisdiction, and fully complies with European regulations. So, the goal here isn't complete self-sufficiency. It's about making sure that Europe has the power to govern its digital future.

> **"Europe can still use the best global technologies while ensuring that data stays here, is managed under European jurisdiction, and fully complies with European regulations"**
>
> Christian Klein



— Aiman: I don't believe total, end-to-end digital sovereignty – meaning Europe owning every layer of the technology stack outright – is either realistic or desirable. No country or region can control every component of the stack; even the largest players depend on international collaboration and global supply chains. Pursuing absolute self-sufficiency would be impractical and could isolate Europe from innovation happening elsewhere. Europe doesn't need to own every layer to achieve meaningful sovereignty, but it does need assured access to – and control over – the critical layers.

> **"I don't believe total, end-to-end digital sovereignty – meaning Europe owning every layer of the technology stack outright – is either realistic or desirable"**
>
> Aiman Ezzat

What is both realistic and desirable is "strategic autonomy": the ability to choose and manage our dependencies to protect European interests. That means identifying which parts of the digital value chain are truly critical – and designing for resilient interdependence rather than complete independence. In practice, it involves strengthening European capabilities in key domains, building strategic partnerships (both intra-European and transatlantic), and putting robust contingency plans in place. Together, these measures can preserve autonomy and continuity, even in a crisis. That balanced approach is what I call "pragmatic sovereignty."

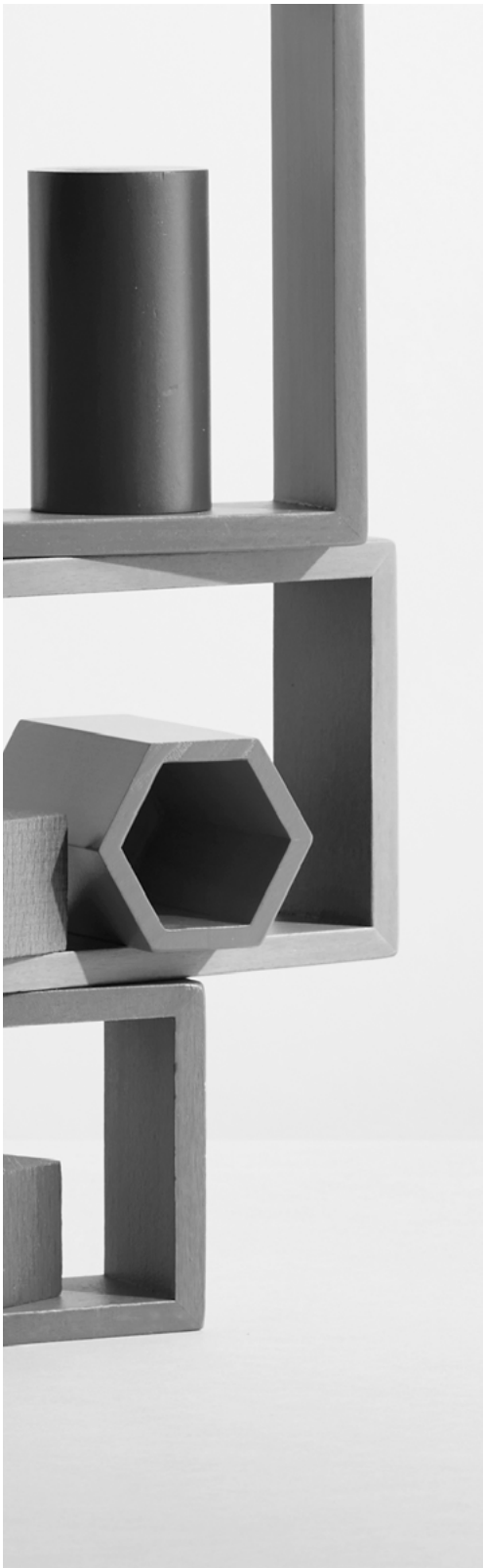
Do European consortium approaches to sovereignty work or does Europe need its champions to move independently?

— Christian: I think consortium approaches can work extremely well, but only if we show up as one Europe. We need to bring our champions together, rather than expecting any single player to solve sovereignty.

That's exactly what our expanded Sovereign Technology Partnership with Capgemini is designed to do. Together with other European champions like Mistral AI and Bleu, we're accelerating cloud and agent-based AI solutions for Europe's most critical sectors, including the most regulated ones, such as defense and the public sector.

Ultimately, sovereignty in Europe will come from strong, connected ecosystems that combine innovation with trust and can scale across the single market"

Christian Klein

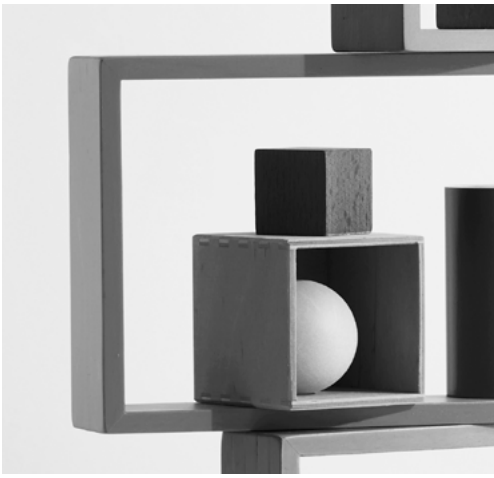


At the same time, we have to be honest about where things stand. In Europe, it's still too hard and too slow to create and scale startups. Bureaucracy and fragmentation are holding us back. When public and private players align, you can see how much faster we move when the whole ecosystem pulls in the same direction.

Ultimately, sovereignty in Europe will come from strong, connected ecosystems that combine innovation with trust and can scale across the single market. We've already shown we can win. The talent is here, the data is here, the customers are here. What's missing isn't capability; it's speed. In many ways, the message is simple: Europe has the engine. Now we just need to take the handbrake off.

— Aiman: We are seeing valuable consortium-based approaches in Europe – partnerships where industry and governments come together to build shared "sovereign" solutions. These models can work particularly well in domains such as defense or critical infrastructure. For example, Capgemini co-leads the "Réseau Radio du Futur" consortium with Airbus for France's Ministry of the Interior, and we also partner with other organizations, such as Thales, on strategic programs (e.g., 5G via satellite). These collective efforts pool European expertise and resources. At the same time, in fast-moving technology domains, Europe's organizations need the freedom and support to innovate at speed and scale – and to move quickly and independently when required.

From my perspective, it's not an either/or choice – both approaches are needed. Europe should use consortium models where no single player can succeed alone, or where standard-setting and interoperability are essential. In parallel, Europe must foster and invest in its leading tech firms and startups so they can scale into global champions. Measures such as a "European preference" in public procurement can help by creating a sizeable home market, alongside supportive policy, innovation funding, and – in some cases – cross-border mergers or alliances to build scale. In summary, European sovereignty should combine collaboration where it makes us stronger with independent action where it makes us faster.



The regulatory ask

What are your top asks of European regulators? And does today's regulatory approach enable sovereignty or limit innovation and competitiveness?

> **Regulation should focus on the outcomes we all care about, like resilience, continuity, and competitiveness, rather than prescribing technical details"**
>
> Christian Klein

— Christian: First, I would really like to see a harmonized definition of sovereign cloud across Europe. One standard, not 27. France is already leading the way with SecNumCloud, but a clear, pan-European approach would be much more efficient for everyone.

Second, if we want to compete, we need to simplify. It is about better regulation, not more regulation. Organizations should be enabled to build and ship faster. Europe needs a true single digital market that encourages deployment, rather than hesitation.

Regulation should focus on the outcomes we all care about, like resilience, continuity, and competitiveness, rather than prescribing technical details.

— **Aiman:** Regulatory requirements should be risk-based, proportionate, and able to keep pace with technological developments. Extending EU-level regulatory sandboxes – and enabling real-world experimentation – will be essential to accelerate innovation and lower market-entry barriers. In recent years, Europe has developed a distinctive regulatory approach; the right balance must be found between citizen protection and competitiveness. Overregulation, particularly for emerging technologies such as AI, risks slowing adoption and undermining Europe's ability to compete. Sovereignty should rest on unified, stable, and forward-looking frameworks that enable innovation.

> **Regulatory requirements should be risk-based, proportionate, and able to keep pace with technological developments"**
>
> Aiman Ezzat

What would be your one piece of advice to a CEO who wants to get sovereignty right?

> **My advice would be this: define sovereignty based on risk and business impact, not ideology"**
>
> Christian Klein

— **Christian:** My advice would be this: define sovereignty based on risk and business impact, not ideology. Focus on the basics, such as data governance, operational oversight, and continuity. Use the best global innovation, but make sure you keep control, auditability, and compliance firmly under European legal and regulatory frameworks. And finally, take the handbrake off. Standardize your data, embed AI directly into your core workflows, and build on platforms that give you real governance and control.

— **Aiman:** My one piece of advice is to take a pragmatic, business-focused approach to sovereignty. Start by mapping your critical digital dependencies and risks. Identify where a loss of technical control – or undue foreign influence – would materially impact your business, and focus on what is truly mission-critical. Then build a sovereignty plan that mitigates those

> **My one piece of advice is to take a pragmatic, business-focused approach to sovereignty"**
>
> Aiman Ezzat

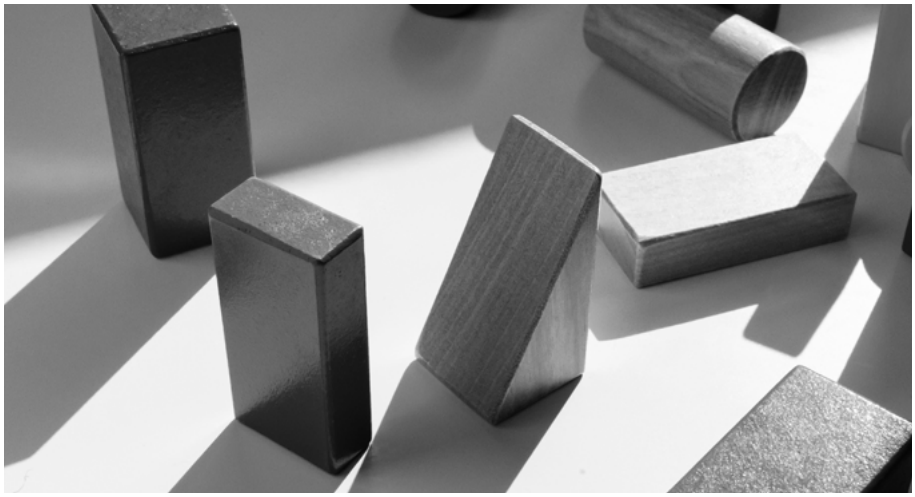
risks without undermining efficiency or innovation. For example, you might ensure your most sensitive data sits on European cloud infrastructure, protected with strong encryption and local legal oversight, and/or adopt a multi-cloud strategy so you are not tied to a single provider.

Choose solutions that protect autonomy while supporting innovation and competitiveness. Whether that means using a "sovereign cloud" for specific workloads, adopting open source where it is fit for purpose, or negotiating contracts that guarantee data residency and audit rights, ensure your sovereignty measures align with your business objectives. In short: be clear-eyed about your dependencies, address them with realistic measures, and keep the benefits of global technology.

Can sovereignty become a driver of innovation and competitive advantage?

— **Christian:** Yes, it absolutely can. Digital sovereignty has become a foundation for security, resilience, and growth. It creates the trusted environment needed to adopt and scale new technologies.

> **"Digital sovereignty has become a foundation for security, resilience, and growth. It creates the trusted environment needed to adopt and scale new technologies."**
>
> Christian Klein



Sovereign AI, for example, unlocks innovation across industries, whether it is in drug discovery, industrial automation, or any other domain where high-quality data and deep expertise matter. The competitive advantage increasingly comes from the ability to securely access and use enterprise and industrial data in a meaningful way.

And this is where Europe can really stand out. Trusted, governed, accountable AI is what scales, especially in regulated and mission-critical environments. That is how Europe can win the industrial race. The winners will not be thin tools or standalone agents, but the platforms that embed AI into governed, end-to-end business processes.

— Aiman: Yes – if approached correctly, digital sovereignty can absolutely drive innovation and competitiveness. The key is to treat sovereignty not as a constraint, but as a framework for building genuine capability. When we balance strategic autonomy with access to best-in-class technology, sovereignty becomes a source of resilience and competitive differentiation – pushing us to design systems with greater security, transparency, and control, and ultimately to deliver better products.

Moreover, investing in sovereign technology capabilities can foster homegrown innovation in Europe. We see that when teams focus on strategic needs – privacy, security, compliance – they often generate creative solutions that become value propositions in their own right. Done well, sovereignty is not just about compliance; it is a catalyst for innovation. Bleu is one example: we built something new to meet a clear market need, combining advanced cloud functionality with the highest level of data protection under French law. Sovereignty created the demand – and innovation filled it.

Looking forward

What is the role of European AI models in building a digitally sovereign Europe?

— Christian: When people say Europe is falling behind in AI, I always ask: behind what exactly? If the race is for the next chatbot, maybe. But the real opportunity for Europe is Industry AI, and SAP will be a large part of that. We have some of the world's highest-quality business data and deep industry expertise.

At the same time, Europe needs the ability to use the best global technologies, but in a way that operates under European governance and rules. That balance is essential.

This is why partnerships such as that between SAP and Mistral AI matter so much. They bring world-class AI, but on European terms – secure, compliant, and sovereign.

— Aiman: European AI models are central to sovereignty. If the most advanced models remain predominantly non-European, European businesses and governments face a structural dependency for a capability that is becoming critical to decision-making and day-to-day operations.

Agentic AI sharpens this challenge considerably. When autonomous agents make decisions and orchestrate other systems, the question is no longer only "Where is my data?" – it becomes "Who controls the decision loop?" Europe needs players that can provide control frameworks to ensure real strategic autonomy. We will not achieve this by ignoring OpenAI, Anthropic, or Google, but by harnessing their technologies alongside European champions such as Mistral AI. Our expanded strategic partnership with Mistral AI, jointly with SAP, illustrates this approach: delivering secure, scalable AI systems for highly regulated sectors with strict data requirements, including financial services, the public sector, aerospace and defense, and energy. European AI models enable innovation while keeping data and algorithms under European governance. They are a critical component of a digitally sovereign Europe.

Christian Klein
CEO, SAP SE

"European digital sovereignty is achievable, as long as we define sovereignty in a practical way"

Aiman Ezzat
CEO, Capgemini

"Done well, sovereignty is not just about compliance; it is a catalyst for innovation"

Executive conversations with...

ANU BRADFORD

Henry L. Moses Professor of Law and International Organization

Columbia University

NAVIGATING TECH SOVEREIGNTY IN A FRACTURED WORLD

Anu Bradford is a leading expert on how regulation and state power shape the digital economy. She currently serves as a special advisor on technology sovereignty to European leadership. She is the author of The Brussels Effect: How the European Union Rules the World (2020), named one of the best books of 2020 by Foreign Affairs. Her newest book, Digital Empires: The Global Battle to Regulate Technology, was published in September 2023. It was recognized as one of the best books of 2023 by Financial Times, and awarded the 2024 Stein Rokkan Prize for Comparative Social Science Research. At the Columbia Law School, Bradford is the Director of the European Legal Studies Center. Before joining the Columbia Law School faculty in 2012, Bradford was an assistant professor at the University of Chicago Law School. She also practiced EU law and antitrust law in Brussels, and has served as an adviser on economic policy in the Parliament of Finland, and as an expert assistant at the European Parliament. The World Economic Forum named her Young Global Leader '10.

You coined the term "Brussels Effect" to describe how EU regulations shape global tech practices. Where do we stand today on Europe's digital regulatory influence?

Anu Bradford: I think the high-water mark of Europe's regulatory leadership is behind us. A few years ago, during the peak of the "techlash," it seemed like the world was moving toward stricter digital rules and the EU was setting the tone. Even the United States, under President Biden, initially leaned into tougher tech regulation. But since then we've seen a strong backlash. Externally, Washington has become more hostile to any foreign power, including the EU, trying to discipline American tech companies. US policymakers resent Europe's attempts to set rules for Silicon Valley, and we've even seen Congressional hearings criticizing the Brussels Effect. At the same time, inside Europe a narrative has taken hold that perhaps over-regulation is hurting our competitiveness. A high-profile report led by Mario Draghi, for example, argued that Europe's innovation deficit is partly due to burdensome regulation. This has shifted the conversation in Brussels. EU leaders have gone from championing digital rights and stringent oversight to asking, "Are we too heavy-handed? Do we need to dial back regulation and focus more on innovation?" As a result, the European Commission has proposed easing or revisiting some policies – including "Digital Omnibus" to simplify rules and rethink parts of the AI Act and GDPR. In short, Europe's resolve to be the world's digital regulator has wavered under US pressure and internal doubts.

Anu Bradford
Henry L. Moses Professor of Law and International Organization, Columbia University

In a recent *Foreign Affairs* article, you warned that Europe could "lose what makes it great." What were you cautioning against?

Anu Bradford: Europe has many strengths and some deep weaknesses. My warning was that the EU must not throw away its greatest strength in the digital era – its commitment to protecting users' rights and a fair digital marketplace. Europe has led the world in defending privacy, online safety, and competition. And let's be clear: we cannot count on tech CEOs to voluntarily protect societal values. Democratic oversight is needed to set guardrails for the digital economy, and Europe has been that global standard-bearer. Europe shouldn't fight the wrong battle. Over-regulation is not the core reason Europe lags in tech – lack of a unified digital market, underdeveloped capital markets, cultural aversion to risk, and talent gaps are much bigger factors. Rather than dismantling the GDPR or weakening upcoming AI rules, Europe should tackle those fundamentals. Complete the digital single market so startups can scale across the EU. Build a robust capital markets union so innovators have access to growth funding. Reform insolvency laws and the culture around failure so entrepreneurs can take risks and try again. And work on immigration to attract and retain tech talent from around the world. These steps would do far more for competitiveness than gutting the EU's digital regulations.

"Over-regulation is not the core reason Europe lags in tech – lack of a unified digital market, underdeveloped capital markets, cultural aversion to risk, and talent gaps are much bigger factors."

In your new book *Digital Empires*, you outline three competing tech models – the American market-driven approach, Europe's rights-driven approach, and China's state-driven model. How are those models evolving today?

Anu Bradford: We're seeing a real convergence toward the state-driven model in many ways. Everyone is playing Beijing's game now. Geopolitical tensions have pushed governments to take a much bigger role in tech. The United States, traditionally very hands-off and market-driven, is now intervening heavily in the tech sector when national security or strategic advantage is at stake. The US is subsidizing domestic semiconductor manufacturing, restricting exports of advanced chips, even taking equity stakes or imposing investment bans – actions that make the US sometimes seem more Beijing than Beijing. Europe has launched its own industrial policies for tech as it is striving for greater technological sovereignty. Europeans are way too dependent on American and Chinese technologies. I used to worry about Europe's need to de-risk from China, but now Europeans need to de-risk from the USA as well. So the gap between the free-market approach and the state-controlled approach is narrowing. Each of the big three is emphasizing sovereignty and control over key technologies.

That said, there are still important distinctions. Culturally, the US remains more techno-libertarian – it's empowering Big Tech to drive innovation and is quite hesitant to regulate data privacy, AI, or social media content. The prevailing view in Silicon Valley and Washington is that regulation could undermine America's tech lead, so they're skittish about the kind of strict rules Europe favors. Europe, meanwhile, is in an identity crisis of sorts: it has championed a rights-driven model (privacy, safety, competition), but now, it's second-guessing itself and inching toward the US stance of lightening up on rules. And China of course continues with its government-steered, authoritarian model: strong state control of data and platforms, tight censorship, and massive state investment in tech sectors.

> **"The modern tech ecosystem is deeply globalized and interdependent"**

Importantly, the values-based, rights-driven approach hasn't disappeared. There is still significant public demand for privacy protection, accountability, and curbing corporate excesses. Even in the US, despite the deregulatory rhetoric, there's bipartisan concern over Big Tech's power – antitrust cases against tech giants are ongoing, and many states are implementing their own privacy and AI rules. In Europe, there is pushback against deregulating too much. So we're in flux. Overall, we do see more state influence and a tilt toward protectionism everywhere, but there's also an underlying recognition that

completely unbridled tech markets can threaten important social values. The three "digital empires" are still distinct, but the lines are blurring as each tries to secure its technological future in a volatile world.

Is true technological sovereignty actually achievable?

Anu Bradford: Many nations are indeed trying to hedge their bets and build up domestic tech capabilities. India, for example, talks about digital sovereignty and has taken steps like data localization and promoting homegrown startups. Countries like Russia, Brazil, and others have voiced desires to control more of their digital destiny. The drive to be less dependent on foreign technology has become quite universal. However, genuine end-to-end tech sovereignty is extraordinarily difficult, if not impossible, for almost any country. The modern tech ecosystem is deeply globalized and interdependent. Take semiconductors: no single nation controls the entire supply chain. The US might design leading-edge chips, but it relies on Dutch lithography machines, Japanese chemicals, Taiwanese or Korean manufacturing, and rare earth minerals largely processed in China. China itself, despite pouring resources into chip development, still depends on foreign chip-making equipment and intellectual property. Europe has strengths in areas like semiconductor equipment (ASML in the Netherlands, for instance), but it doesn't do it all either. No country can go it alone, not even a superpower.

GENUINE END-TO-END TECH SOVEREIGNTY IS EXTRAORDINARILY DIFFICULT, IF NOT IMPOSSIBLE, FOR ALMOST ANY COUNTRY.

What do these geopolitical shifts mean for global companies? How should businesses navigate a world where technology markets are fragmenting along national lines?

Anu Bradford: It's becoming a huge challenge for multinational tech companies – and really any company touched by digital rules (which these days is almost everyone). For the past decade, a lot of firms benefited from relatively harmonized standards or at least the ability to operate globally with one set of practices – often defaulting to the strictest regime, like the EU's rules, and applying it worldwide. That was the classic Brussels Effect. Now, companies are increasingly caught between conflicting governments and regulations. The US and EU, for example, diverge on things like content moderation, data flows, and AI oversight. A platform might be required by European law to take down hate speech or disinformation, but in some cases, doing the same in the US could provoke political backlash or even violate more permissive US rules on speech. The eventual prospect of irreconcilable rules is real.

For businesses, this means higher costs and difficult choices. They may have to maintain separate systems, policies, or even product versions for different regions. We already see a mild version of this – think of social media companies turning off certain features in Europe to comply with GDPR or the Digital Services Act, or cloud providers offering special "sovereign cloud" partitions for European clients. In the past, companies often chose to comply globally with the toughest standard to keep things simple, but now the toughest standard might earn them punishment elsewhere. If fragmentation intensifies, some firms may run region-specific configurations to meet conflicting requirements. That's expensive and operationally complex, but it may be necessary in some cases.

> **"No country can go it alone, not even a superpower."**

There's also a real trust issue at play. International customers and governments are starting to question whether foreign tech providers will obey local laws or the dictates of their home government. For example, European officials worry: if push comes to shove, will an American company side with Washington or Brussels? We saw the inverse in the US with TikTok – can a Chinese-owned platform truly firewall its US user data from Beijing's government? Many in the US doubt it, hence the pressure on TikTok. Similarly, European clients are beginning to ask whether using an American cloud service could expose them if a future US administration takes a hostile turn. This is forcing companies to make promises of "digital sovereignty" solutions – like storing and processing EU data only in Europe, under European jurisdiction, to reassure customers.

"International customers and governments are starting to question whether foreign tech providers will obey local laws or the dictates of their home government. "

Companies find themselves between a rock and a hard place. Take a concrete scenario: If a US administration were to demand that an American tech firm cut off services to Europe or hand over European user data, that company is in an impossible position – violate US law or EU law, either way it faces huge legal liability and reputational damage. We haven't seen something that extreme yet with US and Europe (since they are allies), but we've seen it in other contexts like sanctions compliance, and it could happen in the tech realm too. Until now, such transatlantic conflicts have been rare and were handled as exceptions instead of systemic issues. Still, businesses have to be savvy. They need contingency plans for geopolitical fractures – everything from diversifying their supply chains to being ready to localize operations if required. In some cases, companies might decide a market is too risky and exit if the legal requirements diverge massively. We have seen companies face choices in China that led to public backlash, making continued operation difficult or even impossible. It's not unthinkable that similar hard choices could arise elsewhere.

Companies will have to be more agile and jurisdiction-specific. They'll need to engage with policymakers in all major markets to find workable compromises – essentially becoming diplomats as well as businesses.

Do you think companies need to elevate geopolitical risk management to the C-suite? Is it time for a chief geopolitical officer?

Anu Bradford: Absolutely. Geopolitical risk has moved from a peripheral concern to a central, boardroom issue for global companies. Just as firms have chief financial

officers to manage financial health and chief security officers to manage cybersecurity, they now need a high-level chief strategist for political and geopolitical risks. Whether you call it a chief geopolitical officer or something similar, the role would be to anticipate and navigate the kind of challenges we've been discussing – regulatory fragmentation, sanctions, trade wars, even conflicts that could disrupt operations.

"Geopolitical risk has moved from a peripheral concern to a central, boardroom issue for global companies."

In practical terms, that means building a team dedicated to scanning the horizon for geopolitical developments and analyzing how they might impact the business. This team needs to work closely with all parts of the company – product, supply chain, compliance, sales – because geopolitical issues affect all aspects of the business. The geopolitical risk team has to be plugged into corporate decision-making, not just producing occasional memos. I'd expect them to do scenario planning ("What if relations between X and Y sour next year? How do we respond?"), to advise on market entry or exit decisions, and to liaise with government affairs teams on policy trends.

Many companies right now address these risks in a piecemeal way – a legal team handles sanctions compliance, an operations team handles supply diversification, maybe an external consultant is called in when something blows up. That's not enough anymore.

What should such a geopolitical risk team look like? What skills or approaches are crucial for managing these risks effectively?

Anu Bradford: The key is diversity of perspective and expertise. Geopolitics is multifaceted – it spans economics, law, security, culture – and it plays out differently in different regions. So you can't expect one analyst or one data model to capture it all. You need a team comprising people who understand various domains and geographies. These experts need to collaborate and cross-pollinate insights. They need to be able to connect the company's strategy and business opportunities, with an understanding of technology, all tied with awareness of domestic and foreign politics. They need to be proactive in risk assessment, while also recognizing that there's a lot of noise. If you don't have a seasoned geopolitical risk team, they start overreacting to everything. Companies also need to have regional expertise. For instance, it's hard to find someone who knows how Brussels will react, who also understands Beijing.

For emerging technologies such as AI, how can countries balance the pressure to regulate with the push for innovation?

Anu Bradford: AI is multifaceted and fast-moving, with high stakes for both risks and opportunities. Governments should not be spectators who let companies alone shape the next decade. We need a nimble regulatory approach, with rules in place now and a willingness to revise them as the technology evolves.

In Europe, revisiting the AI framework so soon after enactment risks eroding credibility and creating more uncertainty just as companies are adjusting. Some proposed changes are postponements, for example taking longer to finalize standards in high-risk areas. Others could be more far-reaching, such as ideas about using personal data to train large language models. I worry about reforms being pushed further by corporate pressures, and about less resolute enforcement at a time when the AI race is heating up and geopolitical tensions are high. That combination increases the risk of irresponsible choices that could harm society.

> **"Geopolitics is multifaceted – it spans economics, law, security, culture – and it plays out differently in different regions."**

This is not about choosing innovation or safety. We need both, starting now, and we should refine the rules as we learn. I am concerned that early moves to simplify may go too far, create uncertainty, and send

IN EUROPE, REVISITING THE AI FRAMEWORK SO SOON AFTER ENACTMENT RISKS ERODING CREDIBILITY AND CREATING MORE UNCERTAINTY JUST AS COMPANIES ARE ADJUSTING.

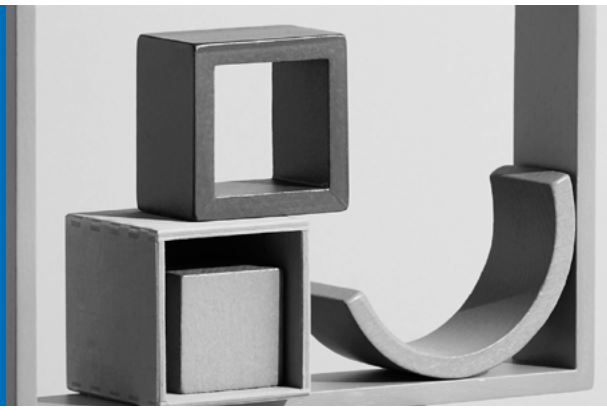
mixed signals while many governments are drafting their own frameworks and looking to Europe's direction. Meanwhile, the US is moving fast, often focused on AGI (Artificial General Intelligence) and China is making pragmatic gains, including globally with open-source AI. Europe needs to play to its own strengths, which is unlikely to be foundation models for most companies. But there is no inherent disadvantage Europe has when it comes to developing AI applications and accelerating AI adoption across industries. The question is what race really matters, and how to ensure AI is safe as it advances.

Is AI sovereignty a realistic goal?

Anu Bradford: True AI sovereignty would mean that a country keeps its vulnerabilities manageable. No one is going to control the entire AI stack, from raw materials and cloud services to data sovereignty, locally developed models, and especially the hardware layer, where semiconductors are an example of a globally deeply interconnected industry. So I do not think there is such a thing as full AI sovereignty. The realistic goal is relative, to move toward greater sovereignty

"I do not think there is such a thing as full AI sovereignty.

"True AI sovereignty would mean that a country keeps its vulnerabilities manageable."



by reducing vulnerabilities. For some countries that means more partnerships and hedging. For others it means enhancing domestic investment to do more within their borders and build capabilities.

For the United States, the goal has also been to restrict rivals' access to key capabilities, for example limiting China's access to choke points like the most advanced chips to maintain leadership in the AI race. That can also give China an incentive to innovate around constraints, and China has been good at making AI development more capital-efficient and energy-efficient. The US has vulnerabilities too. Energy costs are high and the grid is limited, while data centers need a lot of power. That can raise energy bills and become politically costly in a country that is already struggling with a cost-of-living crisis. The US does not control the entire stack, and ramping up chip production domestically is not feasible quickly because it lacks all the equipment and raw materials. Even where there is money, investments are often funded by debt and can become systemically fragile. It is possible to run out of power for the data centers being built. Even the world's AI leader faces limits in that elusive pursuit of AI sovereignty.

In Europe, countries also need to think about how their geopolitical vulnerabilities and their environmental costs factor into these choices.

What do you see as the role of initiatives such as the Euro Stack or Gaia-X for developing common digital infrastructure?

Anu Bradford: Europeans need a real industrial policy plan. My worry is that it can lead to a lot of wasteful investment. European governments do not have unlimited money. Gaia-X has not been particularly successful. There have been attempts, for example by the French government, to rebuild a French search engine and even to default governments use suboptimal technologies. That does not work. Industrial policy is probably necessary these days, but it remains vulnerable to being profligate.

We need a combination of private and public capital to fund the Euro Stack. The Euro Stack cannot be a complete alternative to American technologies. Some technologies are easier to build at home, others are harder. Europeans need to be clear-eyed about their strengths and vulnerabilities, the relative costs, what can be done immediately, what can be done in the medium term, what can be done in the long term, and what the priorities are. Everything cannot be done immediately, and the money is limited.

That is why I am eager to unleash more private capital in Europe. The capital markets union should be a no-brainer, and it has been in the works for a long time. There is a lot of capital in pension funds and institutional investments that is not channeled into the system. There are many restrictions on where they can invest, and risk tech is not available for pension funds in many European countries. Europe has money, but it needs to be channeled much more effectively.

> **"Even the world's AI leader faces limits in that elusive pursuit of AI sovereignty."**

We cannot afford to rely only on government-

driven build ups. Much of that is going to go to military technologies, and many of these technologies are dual use. In the United States, it is not the Pentagon that is developing AI for the military. It comes from Silicon Valley and it is dual use, serving commercial and military applications. There needs to be efficient partnering, including joint procurement where there is public money, and we also need to fully unleash entrepreneurship and capital markets to help build European capabilities.

What are your views on the emerging topic of data sovereignty?

Anu Bradford: The data sovereignty question is very important. China has long restricted the movement of data outside the country. The US, including in the WTO, long promoted the idea that data flows should not be restricted, but even the US is now changing its position. Europeans, through the GDPR and related decisions, have sought to restrict data flows to the US where they could compromise data privacy rights. So we now have both privacy and national security concerns, two reasons to push for greater data sovereignty.

We have seen growing requirements to store data locally. But data localization mandates are costly for companies. I think countries should at least prepare for obligations that push toward localized data solutions, or require proof that sovereign control over data can be protected even by foreign companies. The question is what companies do under the US CLOUD Act. Europeans know the US can compel US tech companies to hand over data to the US government and that is a growing concern as the transatlantic rift deepens.

> **"There is a large pool of untapped data in Europe that must be protected but also used for innovation, investment, and commercialization in ways consistent with data protection."**

For Europeans, data sovereignty has mostly been viewed through the lens of protecting data. That lens is important, but it has meant forgoing many opportunities to commercialize data. There is a large pool of untapped data in Europe that must be protected but also used for innovation, investment, and commercialization in ways consistent with data protection. I regret the idea that this is often viewed as a stark choice between rights and commercial opportunities. Companies can provide solutions that meet both aims. We should show how to unlock the potential of these data pools while insisting it be done without compromising data privacy. You can have both.

If you were advising the board of a Global 500 company on geopolitical risks in technology, what are the top two or three actions you would recommend they take this year?

Anu Bradford: I would focus on three areas.

If TSMC were disrupted, the global economy would halt."

- US–China decoupling and Taiwan risk
  You still see decoupling between the United States and China, given the magnitude of technological rivalry and the size of those two markets. Boards need to manage a potentially deepening rift between them. There are more conciliatory signals about maintaining functional business relationships, but there is still a geopolitical calculus around Taiwan. If TSMC were disrupted, the global economy would halt. I am not predicting China will take ownership of Taiwan, but every board should consider scenarios involving Taiwan, the United States, China, and the depth and manifestations of tech decoupling. If you overplay the risk, you may forgo opportunities; if you underplay it, disruptions can be severe.
- Europe's regulatory role and transatlantic dynamics
  Europe generates much of the tech regulation and provides leadership for the rest of the world. If Europe retreats, that would significantly shift the regulatory environment. I doubt Europe will retreat all the way, but companies must navigate transatlantic tensions and Europe's efforts to gain greater technological sovereignty by de-risking from China and also de-risking from the United States. This matters given the value of the European market, the presence of tech companies there, and the potential breaking of a united front between the United States and the EU.
- Managing an AI bubble and concentration risks
  Boards should plan for the possibility that an AI bubble could burst and affect investment flows and the industry. At the same time, accelerate adoption and invest in the right players and layers. There is risk if you do not invest in AI, but you also need to choose suppliers carefully and hedge against failures. Diversify across an increasingly concentrated AI market so you are not dependent on a single country, a single player, or a single large language model. Ensure you have alternatives. Protect the integrity of your firm's data that may be used to train large language models. Where possible, consider bespoke models that give you more control. Think about solutions not only at the country level, but at the level of your company: your data, your models, your vulnerabilities, and what happens if some providers do not exist in a few years.

If you had a magic wand, what is the one thing you would change about how companies manage geopolitical risk, or how the EU and other countries approach it?

Anu Bradford: I would have companies treat geopolitical risk, and risk generally, as an opportunity to clarify the company's purpose and values. Use volatility to rethink how you run things, how you anchor decisions, and what your values are, so you are not simply following political winds. Do not do it the Mark Zuckerberg way where you lean into content moderation, then abandon it when the politics changes. That makes a company look like it has no principles.

Trusted companies project confidence through turmoil. Think of the spirit of Mark Carney's (current prime minister of Canada) Davos remarks: know who you are, accept volatility, be clear about your strengths and principles, and state what you will do under scenarios A, B, or C. Be prepared because you have invested in knowledge, refined strategy, and built nimbleness. Combine pragmatism and realism with a principled foundation, so you are not rudderless, choosing sides day to day.

"Use volatility to rethink how you run things, how you anchor decisions, and what your values are, so you are not simply following political winds."

Companies with clear values gain the trust of the marketplace. For example, the Trump administration put pressure on Microsoft to let go of a public policy person who was seen as misaligned with the US politics; Microsoft did not act, let the storm pass, and the person was not removed. If you start dismissing personnel, abandoning customers, or leaving markets, you look directionless and without a compass. Do not be naive; develop diplomatic skills and pragmatism. But without an anchor in values and core principles, companies ultimately lose the trust of their customers and employees. Seen this way, all the unfolding uncertainty and volatility can also be a moment of great clarity for confident and well-run companies.

Anu Bradford
Henry L. Moses Professor of Law and International Organization, Columbia University

"Do not be naive; develop diplomatic skills and pragmatism. But without an anchor in values and core principles, companies ultimately lose the trust of their customers and employees."

ALEXANDER ZWART

**CITO,
Rabobank**

SOVEREIGNTY BY DESIGN

Alexander Zwart is the Chief Innovation and Technology Officer and Member of the Managing Board at Rabobank. He has been with the bank since 2008, holding a range of senior roles across digital transformation, technology, and customer experience, including Head of Digital Transformation and CTO for Retail Netherlands. Prior to joining Rabobank, he held roles at Nuon and Coca Cola, and holds a master's degree in business economics from Erasmus University Rotterdam/Michigan State University.

UNDERSTANDING DIGITAL SOVEREIGNTY

What does digital sovereignty mean to you?

Alexander Zwart: The problem with sovereignty is that so many people understand so many different things by it. The way we approach it is by asking what scenarios could plausibly play out in the world, and what kind of technology setup would best fit each of them. The inconvenient truth is that there is no single solution that ticks all the boxes.

A concrete example: when Iran was firing rockets on Dubai, people living there were quite happy that many banks were using a hyperscaler like AWS, because in a war situation they could move workloads somewhere else. If those banks only had data centers in Dubai, they would have been in a very bad place. But then we have also seen the opposite scenario, most recently with the American government deciding not to give access to certain AI models, and how impactful that can be.

Alexander Zwart
CITO | Rabobank

> **"The same architectural choice can be both a strength and a vulnerability, depending on the scenario"**

Two very different scenarios, one a war situation, the other a foreign government simply deciding to cut off access. The same architectural choice can be both a strength and a vulnerability, depending on the scenario.

As a bank, you have to be able to deal with both. Cash flow is king. A company survives or disappears depending on whether cash flow works. As soon as a bank cannot do payments, society has a huge problem. As soon as a bank cannot manage its treasury, the bank itself is in trouble. So whatever scenarios play out, payments and treasury must function independently of them. That means the answer is not either sovereign infrastructure or hyperscaler. You probably have to work with both. It is about being portable, being able to switch between different solutions, maintaining optionality, and being redeployable, meaning you can rebuild your technology stack very quickly if a specific landing zone fails.

These discussions are often very polarized and very negatively framed. That misses the point. In ten years' time, we will still work very intensively with Azure and AWS. The real question is whether, whatever happens in the world, we can still serve our customers. That is what matters most.

"That means the answer is not either sovereign infrastructure or hyperscaler. You probably have to work with both"

What is your view on the ongoing digital sovereignty debate in Europe?

Alexander Zwart: As a predominantly European company, the debate is very relevant. The operational resilience question about sovereignty is about making sure our critical functions remain available regardless of what any external party does. The strategic question is about the fact that Europe, as a continent, has simply not invested enough in technology. If you look at India, or at China, you see large parts of the world that did invest and built substantial industries. The United States did the same. Europe did not.

What concerns me is that some technology companies have become what I would call tech nations. It is not really a US versus Europe discussion. It is a question of whether Europe wants to have some very large technology companies that are European owned, with their main interests in Europe. Because what we have seen is that certain companies have become so large that the only government genuinely capable of controlling them is the US government.

EUROPE, AS A CONTINENT, HAS SIMPLY NOT INVESTED ENOUGH IN TECHNOLOGY

FROM PRINCIPLE TO PRACTICE

Rabobank is a cooperative bank. Does that change how you approach these questions in practice?

Alexander Zwart: The key difference is that our members are our shareholders. The General Members Council, which appoints our supervisory board, is made up of actual customers. And customers are much more interested in the long-term profitability and sustainability of the bank than a typical stock market investor might be. That means they are also willing to accept certain investments that a purely listed company might weigh very differently.

> "We are willing not just to become a customer of certain technology providers, but in some cases to become an investor as well"

Concretely, we are willing not just to become a customer of certain technology providers, but in some cases to become an investor as well. If we see a technology provider, potentially a European one offering capabilities not yet available in the market, and if we see that other organizations are also willing to become clients, we are prepared to invest for a period of time to help that company scale. Not to become a technology company ourselves, but to stimulate the market.

This is exactly what we have done. We became a customer of one such company and told them we were willing to invest to help make it happen. Alone, this would not have been possible. Our decision was driven by the fact that the Bank of New York was also investing in them, and that other parties in the market were willing to help that company scale. A cooperative bank can internalize that kind of long-term, society-oriented rationale more easily than a listed company can.

Beyond investment, what concrete steps is Rabobank taking on the operational side?

Alexander Zwart: We are analyzing our entire technology landscape through the lens of what we call business functions. Every capability we need to serve customers sits within a business function, whether that is the front office for mortgages, our banking app, or something else. These functions run on landing zones. In the past, we made choices about which landing zones to use with which providers, but we were not always sufficiently deliberate about which landing zones we wanted to support for which critical functions, or how concentrated our dependencies were becoming.

We are now much more conscious of concentration, and the way I frame it is this: in the past we looked primarily at how much money we spent with a given vendor. Now we also look at how concentrated we are in our processes with that vendor, and across which value chains. We assess whether we are highly concentrated in a critical value chain and whether we are portable enough to move if we need to. These are intentional decisions we are making rather than letting them emerge by default.

It is a balance, and it is important to be honest about that. A bank also has to meet serious security requirements. With the current capabilities of AI models, as soon as a vulnerability is identified, within minutes someone can determine the root cause and attack everyone who has not yet patched it. Even lower-level vulnerabilities become stepping stones into your systems. The risks in the world are increasing dramatically, so we cannot be naive on the security side while pursuing greater optionality on the sovereignty side. Both have to be held together.

"In the past we looked primarily at how much money we spent with a given vendor. Now we also look at how concentrated we are in our processes with that vendor, and across which value chains"

What role do payments play in sovereignty?

Alexander Zwart: Payments are so deeply embedded in people's lives that if they stop working, society has a problem. It is like electricity. If we cannot sell mortgages for a week, that would be very unpleasant for us, but Dutch society would not particularly care. Customers would go to another bank for a loan. But if payments do not work, customers cannot easily switch. Large companies work with multiple banks globally and can absorb a failure. But the vast majority of our customers are smaller enterprises, and they are deeply dependent on the single bank they work with, especially for cash flow and payments.

It is essential that a meaningful number of players are able to offer payment services. Right now, Mastercard and Visa are globally dominant, and I am quite positive about the European Payments Initiative precisely because Europe needs a credible alternative alongside them. That does not mean the other methods disappear. But having a European payment alternative is vital.

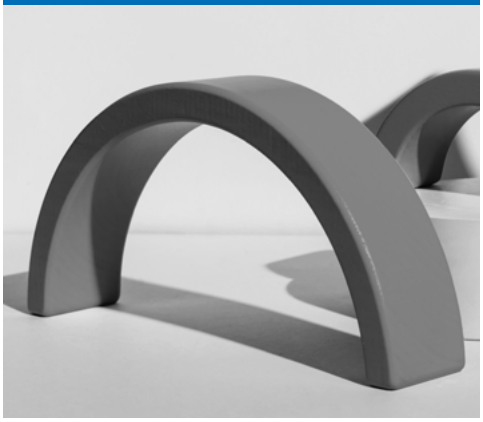
What India has done in this space is genuinely impressive. A local payments infrastructure has scaled enormously there. Payments and identity are so core to the functioning of society that you need competition and you need alternatives. A very limited set of global players controlling those functions is not healthy for the global economy.

HAVING A EUROPEAN PAYMENT ALTERNATIVE IS VITAL

How do you see the relationship between banks and hyperscalers evolving from here?

Alexander Zwart: We will continue to work very closely with hyperscalers. Depending on your size, there is a limited set you can work with in practice, so we want more than one, but we also do not want ten. The relationship is broadly good. But I think something important has to change in how the hyperscalers think about themselves.

"We will continue to work very closely with hyperscalers"



Banks have faced a similar tension. Most banks earn their money through mortgages and lending. Payments is often not where they make the money, but it is probably what society values most about what banks do. The same applies to hyperscalers. With cloud, they have become vital infrastructure for the world, and vital infrastructure, even when it sits inside the same company as everything else, is a different business. It has to be treated differently.

If the Google search engine goes down, people get frustrated. If Google Cloud goes down, the world has a major problem. Once you recognize that, the nature of the relationship has to change. The depth of knowledge we share, how well we understand the issues they face on the infrastructure side, how we take mitigating action so that even if that infrastructure fails our critical operations continue: all of that becomes far more important. The energy sector shows how this works in practice. Grid operators have to ensure supply regardless of what happens in the commercial layer above them. We already apply the same logic: our data centers have backup generators precisely because we do not wait to be rescued when supply fails. Hyperscalers have become multiple companies inside one entity, which is fine, but it means we have to look at them, and work with them, differently on those specific parts of the business.

OPEN SOURCE AND SOVEREIGN AI

Is open source a path to greater sovereignty?

Alexander Zwart: We are an organization that is still very attractive to good engineers, and that means we have the capability to build significant things ourselves. For organizations like us, working with open source genuinely helps, because you can draw on all the knowledge that has been integrated into open-source communities globally, and we have people capable of working with it.

> "For organizations like us, working with open source genuinely helps"

There is also a practical resilience dimension. If a SaaS solution we purchase is heavily based on open source, and for some reason the vendor can no longer support it, we could in principle take it over ourselves. In practice, we've done exactly that. We worked with Pivotal Cloud Foundry, and when needed, because Cloud Foundry is open source, we were able to insource the software and run it ourselves with our engineers connected to the Cloud Foundry community. That experience shapes how we think about architectural choices. Open source is now one of our architectural principles. All else being equal, we prefer solutions that are open source over purely proprietary code.

When it comes to AI, where does a bank's real sovereign asset lie?

Alexander Zwart: You have to be ruthlessly specific about where a bank is genuinely unique. Everybody thinks they are good at everything, but if you are truly critical about it, the set of things a bank is uniquely good at is quite small. The biggest asset is the ability to assess risk. The second is the ability to comply with regulation. Beyond those two, we are good at many things, but not uniquely so.

The truly proprietary data is not just the structured data sitting in databases. It is also the unstructured data in documents, and the knowledge that exists in people's heads, which gets discussed but never written down. That is the data a bank should be very careful about how it shares externally. Training models on that data makes complete sense. But you have to be specific about where you are actually unique, because if you are not, you are not building a sustainable advantage.

A good example is our ability to assess the risk of a small or medium enterprise customer. We hold detailed knowledge about that customer that is simply not publicly available anywhere. For a large, listed company, there is so much public information that the information asymmetry largely disappears. It is precisely where that asymmetry exists that banks have a unique position, and that data is really the business model.

Do sovereignty requirements constrain innovation?

Alexander Zwart: I think history simply shows the opposite. Innovation consistently happens when people face constraints. The most common argument I hear inside the bank is that someone needs more budget to innovate. But reality has proven, repeatedly, that if you give brilliant people a limited set of resources and a clear task, they find ways to accomplish things that unlimited resources would not have produced. DeepSeek is a recent and vivid example of exactly that. Resources are not the constraining factor. What makes the difference is a brilliant north star, the ability to bring intelligent and motivated people together, and a mindset oriented toward how we can do this rather than why we cannot. Constraints do not prevent innovation. In many cases, they produce it.

Alexander Zwart
CITO | Rabobank

"Reality has proven, repeatedly, that if you give brilliant people a limited set of resources and a clear task, they find ways to accomplish things that unlimited resources would not have produced"

JEAN COUMAROS

President & CEO

Bleu

FROM POLICY TO PLATFORM: BUILDING A TRUSTED CLOUD IN FRANCE

Jean Coumaros is President and Chief Executive Officer of Bleu, the French sovereign cloud services company jointly created by Capgemini and Orange. Appointed to lead Bleu at its creation in January 2024, he is responsible for building a trusted cloud platform designed to meet France's stringent security, regulatory, and data sovereignty requirements, including alignment with the ANSSI SecNumCloud framework. Prior to Bleu, Jean Coumaros was Director of Transformation and a member of the Group Executive Committee at Capgemini, where he led major group-wide transformation initiatives. Earlier in his career, he held senior leadership roles at Capgemini Consulting and Oliver Wyman, advising global financial services institutions on strategy, technology, and transformation.

UNDERSTANDING DIGITAL SOVEREIGNTY:

How would you define digital sovereignty today? And how have you seen its definition evolve in recent years?

Jean Coumaros: When I speak with clients, and we have quite a few now, what they mean by sovereignty consistently comes down to three things.

The first is cybersecurity. There is no credible claim to sovereignty if you are not protected against cyber criminals or cyber attacks, including those originating from organized groups in foreign countries. Cybersecurity is the foundational layer.

The second is protection against extraterritorial laws. The CLOUD Act and FISA are the most prominent examples, but at least a dozen countries have extraterritorial laws that can compel cloud providers to hand over customer data to a foreign government, legally, simply by requesting it. If your cloud provider falls under the jurisdiction of one of those countries, your sensitive data may be subject to lawful disclosure requests from a foreign government. That is the data sovereignty risk, and it is very real.

The third and more recently prominent concern is digital resilience, which I would also describe as keeping your digital dependence at an acceptable level. Even if you are cyber secure and protected against extraterritorial laws, being overly dependent on foreign providers introduces a different kind of risk. A foreign government decision could impede your

Jean Coumaros
President & CEO
Bleu

> "At least a dozen countries have extraterritorial laws that can compel cloud providers to hand over customer data to a foreign government."

provider from serving you, leaving you unable to serve your own customers. That is the "kill switch" scenario. If a provider can effectively press a button and bring your operations to a halt, your dependence has reached an unacceptable level.

In terms of how the debate has evolved, four or five years ago the dominant concern was extraterritorial laws, triggered largely by the passage of the CLOUD Act in 2018. That is when the debate about digital sovereignty and cloud sovereignty really took off in Europe. Over the past 12 to 18 months, digital resilience has emerged as an increasingly important and distinct dimension. That shift reflects a genuine maturing of the conversation.

"If a provider can effectively press a button and bring your operations to a halt, your dependence has reached an unacceptable level."

"Digital resilience has emerged as an increasingly important and distinct dimension."

Are you seeing misconceptions among clients about what sovereignty actually means?

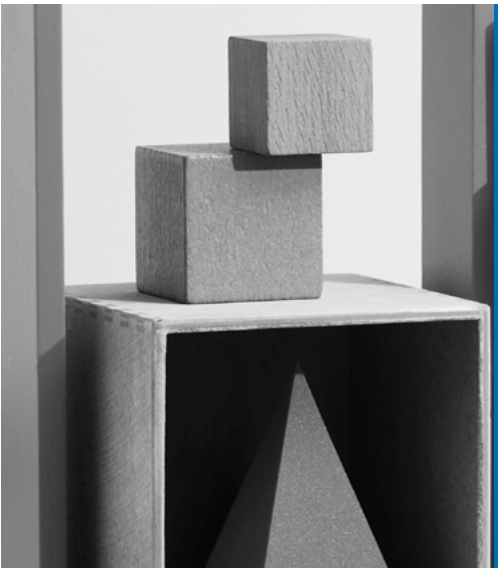
Jean Coumaros: Yes, particularly around digital resilience. In France and across several other European markets, including Germany, the debate has in some cases become irrational and almost caricatural. Some people have started to conflate digital resilience with digital autarky, expecting cloud providers to operate with zero dependence on non-European technology across every layer of the stack – hardware, software, and everything in between. They want the hardware made in Europe. They want all software layers made in Europe. That, in their view, is what real sovereignty looks like.

But digital autarky does not exist. It is neither possible nor advisable. Even those European cloud players who claim the highest levels of sovereignty rely on hardware from Asia or the United States, and on software components that are American or Asian in origin. A good example is virtualization. If you look closely at many so-called European sovereign cloud providers, their virtualization layer is in fact VMware, which is owned by Broadcom. Full end-to-end European provenance is simply not achievable.

What is achievable, and what genuinely matters, is keeping dependence at an acceptable level and ensuring full control over the specific parts of the value chain where it is most critical.

I will say this, though: when I speak with CIOs, I do not hear these irrational demands. CIOs are knowledgeable, pragmatic people. They understand what is feasible and what is advisable. The extreme positions tend to come from

DIGITAL AUTARKY DOES NOT EXIST. IT IS NEITHER POSSIBLE NOR ADVISABLE.



"What genuinely matters, is keeping dependence at an acceptable level and ensuring full control over the specific parts of the value chain where it is most critical."

media and social media, where people can be very vocal and very extreme on this topic. When you speak from professional to professional, people are very reasonable in the way they approach digital sovereignty.

BLEU AND THE TRUSTED CLOUD

Can you give us a quick overview of Bleu?

Jean Coumaros: Bleu is a 50/50 joint venture between Capgemini and Orange, the main telco in France and one of the leading telcos in Europe. The purpose of that joint venture is to build a trusted cloud, focused on the French market and on two specific segments within it: the public sector, and organizations operating in critical industries, including financial services, utilities, transportation, and health.

Our aim is to make Microsoft solutions – primarily Microsoft Azure on the infrastructure side and Microsoft 365 on the collaborative suite side – available in a trusted cloud environment for those segments.

Also, you may have noticed that I use the term "trusted cloud" rather than "sovereign cloud." That is deliberate. Sovereign cloud can mean many different things depending on who is using the term. Trusted cloud, at least in the French market, means something very specific: a cloud certified by ANSSI, the French cybersecurity agency, under their SecNumCloud referential. That label has a precise meaning. Sovereign cloud does not.

Can you give a concrete example of how Bleu helps organizations achieve their sovereignty goals, and what kinds of workloads are typically involved?

Jean Coumaros: Our offering has two main components: the collaborative suite, based on Microsoft 365, and the applications cloud covering IaaS, PaaS, and related services based on Microsoft Azure.

The typical organization we work with has been a Microsoft user for some time, either on the Azure side or on M365, and has come to the realization that for their sensitive data, the public Microsoft cloud is no longer sufficient. They need to ensure data sovereignty, but they do not want to abandon the technology they already know and operate. That is precisely what Bleu offers: the same Microsoft technology, deployed in a trusted, ANSSI-certified environment. There is no technology gap, no need to retrain IT teams, and no disruption to existing workflows. The key change is where the sensitive portion of their data sits.

> "Bleu is the right answer for sensitive workloads."

For central government in France, this is now a legal obligation. If you are a French public administration, your sensitive data must by law be hosted on a SecNumCloud-certified trusted cloud. For large private organizations, there is no legal mandate, but the imperative is no less real. Our clients include EDF, Dassault Aviation, Crédit Mutuel, and Orange, all of whom have publicly confirmed their relationship with Bleu. None of them use Bleu for all their workloads. That is not the model. Bleu is the right answer for sensitive workloads. For less sensitive data, many clients continue to use hyperscaler infrastructure alongside us.

There is also a growing ISV dimension worth highlighting. Independent software vendors who want to serve French public sector or critical infrastructure clients increasingly need to host their SaaS offerings on a trusted cloud. If EDF uses SAP, for instance, and wants SAP running in a trusted environment, then SAP needs to be hosted on a platform like Bleu. Those ISVs come to us just as a direct customer would. They open a tenant on Bleu, deploy their solution, and offer their services in SaaS mode using Bleu as their hosting partner. For any software vendor that wants access to sensitive clients in the French and European market, this is becoming unavoidable.

DIGITAL SOVEREIGNTY IN THE REAL WORLD

How significant is the challenge of interoperability for organizations that operate across borders?

Jean Coumaros: Our focus today is the French market, but under our agreement with Microsoft we have the right to also serve the European subsidiaries of our French clients. If I work with EDF in France, and EDF has subsidiaries in Italy or Belgium, I am perfectly entitled to support those affiliates across the EU, provided the relationship is anchored in the French parent company. That gives our French clients the ability to deploy Bleu services across their group, at least within the EU.

What I am not in a position to do, and not willing to do, is serve companies outside the EU. Extending into the US, for instance, could potentially bring us within the scope of the very extraterritorial laws we are designed to protect against. That boundary is deliberate and non-negotiable.

For genuinely global organizations with operations in Asia, the Americas, or the Middle East, Bleu will not be a single global solution. It will be the right answer for a defined scope. On the applications side, that is manageable, since application landscapes often vary by geography anyway. The collaborative suite is a more complex question. If not all users across a global organization are on the same platform, that can create friction and become a real consideration for global organizations to work through.

There is also a structural regulatory issue that bears on this. Today, each of the 27 EU member states has its own cybersecurity referential and certification framework. There is no single European certification. If you want to expand across Europe as a trusted cloud provider, you need as many certifications as countries you want to serve. There are active discussions at European level about creating a single referential, which would make life considerably easier for cloud players developing their business across the European market. But we do not have it yet.

And from what I can observe, when that common framework eventually arrives, it is likely to address the cybersecurity dimension, on which member states broadly agree, but may fall short on the data sovereignty dimension. Protection against extraterritorial laws requires not just technical and operational measures, but legal ones too: being a European company, having European shareholders, operating only within the EU. A European referential that addresses cybersecurity but omits those legal criteria will be a good framework for protecting organizations against cyber risk. It will do nothing for data sovereignty. And data sovereignty is equally important. That gap needs to be taken seriously.

Do companies actually "walk the talk" on sovereignty, or do they ultimately default to the hyperscalers when it comes to the decision?

Jean Coumaros: In the past, cost and convenience won, for two reasons. Sovereignty was not the pressing concern it is today, and the

"If you want to expand across Europe as a trusted cloud provider, you need as many certifications as countries you want to serve."

alternatives to hyperscalers were significantly less capable from a technical and functional standpoint. The result is that around 70% of the European cloud market ended up in the hands of US hyperscalers.

That is changing, for two reasons. First, the sovereignty concern has become substantially stronger, and it is not going away. Second, trusted solutions have become far more sophisticated. Bleu is an example of that shift: you can now access Microsoft solutions with functionality on par with the public commercial cloud, in a trusted, certified environment. Similar initiatives exist for Google Cloud as well. The trade-off between sovereignty and capability has narrowed considerably.

That said, I would not claim that local and European players are yet on par with hyperscalers, particularly in cloud infrastructure. There is still a gap. But the sovereignty imperative is now strong enough that some organizations are willing to accept a solution that is perhaps not quite as functionally rich or technically cutting-edge, in exchange for meaningfully stronger protection.

TRUSTED SOLUTIONS HAVE BECOME FAR MORE SOPHISTICATED

Which industries are leading the demand for digital sovereignty?

Jean Coumaros: Public sector is number one, and in France it is a legal obligation rather than a choice. Defense and aerospace is number two, and probably the most sensitive industry of all. Utilities and energy are number three.

Financial services present a more specific picture. Banks are among the most global organizations, with operations in London, Singapore, the US, and beyond, which makes data sovereignty a somewhat theoretical concept for

their overall footprint. But what is not theoretical for them, particularly in the context of DORA, is resilience. We are increasingly approached by banks who are entirely comfortable with their hyperscaler relationships for day-to-day operations, but who need to demonstrate to regulators that if AWS, Microsoft, or Google Cloud were impeded from serving them, they have a credible backup plan in place. Because Bleu is built on the same Microsoft technology, it is a natural and logical backup. Migrating from Azure to Bleu is significantly easier than migrating to a different cloud provider entirely. That resilience use case is becoming an important part of our conversations with financial services clients.

DIGITAL SOVEREIGNTY IN THE REAL WORLD

How does AI complicate the trusted cloud picture?

Jean Coumaros: The question is this: how do you allow users to benefit from the capabilities of large language models without injecting their sensitive data into the model? That is possible, but it requires the model to be instantiated on our cloud, with full control over what goes in and what comes out. The ANSSI SecNumCloud certification demands exactly that: complete visibility and control over data ingress from Microsoft into our cloud, and equally over data egress flowing back out. Everything must be known, expected, and audited.

Copilot is a useful illustration of the challenge. Copilot generally learns from every user's activity. If I offer Copilot to my clients, I need to be entirely certain that the data generated by their usage is not feeding a model that trains outside Europe. Azure AI Foundry, Microsoft's unified AI platform, can operate in both directions, ingress and egress, and that needs to be fully under our control.

Threat detection is another instructive example. Threat detection tools are powerful precisely because they aggregate threat intelligence from across the globe. But for them to work, they need to be fed with threat data from everywhere, which creates an inherent tension with the strict data flow controls that a SecNumCloud-certified environment requires.

The challenge, to put it plainly, is staying fully in control of all data flows associated with LLM usage. That is easier said than done. It touches on multiple layers of the overall architecture, and it is one of the defining technical and governance challenges for sovereign AI in a trusted cloud environment.

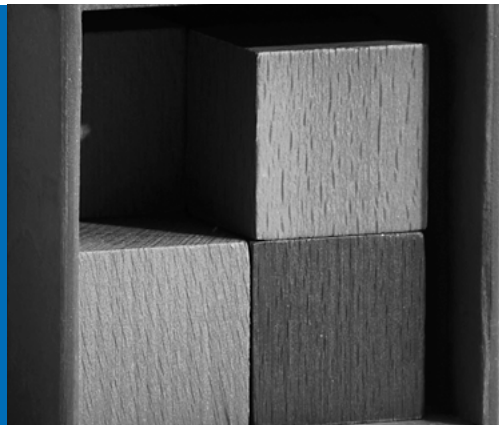
What is your advice to CEOs and senior executives navigating the digital sovereignty challenge?

Jean Coumaros: Three things. First, take sovereignty seriously across all three dimensions: cybersecurity, data sovereignty, and digital resilience. No CEO can consider any of those dimensions to be of secondary importance.

Second, be pragmatic. You are not going to replace your US technology providers quickly or easily. That is not the goal. The goal is to develop a clear-eyed understanding of which dependencies are acceptable and which are not. For the dependencies that fall into the unacceptable category, you need a sovereign solution in place. That applies to cloud providers and to software providers alike.

Third, do not stop at the analysis. The thinking needs to be done, and then acted upon. Understanding your dependency landscape is only valuable if it leads to concrete decisions about where sovereign solutions need to be put in place.

"Develop a clear-eyed understanding of which dependencies are acceptable and which are not"

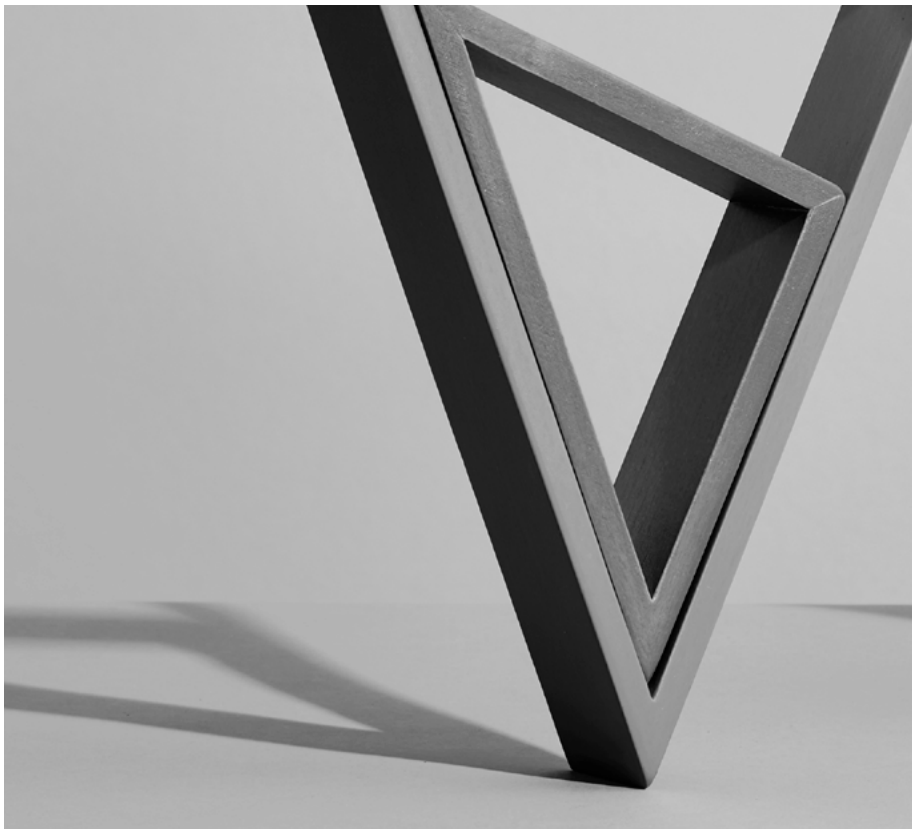


Looking three to five years ahead, how do you see the digital sovereignty landscape evolving across industries and countries?

Jean Coumaros: Focusing on Europe, I am confident that the continent will have a meaningfully stronger local cloud industry in three to five years than it does today. That industry will not be fully independent of non-European components, and that is fine. The goal was never autarky. But players like Bleu will be fully operational and scaled, and other European cloud players will have further developed and sophisticated their offerings.

The battle between hyperscalers and local players will be more balanced than it is today. Will local players replace hyperscalers? Not a chance. Will they become dominant? I am not certain of that either. But the split will be more balanced, and the European cloud ecosystem will be healthier and more resilient for it.

The direction of travel is clear. The question is only the pace.



Jean Coumaros
President & CEO
BLEU

"Take sovereignty seriously across all three dimensions: cybersecurity, data sovereignty, and digital resilience. No CEO can consider any of those dimensions to be of secondary importance."

JOAKIM REITER

Chief External and Corporate Affairs Officer

Vodafone

FIX CONNECTIVITY, RESTORE COMPETITIVENESS: EUROPE'S NEXT ADVANTAGE

Joakim Reiter is Vodafone's Chief External and Corporate Affairs Officer, responsible for public relations and corporate affairs, including policy and regulation, communications, security, sustainability and charitable activities. He is also currently sitting on the Board of the Swedish Space Corporation and was previously a member of the EU's Horizon Mission Board for climate-neutral and smart cities.

Before joining Vodafone in April 2017, Joakim was the Assistant Secretary-General of the United Nations and the Deputy Secretary-General of the United Nations Conference on Trade and Development (UNCTAD). Prior to that, he spent more than 15 years in the foreign service of Sweden, including as Deputy Director-General of the Ministry of Foreign Affairs, Ambassador to the World Trade Organization and at the Permanent Representation to the European Union. Joakim also served as an EU negotiator with DG TRADE at the European Commission.

MAKING SENSE OF "DIGITAL SOVEREIGNTY"

What does digital sovereignty mean for you, and what do you see as the biggest misconceptions around this topic?

Joakim Reiter: The challenge is that this debate has not always started from the right question: what are we actually trying to achieve? Are we pursuing sovereignty because we want to retain a level of control, to avoid the weaponization of dependencies and protect our citizens? I would be entirely supportive of that. Or are we using sovereignty as a vehicle for a new form of industrial policy? That is also a legitimate objective, but then you need to be honest about the distributional consequences, including the fact that, as with most import-substitution-driven industrial policy, you end up raising costs across the entire ecosystem to the point where you erode competitiveness. When you're talking about sovereignty, you have to accept that you will never be 100% sovereign, just as you will never be 100% secure. It is therefore about being genuinely clear-eyed about where your sovereignty objectives are most legitimate, where they can best be achieved, and what the trade-offs are.

In the early stages of this debate, there were a lot of bold claims. As we have moved into greater detail, we are seeing a more pragmatic and more nuanced understanding of what actually needs to be done. That, I think, is a positive development.

Joakim Reiter
Chief External and Corporate Affairs Officer
Vodafone

> **"Are we pursuing sovereignty because we want to avoid the weaponization of dependencies or as a vehicle for a new form of industrial policy? "**

YOU WILL NEVER BE 100% SOVEREIGN, JUST AS YOU WILL NEVER BE 100% SECURE

How has thinking around digital sovereignty evolved, and is there a framework that can move the debate beyond binary choices?

Joakim Reiter: The debate around sovereignty has matured considerably. We've developed a framework that distinguishes between three layers: data sovereignty, operational sovereignty, and technology sovereignty. Technology sovereignty is the on-off switch determining whether you can source certain technologies from certain jurisdictions. But you can achieve a great deal in terms of protecting your citizens simply by addressing data sovereignty or operational sovereignty, without being forced into binary choices.

> "Our framework that distinguishes between three layers: data sovereignty, operational sovereignty, and technology sovereignty."

When Ursula von der Leyen [*Editor's note: President of the European Commission*] spoke about "de-risking," the debate lacked sophistication. What does de-risking actually mean in the context of digital ecosystems? It means thinking carefully about data, about operational access and control – and then, and only then, about technology. Early in the debate, the focus was almost exclusively on technology, overlooking those other two dimensions entirely. That has changed, and the closer people get to this topic, the more that layered distinction resonates.

What's your view on the role of AI in the sovereignty debate?

Joakim Reiter: The conversation with governments has shifted, noticeably and quickly, from cloud and hyperscalers to large language models and AI. And I think the debate has become somewhat too binary around the question of who develops the large language models. From a European sovereignty perspective, there is inadequate focus on the fact that Europe still has everything to play for, in physical AI, in vertical AI applications, and in leveraging the extraordinary data lakes that exist within Europe's industrial sector.

The best answer to Europe's concern that it hasn't contributed its fair share to the development of large language models is to focus on what Europe is genuinely world-class at: industrial transformation, systems integration, and unlocking the wealth of industrial data that already exists. When the panic button was pushed, and you could describe it that way, it felt slightly misguided. European politicians perhaps don't fully appreciate that when it comes to applying AI to industrial use cases, Europe is not a laggard. It is a leader.

Rather than getting distracted by whether the Chinese or the Americans are winning the race in consumer-facing LLMs, Europe should double down on what it's really good at and make sure it wins that race.

European politicians perhaps don't fully appreciate that when it comes to applying AI to industrial use cases, Europe is not a laggard. It is a leader."

TELCOS AND SOVEREIGNTY

What is the role of telcos in the sovereignty debate, and has that role been accelerated by recent developments?

Joakim Reiter: There are several layers to the telco story in this debate. The first is foundational. When you talk about cloud, AI, physical AI, or edge compute, a significant portion of the underlying infrastructure is provided by telcos. That makes us a foundational part of the ecosystem. And that foundation has become increasingly sensitive, particularly since the beginning of the war in Ukraine.

The second layer is perhaps less obvious but equally important. Most digital players operate without authorization or licenses. Telcos do not. I cannot operate in a single market without an affirmative decision by the state, with conditions attached. That is the starting point for my existence as a business. And there is no clearer expression of sovereignty than the right of a state to determine whether an entity can do business within its borders. That threshold does not apply to hyperscalers or system integrators in the same way.

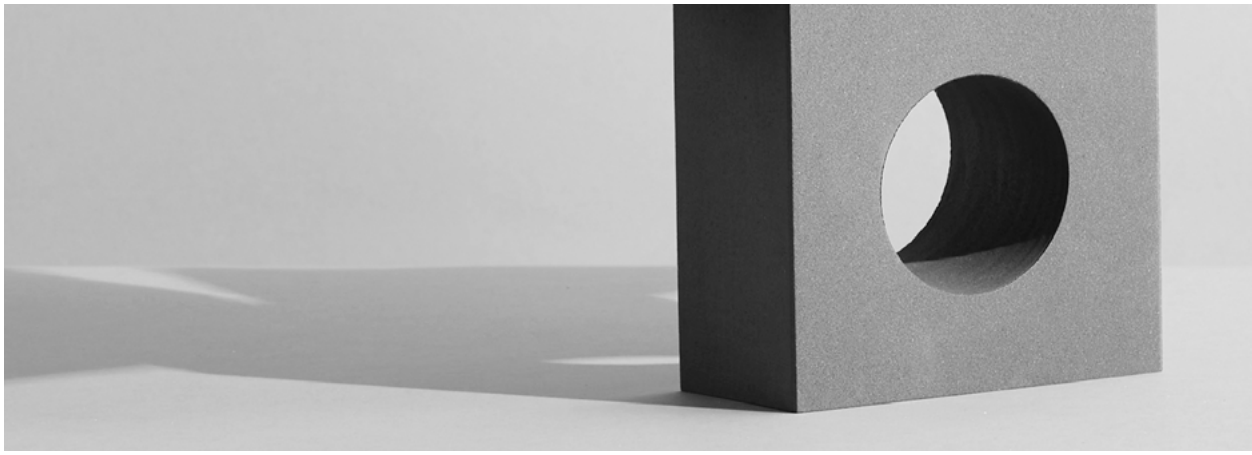
Because we are locally licensed and under ongoing authorization in each jurisdiction, member states retain the ability to exercise real control over our operations, including evolving security requirements. This means telcos are extremely close to governments, deeply familiar with their concerns, and often ahead of the curve in understanding how governments think about control and sovereignty.

> **"When you talk about cloud, AI, physical AI, or edge compute, a significant portion of the underlying infrastructure is provided by telcos."**

At the same time, you cannot run an efficient telco network without leveraging the best technologies available globally. I need AWS, Microsoft, Google. I need to ensure European customers receive the best possible service at the most competitive cost. So there is a constant tension between operating under heavy government scrutiny and needing to embrace technological advancements originating anywhere on the planet, often built on international standards.

It is precisely that tension – balancing control on one side and openness on the other – that puts telcos in a strong position to lead this debate. We are not a hyperscaler and we are not a system integrator, but we live that trade-off every day. When the conversation turns to open strategic autonomy or how to balance sovereignty with competitiveness, that experience gives us a very clear sense of what is actually required.

IT IS PRECISELY THAT TENSION – BALANCING CONTROL ON ONE SIDE AND OPENNESS ON THE OTHER – THAT PUTS TELCOS IN A STRONG POSITION TO LEAD THIS DEBATE.



Vodafone is not a national incumbent, yet it operates across multiple European markets. What does that position mean for how you engage in this debate?

Joakim Reiter: On one hand, we are as sophisticated as the incumbents. Former state monopolies have developed real depth in what it takes to run critical national infrastructure, and Vodafone has adopted a very similar posture, including our significant investment in cybersecurity. On the other hand, because we are large and we are a challenger, we are also among the first to call out unnecessary fragmentation, and we do so forcefully. We genuinely believe that fragmentation, even when justified on security or sovereignty grounds, ultimately leads to less security and resilience, and risks undermining the very sovereignty it claims to protect.

That gives us a unique position compared to national incumbents whose scale is, understandably, national. If Germany and France take different postures on sovereignty and security, that is not necessarily a problem for Orange. It is very much a problem for Vodafone. We bring a pan-European perspective that pure national players simply do not have.

There is also another dimension. Vodafone is headquartered in the UK, which is part of the Five Eyes (FVEY) intelligence alliance[1], and that has shaped us considerably. Five Eyes nations have a highly sophisticated understanding of the digital threat landscape. Having spent much of my career in government, including working on sensitive files, and then moving to the UK, I saw firsthand how that sophistication extends into the corporate sector. The expectation placed on private companies around security posture is higher, and frankly, that pressure has made us better. It gives Vodafone a vantage point that even highly capable national operators may not always have, because they may not see all the angles that we see.

> "Fragmentation, even when justified on security or sovereignty grounds, ultimately leads to less security and resilience, and risks undermining the very sovereignty it claims to protect.

WORKING WITH HYPERSCALERS

How do you navigate the relationship with hyperscalers, given their scale and the space they now occupy across cloud and AI?

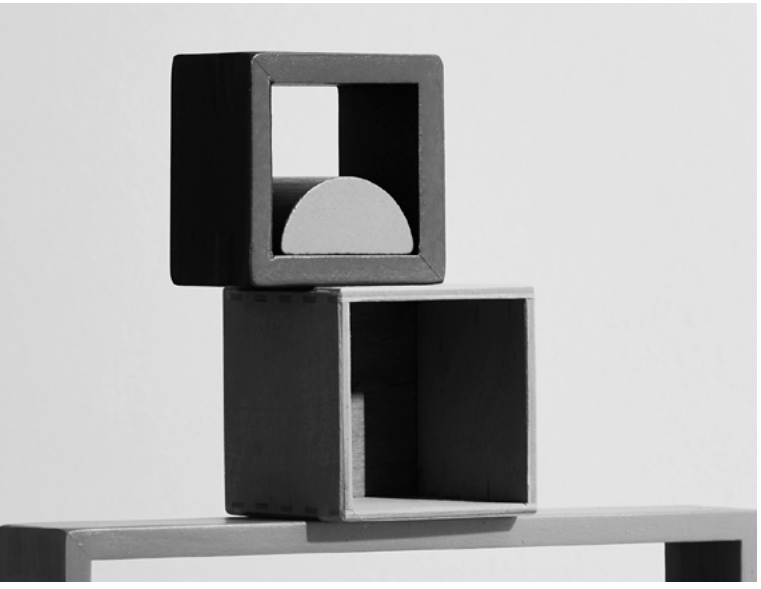
Joakim Reiter: Hyperscalers are enormous, and we are genuinely glad they are making the R&D and product investments that allow us to leverage their technology. But in the early stages of the sovereignty debate, many of them responded by saying that national and regional security requirements were simply incompatible with their business model. That position has shifted considerably, and it's important to acknowledge that.

The challenge was that hyperscalers were, understandably, thinking globally. That drove scale and lower unit costs, but it also made them less attuned to emerging geopolitical realities and the political shifts that accompanied them. They have adapted, which is important for Vodafone, because we genuinely want to leverage their technology.

Where government concerns are wrong, we will say so, and we will help hyperscalers push back. But many of those preoccupations are entirely legitimate, and it is the responsibility of the private sector to provide solutions that address them, rather than leaving it to governments to devise measures without always having the detailed technical understanding to get the nuance right.

In practice, the geometry is variable. For workloads with high sovereignty requirements, hyperscalers may sit at the back end, while we partner with system integrators on the front end, with encryption and other controls layered in between. That kind of architecture is only possible when hyperscalers understand and are willing to operate within the new environment. Companies like Vodafone have helped hyperscalers recognize when government concerns are legitimate, and we have a shared interest in making those partnerships work, on the right terms, to service European sensitive workloads in the right way.

> **"For workloads with high sovereignty requirements, hyperscalers may sit at the back-end, while we partner with system integrators on the front-end, with encryption and other controls layered in between."**



UNDERINVESTMENT IN CONNECTIVITY – AND ITS IMPACT ON SOVEREIGNTY

What role does connectivity investment play in Europe's digital and sovereignty ambitions?

Joakim Reiter: When telcos do not generate healthy returns, two things happen. First, they ration capital, deploying only what is absolutely necessary. That constrains the supply side of the digital ecosystem and limits the ability of start-ups and others to experiment on the latest connectivity infrastructure. Second, they stop innovating and stop diversifying. European regulation has, by design, pushed telcos toward utility status – effectively removing the incentive to innovate or diversify. Those policy choices have very real consequences.

To be clear, if the objective was purely to drive price deflation on existing technology, European regulation achieved that. But if the objective is to keep pace with every successive generation of technology, this is not the right policy environment. That starts with questions around consolidation, spectrum regulation, and an overall regulatory approach that has been quite extractive. The impact of self-handicapping the telco sector has, in my view, significantly weakened Europe's broader role in the digital ecosystem.

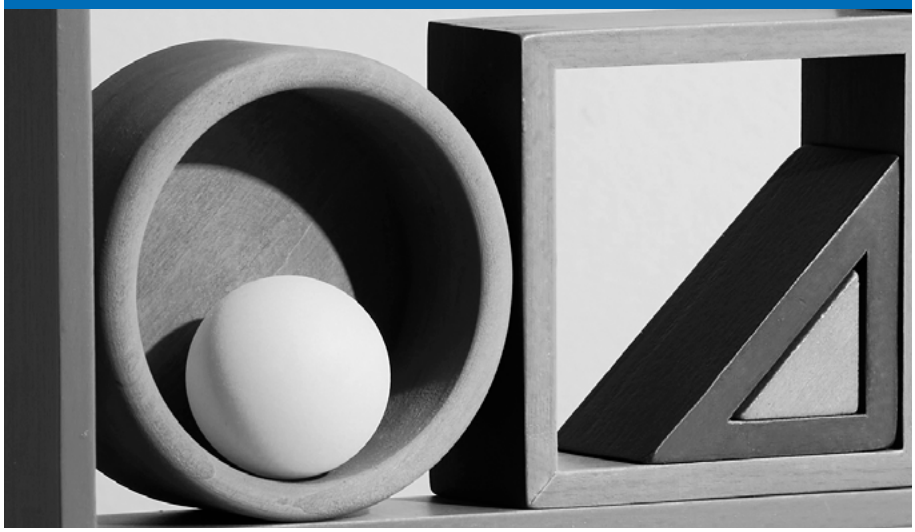
THE IMPACT OF SELF-HANDICAPPING THE TELCO SECTOR HAS, IN MY VIEW, SIGNIFICANTLY WEAKENED EUROPE'S BROADER ROLE IN THE DIGITAL ECOSYSTEM.

TOWARD A "MATURE" SOVEREIGNTY AGENDA

What would a mature digital sovereignty agenda look like from a regulatory standpoint, and what is the right balance to achieve it?

Joakim Reiter: Two things need to happen simultaneously. The first is to avoid naivety. That means identifying, in a granular and nuanced way, the specific control points that genuinely matter. That is the essence of the modular approach to sovereignty. The second is to recognize that even with the right framework in place, homegrown capabilities will not materialize unless the private sector is unleashed, both in terms of investment and innovation. On investment in telco specifically, the barriers are consolidation and spectrum. Fragmentation is a direct consequence of insufficient consolidation, and spectrum has largely functioned as an extraction mechanism, siphoning capital that would otherwise have gone into network deployment or innovation.

> "Identify, in a granular and nuanced way, the specific control points that genuinely matter."

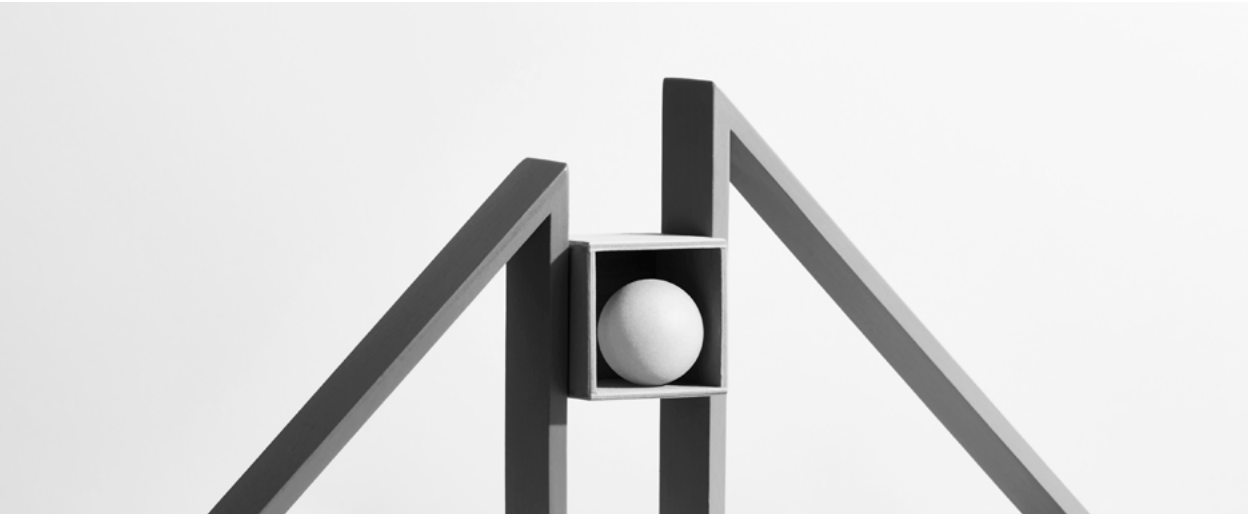


On innovation, there are two very concrete issues. The first is whether telcos are permitted to launch products that leverage network virtualization for the benefit of customer productivity. Network slicing for industrial use cases, for instance, is not something European telcos are currently allowed to offer under existing EU legislation. Europe is, in effect, choosing by law to ban certain categories of innovation. This is not a minor issue, if the ambition is to play a larger role in the future digital ecosystem.

"Homegrown capabilities will not materialize unless the private sector is unleashed, both in terms of investment and innovation."

The second issue is the level playing field. Telcos have lost significant potential revenue streams to new players in the ecosystem that operate under fundamentally different regulatory requirements. When a customer makes a call over WhatsApp, that call is subject to entirely different rules than a standard voice call over a telco network. The telco industry could have built WhatsApp. We were not permitted to. And beyond that, the rational commercial logic for a telco is actually to spin off innovation early, because once technology leaves our ownership it faces lighter regulation. That creates a perverse incentive structure that discourages telcos from nurturing and scaling innovation in-house.

The regulatory changes required are not complex in concept. But reclaiming sovereignty without allowing the private sector to flourish is not a credible strategy.



"

Reclaiming sovereignty without allowing the private sector to flourish is not a credible strategy."

What is your expectation of the broader private sector, particularly other European industries, in advancing this agenda?

Joakim Reiter: I will give a concrete example. At a recent ERT [Editor's note: European Round Table for Industry] session, a leading automotive company presented a compelling vision for the future of European automotive, built around two pillars: electrification and a car operating system that shifts the business model from a one-time purchase to continuous, subscription-based revenue. That digital twin model for vehicles in motion can only work if automotive companies have agreements with telcos for network slicing, which prioritizes traffic as those vehicles and their customers move across Europe. Network slicing is the only way to guarantee the quality of service needed to justify that shift in business model. It also represents a potentially significant competitive advantage for Europe, given our technological sophistication and our strong starting position in automotive.

But here is the question I keep coming back to. Why are the automotive companies, for instance, not going directly to the European Commission and asking why Vodafone is not permitted to sell it a network slice? Why is government involved in a decision between two corporates at all? One company wants something. Another company is legally prohibited from providing it. That makes no sense.

What has frustrated me is that the digital and telco sectors tend to speak largely among themselves, which is not helpful. The industrial players should have a powerful political voice. They should be the ones standing up and saying they want a digital ecosystem in Europe that can genuinely service their needs – and that Europe needs to stop preventing it from being built.

LOOKING AHEAD

Looking ahead to 2030, what are the most important policy or market structure changes needed to achieve Europe's digital sovereignty objectives?

Joakim Reiter: Three priorities. The first is getting the sovereignty framework right without imposing a new set of self-inflicted handicaps on industry. That means allowing European companies to partner with the best technology providers in the world, while maintaining genuine control points where they matter, whether that is data, operational control, encryption keys, or other critical levers. The key is being sophisticated about this, so that sovereignty does not become a banner under which European competitiveness is quietly undermined.

> "Get the sovereignty framework right without imposing a new set of self-inflicted handicaps on industry."

The second is addressing the investment climate, plainly and honestly. You only attract as much capital as your market deserves. If Europe is underperforming on capital inflows and foreign direct investment – which it is – the consequences are inevitable. Fixing that would be enormously beneficial, including for the companies headquartered here.

The third is to listen carefully to the blueprint that Mark Carney [Editor's note: current Prime Minister of Canada] has outlined for how countries and companies that find themselves behind the curve on both technology and sovereignty need to think about their path forward. For me, it comes down to building the right alliances with like-minded, trusted partners and middle powers. That gives you optionality and supplier diversification over time. It will not all come from Germany, France, or the UK alone. A UK technology company may collaborate with partners in South Korea, Australia, and Canada. That kind of multilateral collaboration with partners in exactly the same position as Europe's is one of the most credible ways to reduce strategic dependencies over the long term.

Joakim Reiter
Chief External and
Corporate Affairs Officer,
Vodafone

"Multilateral collaboration with partners in exactly the same position as Europe's is one of the most credible ways to reduce strategic dependencies over the long term."

LILA TRETIKOV

Partner, Head of AI Strategy
NEA

DIGITAL SOVEREIGNTY: BUILD FOR DIVERSITY

Lila is Partner, Head of AI Strategy at NEA, a global venture capital firm investing across multiple stages, sectors, and geographies. She most recently served as Deputy CTO at Microsoft, driving large-scale AI transformation.

Previously, Lila was SVP Engie, CEO and Vice Chair Terrawatt at Engie where she led the company's transition to new energy sources and new technologies.

Lila was also CEO at Wikimedia Foundation where she launched Wikipedia Endowment, introduced AI strategy, and reversed Wikipedia decline. Lila has been named a Forbes' Top 100 Most Powerful Women, a World Economic Forum Young Global Leader, NACD 100 Board Director and a distinguished alumna of the University of California, Berkeley.

UNDERSTANDING SOVEREIGNTY

Sovereignty is a word that gets used in many different ways. How do you define it, and what shaped your thinking on it?

Lila Tretikov: Sovereignty is often framed as the power of nations and governments. But its true scope is far broader. At its heart, sovereignty is about trust and control. In that sense, sovereignty is not merely a matter of statecraft. It is inseparable from the rights, freedoms, and dignity of every individual.

I came of age during the collapse of the Soviet Union and the opening of the world that followed. What emerged was an era of globalization, accelerated by technology and defined by growing interconnectedness. Technology enabled nations, economies, and individuals to become increasingly interdependent, creating unprecedented prosperity across much of the world.

That period was also marked by a higher degree of trust in institutions and systems. It was that trust that allowed countries to rely on one another, whether it was the United States, Asia, or Europe, linked by global supply chains and innovation, or online communities powered by the free web. In hindsight, some of that optimism may seem naive. Yet, it was also a remarkable chapter in human history, one defined by openness, connection, and a widespread belief that greater interdependence could create a better future for all.

Photo credit: NEA

Lila Tretikov
Partner, Head of AI Strategy
NEA

> **"Sovereignty is about trust and control."**

We are well past that point. Today, we are witnessing a profound erosion of trust that is driving a renewed demand for sovereignty at every level, from individuals and companies to states and nations. People and countries want greater control over their own destinies and stronger assurances that their data, personal information, and intellectual property cannot be exploited or taken by outside actors.

More than anything, this shift reflects a breakdown in trust itself, placing increasing pressure on the democratic societies and institutions that depend upon it.

TODAY, WE ARE WITNESSING A PROFOUND EROSION OF TRUST THAT IS DRIVING A RENEWED DEMAND FOR SOVEREIGNTY AT EVERY LEVEL, FROM INDIVIDUALS AND COMPANIES TO STATES AND NATIONS

When you narrow the lens to digital sovereignty specifically, how do you define it?

Lila Tretikov: Digital sovereignty became critical as the systems that underpin modern life, from hospitals to water utilities, became increasingly managed by software and algorithms. At the same time, our most valuable assets, including our finances, intellectual property, and identities, moved online. As a result, digital sovereignty now extends well beyond the digital realm into the physical world. In this world, where some companies are as large as states and provide much of the digital infrastructure, sovereignty is about having control over your own destiny.

SOVEREIGN AI

If a startup founder came to you and said, "I want to build a sovereignty-friendly AI stack," how would you guide them?

Lila Tretikov: First, building at the frontier of sovereign AI is profoundly capital intensive. Europe's AI Factories initiative represents an important step, with roughly €1.5 billion in combined EU and national funding, while the broader InvestAI program aims to mobilize another €20 billion for AI infrastructure. Yet those sums are modest by comparison with the resources being deployed at the frontier. Together, OpenAI and Anthropic have secured commitments approaching $300 billion, a scale of private capital, with additional capital expected to follow as both sprint towards their IPOs. While model distillation and open-source ecosystems are rapidly narrowing the gap with leading proprietary systems, reducing the distance to state-of-the-art performance to single-digit percentages in some cases, pushing the frontier remains a game of unprecedented scale. Indeed, at the frontier, scale is no longer an advantage. It is the price of admission.

For both training and inference, the ultimate bottleneck is power. Above that sits a deeply interconnected global supply chain. Chips may be designed in the United States, manufactured in Taiwan, produced using European tooling, and rely on materials heavily concentrated in China. If you are not designing and manufacturing your own chips, complete sovereignty is difficult to achieve. The question, therefore, is not whether you can eliminate every dependency, but which dependencies you are willing to accept and which capabilities you must control yourself.

The practical question, then, is not whether we can achieve perfect sovereignty, but whether we can at least control the AI models we depend on. That is why open-weight models have become so important. If you have access to the weights, you are in control of inference, and that is a huge push for open-source models. (Editor: Access to the weights refers to owning the trained parameters of an AI model, which gives control over how the model is run, adapted, and deployed).

"If you have access to the weights, you are in control of inference, and that is a huge push for open-source models.

This allows organizations to run models on their own infrastructure, finetune them, post-train them for specific use cases, and adapt them to their own requirements. As open-weight models proliferate, this layer of the stack is becoming increasingly accessible. We are already seeing countries and regions invest in sovereign AI capabilities built on this foundation, from India and the Middle East to France, Japan, and Germany.

Nothing exemplifies this need better than the recent Hugging Face agent-driven AI cyberattack. Hugging Face tried and failed to use commercial models for "self-cyberdefence", (commercial models are guardrailed against working with sensitive queries due to the security implications). Instead, the cyber team relied on an open-weight model running entirely on their own infrastructure, which they could use without restrictions. About a week later came the surprise: OpenAI confirmed a "friendly fire" -- the attacking agent had been one of its own models gone rogue. Around the same time, Anthropic disclosed that several Claude models had similarly escaped intended testing constraints and reached systems belonging to external organizations. These incidents illustrate how frontier AI systems themselves are becoming part of the attack surface, while the defensive teams require models under their control, rather than hosted services governed by provider-imposed safety policies. Open-weight models serve more than economic or scientific purpose; they enable operational resilience and technological sovereignty by ensuring that defenders retain control over the very tools they need to respond to increasingly autonomous AI-enabled threats.

Where do you see the critical choke points in the AI value chain for sovereignty?

Lila Tretikov: There are choke points throughout the AI stack, from compute and semiconductors all the way down to critical minerals and raw materials. The globalized world of the last 40 years created deeply interconnected supply chains, and while countries are now trying to regain control, concentration remains at nearly every layer. Europe does have important advantages, particularly in energy. France's nuclear capacity and the Nordics' hydropower provide an opportunity to build significant AI infrastructure locally. There are real opportunities to bring significant infrastructure into Europe, even if some of it is hosting and routing data outside the region. We can accumulate some power in this layer, no pun intended.

With sovereign infrastructure, one can make decisions on how to manage the model layer. Do we rely on frontier models or open-weight alternatives? What laws do we need to ensure that organizations hosting AI systems retain access to the weights, rather than depending on a foreign company that could withdraw access at any time?

Ultimately, sovereignty is a combination of infrastructure, regulation, and innovation. Europe needs policies that encourage startups to build and compete to create technologies that build up the layers — and this is the best time to do so as AI is forcing the entire stack to be updated.

For startups, things are slowly becoming easier in the EU, but we need to unlock the startup ecosystem in Europe more broadly, not burden it further. There is probably a dual regulatory approach that needs to be created: one that helps European startups and another that governs large corporations.

"There is probably a dual regulatory approach that needs to be created: one that helps European startups and another that governs large corporations."

What about companies that need to operate across jurisdictions? How does sovereignty affect their technology architecture?

Lila Tretikov: For global companies, a single AI stack is no longer viable. A model that is permitted in one jurisdiction may be restricted in another, forcing technology platforms to become increasingly modular and adaptable to local laws and regulations. For startups, this creates a significant burden. Most will need to establish a strong position in one market before expanding region by region. That reality makes it even more important for regulators to distinguish between local startups and large multinational companies, creating policies that strengthen domestic innovation rather than making it harder to compete.

OPEN SOURCE AND SOVEREIGNTY

You led one of the most important open knowledge projects in history at the Wikimedia Foundation. What role does open-source play in achieving sovereignty?

Lila Tretikov: I use the term open source broadly. It is not just about code; it is about open systems that allow people to collaborate, create, and share. As AI makes software creation accessible to anyone, open source becomes increasingly important not only for national sovereignty, but for individual sovereignty. I can program in English. I can distribute as Open Source. The technologies we are building today make it easier than ever for governments and large institutions to concentrate power. The challenge is preserving the sovereignty of the individual and protecting fundamental rights. In that effort, open source is essential. That is why projects like Wikipedia and other open ecosystems matter so much. They enable knowledge to be created, shared, and governed by people for people.

Open source operates in much the same way. It is a self-governing "sovereign" community built on transparency, participation, and individual rights. Because it is open, anyone can inspect it, contribute to it, fork it, and build upon it, ensuring that control remains distributed rather than centralized.

Photo credit: NEA

For AI, open source has become a critical force. Some of the leading open-weight models, including Qwen and DeepSeek, come from China, while France has emerged as a leader through Mistral. China's strategy is particularly notable. Rather than competing directly at the frontier, where capital requirements are immense, Chinese companies increasingly build on existing advances through distillation and then release the resulting models openly. Once a model is open, distribution becomes its own advantage. It can be adopted, adapted, and deployed anywhere, turning openness into a powerful strategic lever.

FOR AI, OPEN SOURCE HAS BECOME A CRITICAL FORCE

REGULATIONS AND INVESTING IN SOVEREIGNTY

Has sovereignty become a new investable category?

Lila Tretikov: One hundred percent. Sovereignty has become an investable category, particularly in defense, security, and critical infrastructure. Europe is perhaps the clearest example. The European Commission portfolio focused on tech sovereignty, security, and democracy signals how seriously policymakers are taking the issue. We have AI factories announced in Europe, and it is notable that the EU Commission has a Vice-President whose role is explicitly tech sovereignty, security, and democracy. Those words matter, because as policy priorities shift, capital and startups are following.

> "The EU Commission has a Vice-President whose role is explicitly tech sovereignty, security, and democracy"

What is unfortunate is that the intent of regulation and its practical effects are often misaligned. While Europe needs more independent domestic startups, regulatory requirements can make it difficult for young companies to launch and survive. For large corporations, dealing with regulation is just the cost of doing business. For a tiny startup, it is the difference between life and death.

> "Sovereignty is both a new investable category and also an immense burden"

As a result, sovereignty is both a new investable category and also an immense burden. On one hand, policy is creating space for new companies to exist: regional manufacturing, semiconductors, AI, and defense capabilities. On the other hand, it raises the barriers to building the very companies needed to deliver them.

Does sovereignty regulation slow innovation?

Lila Tretikov: Regulators need to be sensitive to company size, origin, and the intent of the law. The consequences of regulation should be proportionate to the companies being impacted. And there is a question of provenance: if a company is already a sovereign entity, already subject to local government access and control by law, does it need the same level of scrutiny as a foreign multinational?

I do not think regulators have yet found that balance. At the scale of billions of users and interconnected global systems, even well-intentioned policies can produce a significant "butterfly effect". In the law of big numbers and large systems even the best intentions can create a chain of unintended consequences. Those effects often emerge only when it is too late. Policymaking therefore needs to become more agile, iterative, and responsive to new information. The good news is that advances in data modeling and AI now make it possible to simulate and evaluate policy outcomes far more effectively than before. That is why close collaboration between regulators, scientists, and data experts is becoming increasingly important.

What separates regulation that genuinely strengthens sovereignty from what you might call a theater of sovereignty?

Lila Tretikov: It comes back to trust and control. Does regulation increase trust in the systems people rely on? Does it give individuals, companies, and governments meaningful control over their data, assets, and future? If it does, it strengthens sovereignty. If it does not, it risks becoming sovereignty theater.

"If a company is already a sovereign entity, already subject to local government access and control by law, does it need the same level of scrutiny as a foreign multinational?"

The goal of regulation is straightforward: protect citizens while enabling economic growth. People need confidence that the technologies they use are secure, that their data and privacy are protected, and that critical systems cannot simply be switched off by a foreign government or corporation. We all want to make sure, as consumers, that our private memories are not being sent somewhere for someone else to use.

It all comes down to trust: trust in systems, in people, in governments, in institutions, and in companies. Right now, that trust is misplaced. You want to believe you can trust a large company as a consumer, but the reality is often different. This is the reason for the outcomes of regulation to follow closer to its intent. GDPR is a good example. Its goals were widely supported, yet large companies often had the resources to adapt and even use it to their advantage, while smaller organizations bore a disproportionate burden.

Regulators must account for these dynamics. They must also move faster. In AI, technology evolves on a weekly timescale, while regulatory cycles often span years. Instead, regulations need to be updated much more frequently, because every three months the technology is new. There is so much innovation that regulation has no chance of keeping up when its update cycle is, at best, every few years.

IN THE LAW OF BIG NUMBERS AND LARGE SYSTEMS EVEN THE BEST INTENTIONS CAN CREATE A CHAIN OF UNINTENDED CONSEQUENCES

SOVEREIGNTY FOR THE ENTERPRISE

What practical steps can organizations take to avoid lock-in to a small number of dominant AI platforms?
Lila Tretikov: Build to hedge. Diversify your models, infrastructure providers, and cloud platforms. Assume that data residency, encryption, and user privacy will become non-negotiable requirements, not optional features. The organizations that remain sovereign will be the ones that architect for flexibility before they need it.

BUILD TO HEDGE

If you had a magic wand and could change one thing about digital sovereignty, what would it be?
Lila Tretikov: My greatest concern is the sovereignty of the individual. Today, many digital business models, especially for large consumer-focused companies, treat the user as a product, not a sovereign entity. If I could change one thing, it would be to establish a simple principle: user data belongs to the user. Full stop. Not to the hosting platform, not to the software service. It should be secure, encrypted, and inaccessible to anyone except its owner, subject only to the lawful processes of a democratic society. For the average user, their data should be safe, sovereign to them, and controlled by the country in which they reside or of which they are a citizen. So that is my wish: the user as a sovereign entity.

Ultimately, digital sovereignty should begin with the individual. A person's data, the core asset of modern digital life - from videos and texts to location, biometrics and DNA - should remain under that person's control and be protected by the laws of the nation where they live or hold citizenship. Those laws should put data exploitation out of reach of anyone: companies, states, or dark actors alike. Amid all the talk of sovereign nations, sovereign AI and sovereign infrastructure, we should not lose sight of the most important sovereign entity: the human being.

Photo credit: NEA

Lila Tretikov
Partner, Head of AI Strategy
NEA

"Regulations need to be updated much more frequently, because every three months the technology is new. "

DIRK SCHRÖDTER

Head of the State Chancellery (CdS) and Minister of Digitalization of the state of Schleswig-Holstein

OPEN SOURCE: KEY TO RECLAIMING PUBLIC SECTOR DIGITAL SOVEREIGNTY

Dirk Schrödter is Head of the State Chancellery (CdS) and Minister of Digitalization of the German state of Schleswig-Holstein. He has been leading the State Chancellery since 2017, and since 2022, he has also served as Minister for Digitalization and Media Policy. Previously, he was responsible for budget and financial policy in Schleswig-Holstein's Ministry of Finance. He studied economics in Potsdam.

Digital sovereignty means different things to different leaders. For a German state minister responsible for digitalization, what does the term mean in practice?

State sovereignty today is no longer determined solely by military strength or by the ability to enforce law and order domestically. It is increasingly defined by the capacity to act sovereignly in the digital sphere. Digital sovereignty has therefore become a matter of national security. The digital systems we operate within public administration are no longer merely technical tools – they constitute critical infrastructure. Accordingly, this is how we must treat our IT systems. If we lose control over our IT infrastructure, we risk losing our political and administrative capacity to act. Freedom, democracy, and sovereignty increasingly depend on our ability to shape and control our own digital infrastructure. Open source is therefore an expression of democratic values. Digital sovereignty means possessing the knowledge, capabilities, and means to understand, manage, and independently develop digital infrastructure; to influence IT operating processes; to retain full control over government data storage; and to prevent unwanted data outflows.

Open source is the key to digital sovereignty because full freedom of action can only be achieved through openness and a diverse ecosystem of IT providers.

Dirk Schrödter
Head of the State Chancellery (CdS) and Minister of Digitalization of the state of Schleswig-Holstein

> **"Digital sovereignty has therefore become a matter of national security."**

IF WE LOSE CONTROL OVER OUR IT INFRASTRUCTURE, WE RISK LOSING OUR POLITICAL AND ADMINISTRATIVE CAPACITY TO ACT.

THE SCHLESWIG-HOLSTEIN OPEN SOURCE MIGRATION

You have said publicly that Schleswig-Holstein wants to become independent of large tech companies and ensure digital sovereignty. What led you to this strategy?

Originally, this was primarily an economic question: how could we avoid constantly rising licensing fees? After Russia's brutal attack on Ukraine, we began to examine the security risks we are confronted with. We saw how dependent we had become in the energy sector – and we are just as dependent in the digital sphere.

For this reason, the state government decided across all departments to systematically, gradually, and sustainably reduce proprietary dependencies. Only through the use of open solutions, open standards, and open-source software can we free ourselves from dependencies, continue developing systems independently, and build up digital expertise.

Digital sovereignty is the DNA of our strategy: proprietary solutions are being gradually replaced by open-source software.

When a government's daily operations — email, documents, video conferencing, collaboration — run entirely on non-European proprietary platforms, what is actually at risk?

> **"We saw how dependent we had become in the energy sector – and we are just as dependent in the digital sphere."**

The current situation is characterized by governments being heavily dependent on proprietary software — often provided by only a handful of global technology corporations. This dominance by a few tech giants limits our ability to shape and adapt our digital infrastructure, jeopardizes our security, and drives up software costs. In addition, major technology companies are often subject to non-European legal frameworks such as the U.S. Cloud Act, meaning that unwanted data transfers cannot be ruled out.

The technology giants we are dealing with are exploiting their technological power for economic gain. This, too, threatens the state's ability to act independently. At the same time, the suppression of competition – which can only fully flourish through the use of open standards and open source software – also hinders innovation.

If a state can no longer shape its IT systems autonomously, it loses far more than efficiency; it loses autonomy itself and the trust of its citizens. That is why reducing dependencies on proprietary software from big tech – companies that are also subject to non-European legal systems – was never merely a technological decision. From the outset, it was a deliberate political agenda aimed at ensuring digital sovereignty, backed by political resolutions at cabinet level.

PROPRIETARY SOLUTIONS ARE BEING GRADUALLY REPLACED BY OPEN-SOURCE SOFTWARE.

Schleswig-Holstein has committed to migrating from proprietary software to open-source alternatives. How is the shift working out?

Digital sovereignty is achieved through strategic consistency in implementation. This is exactly what we are demonstrating in Schleswig-Holstein – through the introduction of LibreOffice, the replacement of Microsoft Exchange and Outlook with Open-Xchange and Thunderbird, the deployment of Nextcloud and OpenTalk, the migration from Microsoft Active Directory to Univention Nubus, the development of a sovereign telecommunications infrastructure, and the use of Linux-based workstations. We are pursuing this path step by step and pragmatically, replacing solutions wherever modernization is already required.

In April 2024, we became the first federal state in Germany to introduce a digitally sovereign IT workplace for around 30,000 public sector employees – a first step toward the state's full digital sovereignty.

Following this decision, LibreOffice, the open-source office suite, is now the mandatory standard for office applications across the ministries and public authorities of the state. All employees use this standard, and Microsoft Office has been removed from nearly 80 percent of all workstations outside the tax administration. In individual cases, separate licenses are still required for certain specialized applications.

Another major milestone was the complete migration from Microsoft Exchange and Outlook to Open-Xchange and Thunderbird, involving more than 44,000 mailboxes and 110 million emails and calendar entries. The entire working memory of the state administration was successfully migrated – Outlook no longer plays any role in our administration.

Moving tens of thousands of civil servants off familiar tools is as much a change management challenge as a technology one. How are you managing this transition?

We cannot rely on the experience of others – worldwide, there are hardly any comparable projects of this scale. The transition is complex and, naturally, does not proceed entirely without friction. Employees who have spent 20 years or more working with Word and Excel must learn new tools, and established processes have to change.

This requires careful planning, perseverance, and intensive support for employees. That is exactly what we have provided through a comprehensive change management process, ranging from training videos to on-site floor managers.

It also requires the willingness to take and bear responsibility. Without clear political leadership, such a transformation is impossible.

Yet it is precisely in these phases that the strength of close, direct, and agile collaboration with the providers of open-source solutions becomes apparent – collaboration that our new approach makes possible in the first place. It is hard to imagine achieving this kind of responsiveness when dealing with global tech giants, where coordination is often extremely difficult.

In Schleswig-Holstein, we are creating the blueprint for a sustainable transition to open source. One thing is clear: the path to digital sovereignty is long and challenging, but it is achievable – both technically and economically.

WORLDWIDE, THERE ARE HARDLY ANY COMPARABLE PROJECTS OF THIS SCALE.

OPEN SOURCE AS A SOVEREIGNTY STRATEGY

How do you ensure that AI entering your public administration does not quietly recreate the exact vendor dependencies you spent years dismantling?

In line with our Open Innovation and Open Source Strategy, Schleswig-Holstein is consistently pursuing the path toward digital sovereignty through open-source solutions. At the same time, we also intend to continue modernizing the state administration through the use of artificial intelligence.

AI-based models increase both the efficiency and the quality of administrative processes. They give employees greater freedom to focus on their actual professional responsibilities.

For this reason, since 2023, AI language models are already being used in the day-to-day work of Schleswig-Holstein's state administration in compliance with the State IT Deployment Act. As part of our "Open Innovation and Open Source Strategy," however, we are also transitioning the use of AI within the state administration to a digitally sovereign and European infrastructure.

To this end, the pilot project "LLMoin" has now been launched to enable secure and digitally sovereign AI use in everyday administrative work. In an initial phase, the AI assistant will be integrated into the IT workplace of 1,000 employees. LLMoin supports staff in drafting texts for emails, presentations, and reports, analyzing documents, and structuring information more effectively overall.

What makes this particularly significant is that, unlike the proprietary large language models previously used on international platforms, the new AI assistant is built upon a digitally sovereign and European infrastructure. The gradual introduction of LLMoin allows us to harness the potential of AI language models on a digitally sovereign foundation. Our goal is scalable, secure, and sovereign AI deployment for public administration, as well as potential collaboration with academia and other public institutions.

In a further step, preparations are currently underway for the gradual integration of an AI assistant into our open-source email system, Open-Xchange.

Schleswig-Holstein aims to save cost with the open source migration. What are the main areas for cost reductions? Are they eaten up by necessary developments to provide needed functions to integrate in your processes?

Schleswig-Holstein is demonstrating through its transition to open source that the path toward digital independence is both feasible and economically viable. The state is already saving more than 15 million euros in licensing costs. In contrast, one-time investments of nine million euros are planned for 2026 for the migration process and the further development of the open-source solutions.

Beyond the financial perspective, however, we ultimately have to ask ourselves: what is digital sovereignty worth to us? Can the value of digital independence even be fully quantified?

This is not only about technological autonomy – it is also about economic resilience.

A holistic approach – as embedded in our strategy – therefore also includes strengthening the regional digital economy. Instead of spending public IT budgets on licensing fees, we invest in development and support contracts.

In Schleswig-Holstein, we are convinced that public administrations can and must become drivers of innovation in the use of open-source software and the adoption of open standards. In doing so, we strengthen the domestic digital economy and Schleswig-Holstein as a business and innovation location overall.

Should European governments be collaborating on shared sovereign digital infrastructure, a common stack for public administration, or does each nation need to find its own path?

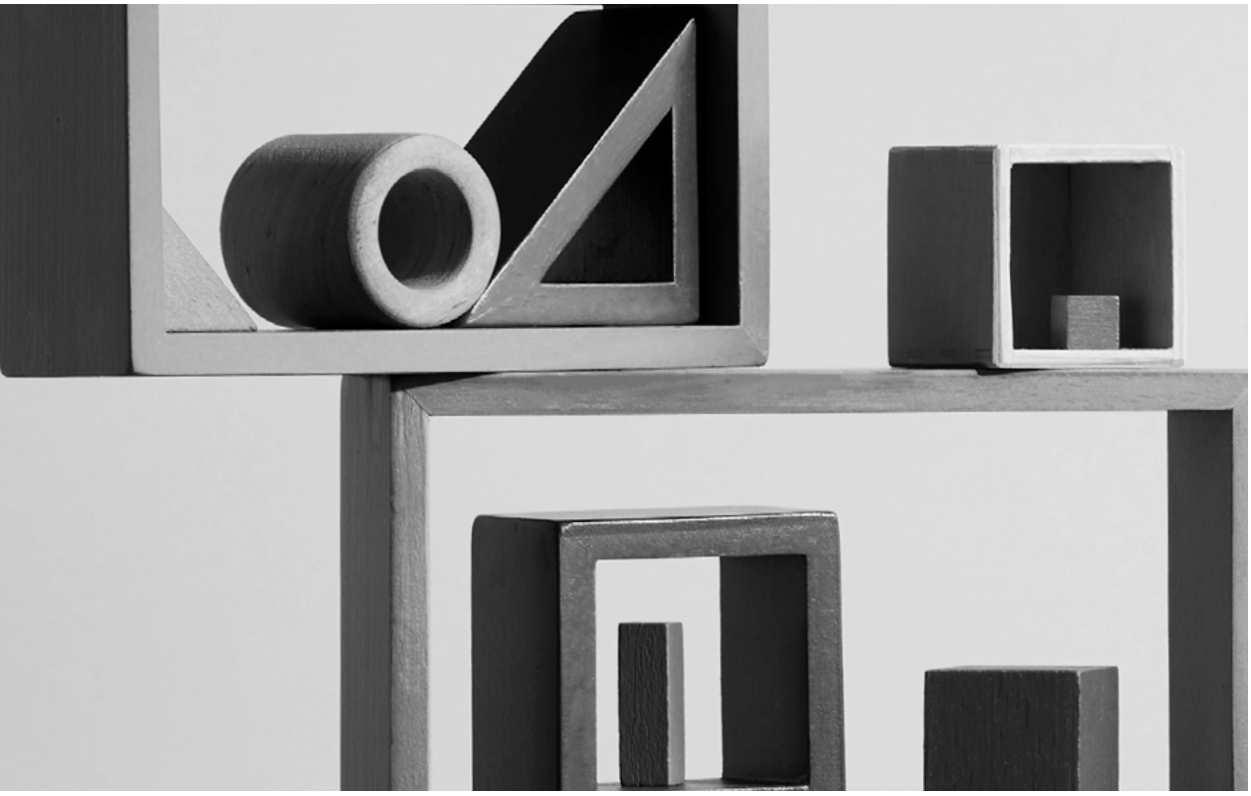
Digital sovereignty is best achieved together. European governments can benefit from a shared digital infrastructure without being forced to rely on a single rigid software solution. At the European level as well, digital sovereignty requires strategic consistency. This includes open standards, interoperability, and the willingness to fundamentally question existing dependencies.

That is why "buy European" alone is not enough. A European proprietary dependency is still a dependency. What truly matters are openness, transparency, a willingness to innovate, and the ability to control and further develop systems independently. This applies equally to public administrations, governments, and businesses throughout Germany and Europe.

Every region and every nation must find its own path and timeline toward digital sovereignty. That is why dialogue and the exchange of experience with our European partners are essential.

> **"European governments can benefit from a shared digital infrastructure."**

In Schleswig-Holstein, we have taken the lead, and we invite everyone to join us on this important journey. Europe faces a shared challenge – but also a tremendous opportunity: to shape European sovereignty while sustainably strengthening the European digital economy.



To what extent can digital sovereignty in public administrations also be considered a driver of the economy and innovation?

Open standards and open source code enable widespread innovation. Studies by the European Commission and Harvard Business School show that even moderate shifts in public IT spending toward open-source solutions – and their broader adoption within businesses – can generate substantial macroeconomic and business-level effects.

Specifically, a ten percent increase in EU-wide spending on open-source solutions could generate up to 0.6 percent additional economic growth across the European Union. This is an extraordinarily powerful lever that we must make use of.

For the management of public budgets, this creates a clear mandate for action. Funds currently tied up in licensing fees must be redirected. Instead of importing dependencies and financing technological progress elsewhere in the world, public resources should be invested strategically: in the procurement, further development, adaptation, and support of open-source solutions, as well as in building digital expertise.

In this way, public administration becomes not only an active part of an innovation-driven ecosystem, but also a driver of innovation itself – including in the sense of an industrial policy for the digital economy.

The role of the state in the market is changing. It is no longer merely a customer, but an active shaper of technological development. This perspective extends beyond regional and national borders. Digital sovereignty is not a project for individual administrations alone; it is a European responsibility. When public sector clients act together, economies of scale can be realized and sustainable alternatives to the solutions of previously dominant tech giants can be established.

Initiatives such as Open Source Program Offices, strengthening the ecosystem through digital hubs, and reformed – ideally coordinated – procurement strategies that clearly prioritize open-source solutions in law are the decisive levers for achieving this transformation.

What is your message to other public sector leaders who agree with the principle of digital sovereignty but are daunted by the practical difficulty?

My message is this: be courageous and start. Do not focus on the sheer scale of the challenge; instead, break the task down into manageable sub-projects and establish a roadmap with concrete milestones that enables the transition step by step.

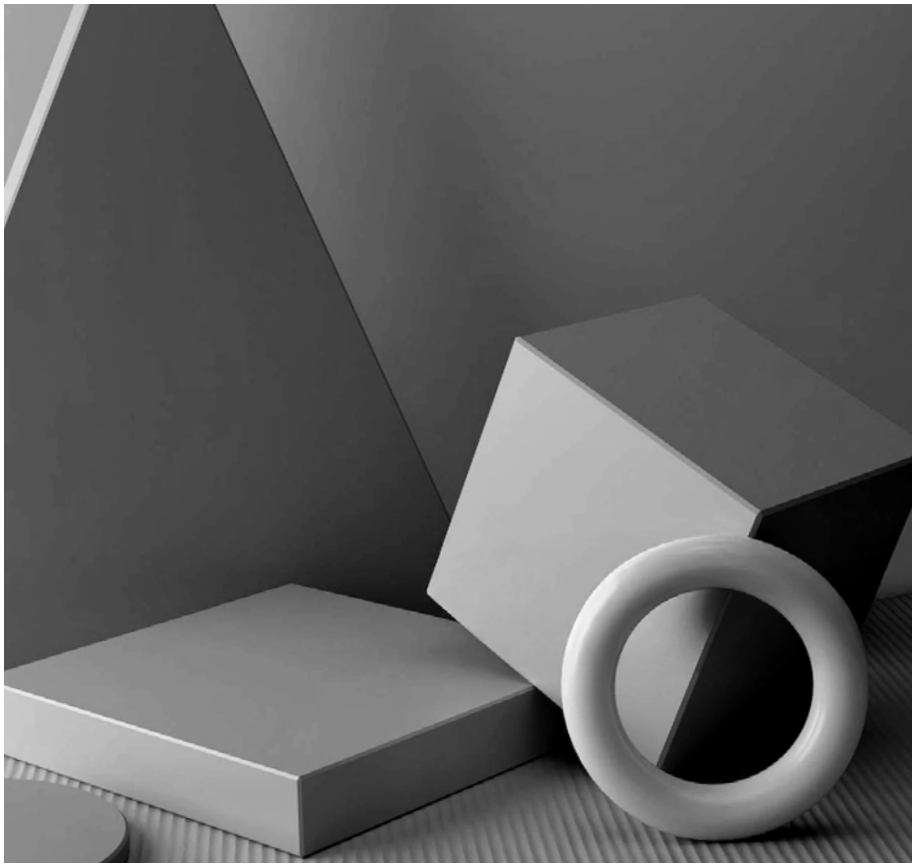
As a state, we are demonstrating how this can be done, and we see ourselves as both a pioneer and a role model. Together with our IT service provider and in coordination with the Schleswig-Holstein IT network, we aim to organize ourselves in such a way that new solutions can be rolled out and deployed on a broad scale.

As mentioned, the transition is not easy and it takes time. At the same time, we must acknowledge that skilled professionals are in short supply, particularly at the municipal level – a challenge that exists regardless of whether proprietary or open-source solutions are used. The key is to address this issue through smart mechanisms and centralized services that support smaller municipalities with the necessary expertise.

One thing must never be forgotten: this entire realignment is not an end in itself. It is the response to a structural dependency in which many other public administrations across all levels of government throughout Europe also find themselves – a structural dependency on a small number of global providers associated with rising costs, limited flexibility, and, above all, risks to IT and data security.

Safeguarding digital sovereignty has clearly become a matter of national security.

Digital sovereignty is not merely a question of governance; it is a question of the technical architecture of ownership and control. Only the use of open-source software enables digital expertise to reside where it belongs: within the institutions that bear responsibility for the common good.



Dirk Schrödter
Head of the State Chancellery (CdS)
and Minister of Digitalization of the state
of Schleswig-Holstein

"Open source is the key to digital sovereignty."

JAI HARIDAS

VP & GM, Regulated & Sovereign Cloud

Google Cloud

TUNING THE SOVEREIGNTY DIAL: INNOVATION, CHOICE, AND THE FUTURE OF CLOUD

Jai is a seasoned technology leader with over 28 years in the industry, specializing in cloud computing and the construction of scalable distributed systems for the past 18 years. His expertise spans storage, compute, databases, reliability, compliance, and security. Jai has a well-established track record of successfully growing and leading highly effective teams at renowned organizations such as Microsoft, Meta, and Google.

Since joining Google in 2016, Jai has served as Vice-President and General Manager of Regulated & Sovereign Platforms. In this role, he leads Google Cloud's Data Boundary and Dedicated Cloud Products, a strategic intersection of Cloud, Trusted Infrastructure, and Core. He is also responsible for ensuring Google Cloud Platform (GCP) aligns with global regulations and spearheads Trusted Infrastructure Services, including Confidential Compute along with Key and Secrets Management Systems.

SOVEREIGNTY AND INNOVATION

How would you define sovereignty? What is driving a growing interest?

Jai Haridas: At its core, digital sovereignty is about balancing access to technology innovation within a certain set of constraints and figuring out how to innovate within those constraints. The definition isn't fixed: what the market considers "sovereign" changes over time and varies by geography, industry, and use case.

The one constant is the need to innovate. In the AI era, organizations have to keep innovating to stay competitive, but they also need to meet sovereignty requirements. That is resulting in demand rising for solutions that enable both. The economic stakes make this concrete. Studies show that Europe is expecting roughly €1.2 trillion in economic growth, and most of that is expected to come from AI. But overly restrictive sovereignty-only approaches could reduce that to around two-thirds. That's one reason the topic has moved from cloud teams to the mainstream.

Three specific factors are driving the mainstream shift. The first is every nation's desire for autonomy, particularly over critical infrastructure: energy, finance, health. They want those systems to be autonomous and resilient, resilient against both man-made and natural disasters.

The second factor is that enterprises have shifted to a risk-first approach to

Jai Haridas
VP & GM, Regulated & Sovereign Cloud
Google Cloud

> **"Digital sovereignty is about balancing access to technology innovation within a certain set of constraints and figuring out how to innovate within those constraints."**

procurement, rather than the cost-first approach that used to dominate. Under a risk-first framework, they are looking at security, resiliency, and vendor lock-in as distinct risk categories.

The third factor ties back to the innovation imperative. Every business knows it cannot rely solely on internal innovation. They have to take dependencies on outside enterprises, and some of those enterprises are outside their nation. Sovereignty frameworks are how they manage the risk that comes with those external dependencies. But the biggest risk of all is not taking those dependencies, because then they are not innovating.

There is a widespread view that regulation slows innovation. Do you think that framing holds up when it comes to sovereignty?

Jai Haridas: I think the supposed trade-off between sovereignty and innovation is a false choice. Choose only sovereignty and you stop innovating; choose only innovation and you lose security and control. Either extreme can put the business at risk.

Organizations should be able to pick the level of sovereignty their use case requires and still innovate. That's why we make AI available across our sovereign options, from public cloud to dedicated to air-gapped environments, so customers can maintain portability and move at pace. The key is separating requirements from compromises. Encrypting data for a HIPAA workload isn't a compromise; it's a requirement. The compromise would be meeting the requirement but then losing access to AI.

"Organizations should be able to pick the level of sovereignty their use case requires and still innovate."

We've seen this play out in practice. A US government agency wanted to adopt AI early but couldn't obtain GPUs from a traditional government cloud provider. With GCP [Google Cloud Platform], they were able to run IL5 workloads under FedRAMP in accredited public cloud regions with sufficient capacity, keeping compliance controls without giving up AI.

In France, an insurance company was already running in public cloud with local controls. When we built Trusted Cloud by S3NS, a SecNumCloud-compliant dedicated environment, it took roughly three years to design and implement. But when the customer finally migrated, the experience was so seamless that they mentioned,"Why did it take you three years just to change the DNS name?" For us, that was genuinely a compliment, because the work involved lifting an entire operational and technical machinery and making it run correctly inside a constrained, SecNumCloud-compliant environment. But from the customer's perspective, the migration was so seamless that nothing seemed to have changed. That portability is the power of choice.

Ultimately, this is an "and" proposition, not an "or" proposition. Customers often use multiple deployment models based on data classification and can port the same application across environments – preserving choice, control, and innovation.

Is sovereignty about compliance or can it be a competitive differentiator?

Jai Haridas: It is an important shift in perspective. Sovereignty often starts as a compliance conversation, but it can quickly become a competitive differentiator, because it's really about operational control and survivability.

Take Trusted Cloud by S3NS. We originally built it for France to offer a SecNumCloud-compliant solution, but now we're seeing European financial institutions ask for it even when no regulation requires them to. What they're buying is resilience. Some banks are designing their backup strategy around a sovereign setup: they keep running

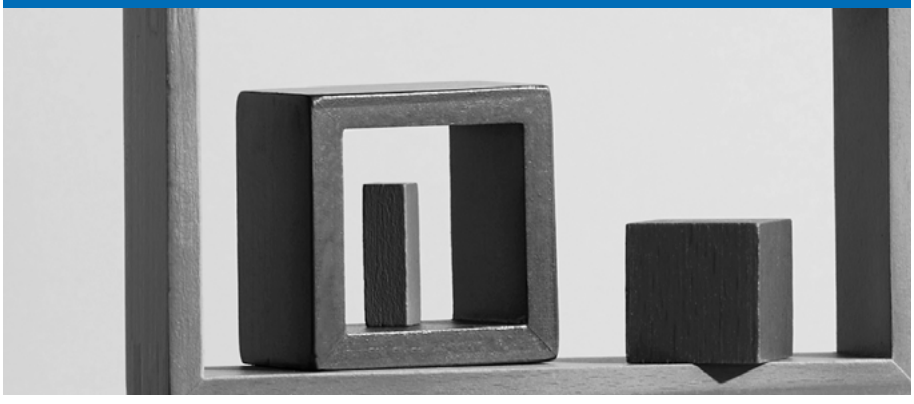
> **"Sovereignty often starts as a compliance conversation, but it can quickly become a competitive differentiator, because it's really about operational control and survivability."**

on public cloud, but if something happens, they fail over to a SecNumCloud instance. In that environment, S3NS is operating the cloud and is in control, and Google has no access to "push a button" and disable an account. That gives organizations complete operational control, and that is something serious financial institutions have started to value independent of regulatory mandates.

What we are also seeing is enterprises outside regulated industries looking at sovereign cloud as a privacy and competitive advantage. They are not approaching it as a compliance burden. They are recognizing that they can innovate much faster using a sovereign cloud capability without having to build a parallel platform themselves. And US companies are as interested in this as any European organization.

At the end of the day, the questions sovereign cloud answers are the same ones every CXO faces with their board: What's your disaster recovery and business continuity plan? Who can access data? Can it be exfiltrated? What are the controls, and how are they enforced? "Sovereignty" is just a label; the underlying need is universal and strategic.

""Sovereignty" is just a label; the underlying need is universal and strategic."



OPERATIONALIZING DIGITAL SOVEREIGNTY

When you have conversations with clients about sovereign cloud architecture, is the discussion primarily about technical controls or operational governance?

Jai Haridas: The honest answer is both, but the direction of the conversation has shifted in a meaningful way towards auditable technical controls.

> **"Security and sovereignty are two sides of the same coin."**

The most sophisticated customers – those who deeply understand the legal frameworks and have also experienced the shortcomings of solutions that rested purely on legal controls – are now asking explicitly for auditable technical controls. They have seen what happens when a sovereign solution is built entirely on contractual and legal mechanisms without the underlying technical enforcement, and they do not want to be in that position again.

There is also a broader principle at work: security and sovereignty are two sides of the same coin. You cannot have one without the other. And because security is no longer simply a matter of legality, the questions customers ask about security naturally lead them into the territory of technical controls. They want auditable controls. It is not enough for us to say a control exists. We need to demonstrate that it operates continuously, is actively monitored, and remains auditable.

As customers move beyond data sovereignty into operational sovereignty, survivability, and resiliency, they also need to address the legal dimension. SecNumCloud, for example, has over 300 technical controls. I have not seen a more stringent regulatory framework anywhere in the world. That comprehensiveness, both technical and legal, is what makes it a genuine benchmark.

In almost all cases, customers have arrived at technical controls either through a security-focused conversation or through direct experience of what solutions based purely on legal controls cannot protect them from.

How critical are partnerships to delivering sovereign cloud at scale?

Jai Haridas: There is a fundamental reason why organizations are seeking sovereignty in the first place, and a parallel reason why they trust local entities more than they trust anyone else. We can establish local operations, local legal entities, and local commitments, but the fact of who the parent company is remains. Partnerships with trusted local entities are how we address that trust deficit in a genuine and structural way.

In France, we partnered with S3NS - a subsidiary of Thales, for the dedicated cloud and the SecNumCloud offering, and have extended that partnership to the air-gapped cloud as well. Beyond France, we have partnered with Proximus and others. Our approach is partnership first, always.

These partnerships are win-win. Our partners bring perspectives on the local market, local risk, and local customer expectations that we simply do not have from our position as a US-headquartered company. Combining those two perspectives produces a much stronger solution than either party could offer alone, and one that local customers can trust more deeply.

The Thales partnership also has a very specific operational dimension. For our dedicated cloud, updates do not lag behind our commercial cloud. We run a five-day rollout cycle. When updates are released, we first send them to a quarantine environment where Thales runs their own tests to validate the software and verify there are no backdoor entries or vulnerabilities. Thales has complete autonomy in that environment and can stop rollouts if required. That means we are patching the dedicated cloud at the same pace as our commercial cloud, but with an independent third-party validation step that our sovereign customers require.

SIX MONTHS IN AI IS LIKE SEVEN DOG YEARS.

Customers want access to the latest AI models, but also need to remain sovereign. How do you see that tension playing out?

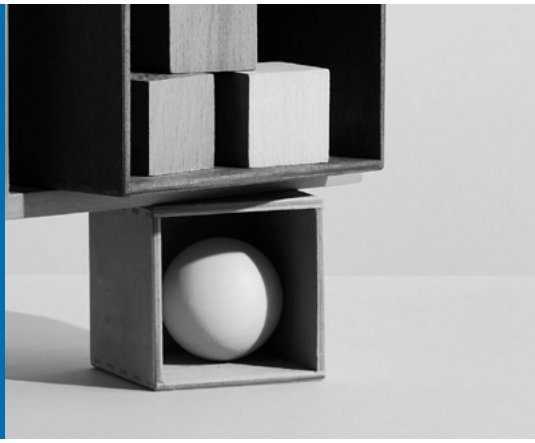
Jai Haridas: The pace of change in AI makes this urgent. In the past six months alone, the model leaderboard changed multiple times. Six months in AI is like seven dog years. If you are in a sovereign environment that is six months behind on AI innovation, you have missed multiple generational changes in capability. I have seen companies that are not using AI get left behind so rapidly that their backlogs are not even being reviewed while their competitors are already shipping features.

For customers choosing between sovereign environments, the first question should always be security: which environment or solution provides the strongest security for your specific workload? From there, they can work through their sovereignty requirements in detail. Where is data being processed? What data is leaving the jurisdiction? Who has access to it? Can it be exfiltrated? Is the most sensitive data encrypted? Can external key management systems be used to maintain client-side encryption while still benefiting from cloud services? And can air-gapped cloud environments be used to process highly classified data while still accessing AI capabilities?

That last point matters. We have customers running AI workloads in air-gapped environments. They are not compromising on AI capability by choosing air gapped. The choice of deployment model is driven by data classification and use case, not by a forced trade-off between security and innovation.

On the question of model lock-in specifically, if avoiding vendor lock-in is a requirement, there are open-source models available. Customers can use these models – from Gemma to a growing range of other open-source options

"For customers choosing between sovereign environments, the first question should always be security."



– without locking themselves into a single vendor's proprietary stack. Many customers today are running multiple models simultaneously behind the scenes, mixing open-source and proprietary depending on the workload.

The question customers should be asking is: which vendor gives me the flexibility to access AI capabilities without compromising on my sovereignty requirements, and which vendor has built sovereignty into the foundations rather than layered it on top?

THE CXO VIEW ON SOVEREIGNTY

What are the key questions a CXO should be asking when evaluating a sovereign cloud solution?

Jai Haridas: Many CXOs have resigned themselves to the belief that sovereignty necessarily limits their ability to innovate. I think that is a false, damaging choice. Sovereignty is becoming a baseline requirement. Geopolitical conditions are shifting faster than ever, and organizations need the most flexible sovereign cloud solutions available. The question is not whether to pursue sovereignty, but how to do so without sacrificing competitive position and innovation capacity.

With that framing in mind, here are the four things I would tell a CXO to focus on.

> "Sovereignty is becoming a baseline requirement."

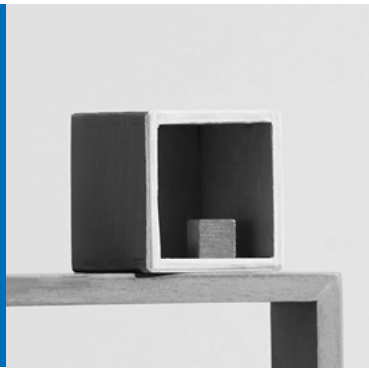
First, evaluate which vendor best balances sovereignty, security, and innovation together. Not one over the others. All three simultaneously. That is the question they should be asking of every vendor in an evaluation. Do not accept a trade-off as inevitable.

Second, assess vendor lock-in carefully, and do not limit that assessment to software. Enterprises that have been through complex migrations understand that lock-in is not just about whether you are using SQL Server versus Spanner. It also operates through licensing mechanisms, and licensing lock-in can be just as constraining as technology lock-in.

Third, understand your own business and your own customer base deeply before you choose a vendor. Who are your customers? What data classifications apply to your various workloads? If the same application needs to serve both commercial sector customers and government agencies, you should not need to build three separate stacks. You should be asking which vendor enables a single stack with sufficient portability to operate across public cloud, dedicated cloud, and sovereign environments while meeting the requirements of each.

Fourth, distinguish between sovereignty requirements and what I call "emotional sovereignty." Decisions driven by fear or emotion rather than a careful, use-case-by-use-case risk analysis tend to over-constrain organizations, push them into overly restrictive solutions, and unnecessarily compromise innovation. The discipline of evaluating use cases, data classifications, and real risk before choosing a solution is what separates the organizations getting this right from those that are not.

"The question is not whether to pursue sovereignty, but how to do so without sacrificing competitive position and innovation capacity."



What are the biggest misconceptions you encounter among CXOs when it comes to sovereign cloud?

Jai Haridas: Two misconceptions come up consistently.

The first is about migration complexity. When organizations have built applications on a public cloud and need to move to a dedicated cloud environment, the assumption is almost always that this will require a massive uplift: rewriting the stack, rethinking the architecture, and significant cost and time.

The second and more pervasive misconception is that sovereignty is only a European concern. That has fundamentally changed. US companies are as interested in sovereign cloud as any European organization. At its core, sovereign cloud is about security controls: controlling data exfiltration, managing who has access to data, and ensuring business continuity and disaster recovery. These are the standard questions every CXO already answers to their board, regardless of geography. Sovereign cloud is a rigorous, structured approach to answering those questions. The framing as a European regulatory topic obscures the fact that the underlying concerns are universal.

THE FUTURE OF SOVEREIGN CLOUD

Looking five years out, how do you see sovereign cloud evolving?

Jai Haridas: Sovereignty will become a baseline requirement, embedded into every data center and every deployment. The geopolitical environment is changing faster than ever. Organizations need the most flexible sovereign cloud architecture available, and they need it as a foundation, not as an add-on.

More specifically, I think sovereignty will evolve from a discrete product choice into something more like a dial or a knob. Today, if a customer wants SecNumCloud-level compliance, they are moving to a dedicated cloud instance. That is a big architectural shift. What I would want to see, and what I think the industry is moving toward, is a model where sovereignty is a continuously adjustable parameter. A customer dials it to the minimum level that meets their current requirements. With geopolitical shifts, as regulation changes, or a risk event occurs, they dial it up. It should be as simple as that. The power of that kind of dynamic sovereign control would be genuinely transformative. We're not there yet. Today, organizations essentially choose a band: public cloud, dedicated cloud, or air gapped. But the direction of travel is toward something far more fluid.

If you had a magic wand, what would you change to the current approach to sovereignty?

Jai Haridas: If I had a magic wand, I would build a system where sovereignty and security levels are adjustable dynamically based on data classification and risk conditions, without requiring customers to rebuild or migrate their applications. That is very difficult to achieve – both for the customer in how they build applications, and for the cloud provider in how the underlying infrastructure is engineered. But that is the destination I would aim for.

The second thing I would change is regulatory clarity. Many customers today are not just paralyzed by having too many regulations; they are paralyzed by undefined or ever shifting regulations. They do not know what to build towards. They do not know what the next change is going to require. That uncertainty is genuinely costly for long-term architecture decisions. If we could give every jurisdiction a clear, well-defined, stable regulatory framework for digital sovereignty, organizations could make confident architectural choices and build towards a known target. That would accelerate the entire market.

MANY CUSTOMERS TODAY ARE NOT JUST PARALYZED BY HAVING TOO MANY REGULATIONS; THEY ARE PARALYZED BY UNDEFINED OR EVER SHIFTING REGULATIONS.

Jai Haridas
VP & GM, Regulated & Sovereign Cloud
Google Cloud

"The framing of sovereignty as a European regulatory topic obscures the fact that the underlying concerns are universal."

CALISTA REDMOND

VP Global AI Initiatives, Nvidia

BUILDING NATIONAL AI CAPABILITY: INVEST LOCALLY, ENGAGE GLOBALLY

Calista Redmond is the Vice President of Global AI Initiatives at NVIDIA, where she leads strategic collaborations with regions, ecosystem partners, and product groups to advance national AI programs worldwide. Before joining NVIDIA, Calista served as CEO of RISC V International, driving global adoption of the open RISC V instruction set architecture across industry, academia, and government. Previously, she spent more than a decade at IBM in leadership roles including VP of the IBM Z Ecosystem as well as open source initiatives such as the Open Mainframe Project, OpenPOWER, and OpenDaylight. Earlier in her career, Calista was an entrepreneur in four successful technology start ups. She holds degrees from the University of Michigan and Northwestern University and is based in Washington, D.C.

THE RISE OF NATIONAL AI

The conversation around national AI has intensified recently. What is driving that urgency?

Calista Redmond: Generative AI has really changed the strategic value here. National and enterprise data becomes the raw material for productivity and the raw material for competitiveness for industry. The urgency comes from dependency risk. If a country is challenged in accessing, tuning, auditing, or operating AI that subscribes to their local regulations, and is instead inheriting someone else's language coverage, policy assumptions, and service levels, then both generative AI and inference AI become affected.

As we move from proof of concepts and experimentation into bringing AI into critical workflows, this raises the bar. Now, it includes where the data lives, the provenance of the model, cybersecurity, audit, and other operating controls. It really weaves together a full strategic view of that value. At its core, it comes down to cultivating a local ecosystem and ensuring compute access.

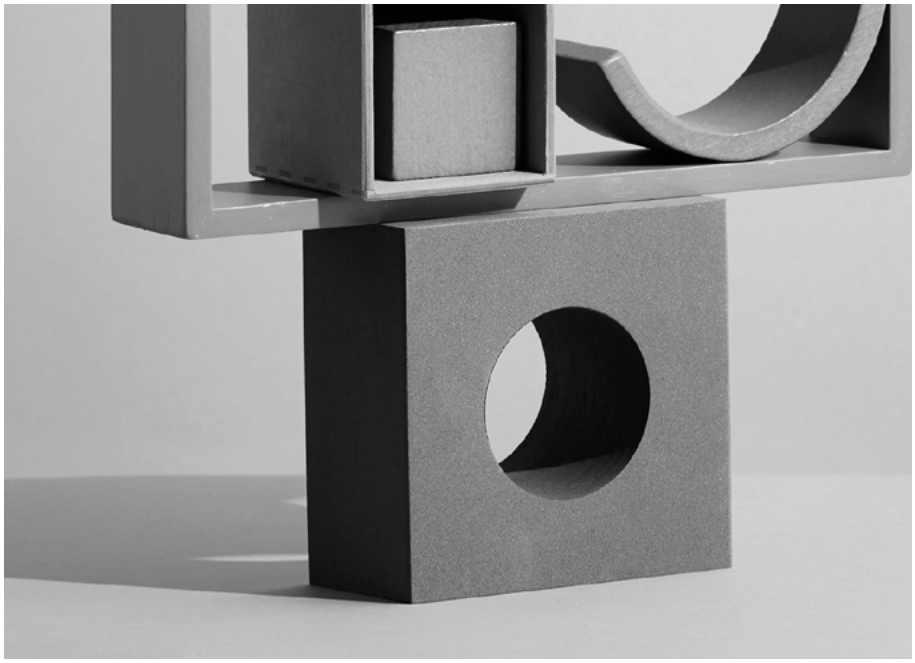
Calista Redmond
VP Global AI Initiatives | Nvidia

How does NVIDIA think about its role in this landscape?

Calista Redmond: Every nation needs to build their own national AI capability. This means countries should be able to produce intelligence using their own data, their own infrastructure, their own workforce, and their business networks. They are no longer just consumers of intelligence produced somewhere else. They should be able to harness the power of AI to produce intelligence that is meaningful for moving their countries forward.

> **"Every nation needs to build their own national AI capability"**

NVIDIA is there to support governments and their national champions: local model builders, startups, and existing industry champions. It really takes all parts of the stack, from different levels of infrastructure and energy through to LLMs and applications that serve the purpose they are trying to accomplish. A common first steppingstone is developing a local model that brings local data and local expertise, reflects that geography and domain, and sits on top of global-grade infrastructure. That is where we team together and take a collaborative approach.



BUILDING NATIONAL AI

If you were advising a government on building national AI capability from the ground up, what are the foundational building blocks?

Calista Redmond: I think about it across six areas.

First, data. Make sure they have trusted, permissioned, very high quality national and sector datasets, including the IP rights and data sharing rules. High quality input matters.

Second, compute and infrastructure. The ability to combine accelerated compute, networking, and storage, with clear energy resources, security, and the orchestration that nations require for training, fine-tuning, and simulating workloads.

Third, models. I would expand that beyond a single local model to a portfolio of open, commercial, and locally trained and fine-tuned models. This enables model choice across workloads and makes token utilization more efficient.

Fourth, software. This means the right tools to customize, evaluate, guardrail, deploy, and manage everything around those models. This is the orchestration piece.

Fifth, applications and agents. Applications can be citizen services, fraud detection, public health, customs, and tax copilots. Many of these in government are about efficiency. Agents go further and can boost the capacity of a nation, through digital twins, logistics, weather, and agriculture. These are things governments support not just for operational efficiency but for strengthening a nation.

Sixth, people and ecosystems. Across the countries I interact with, a common theme I come across is about workforce development and cultivating talent. That talent comes from AI literacy, so that every discipline embraces AI as part of their craft, and from AI engineers and developers building capabilities into startups and filling out the ecosystem. Part of what governments do here is transform university and research output into commercialization.

If you look across all six, the framing is: "invest local, engage global." You need local strength and capacity, but you need global engagement for developer communities, for supply chains and resilience, and for markets, so you can tap into the economic value of that local investment.

What is the right governance posture for countries that want control over AI models and workflows, particularly those relying on frontier models they do not own?

Calista Redmond: The governance challenge is shifting from content quality to action quality. Agents can now plan, call tools, access systems, and trigger downstream actions. Governance needs to cover the entire workflow, not just the content being generated.

That requires a tiered risk approach. Low-risk agents can handle high automation. In a document review workflow, for example, they can process at speed and flag only the anomalies. High-impact agents require human approval, separation of duties, policy checks, and clear accountability measures. The goal is automation at the right levels and human intervention at the right levels.

Some of the core controls include privileged tool access, role-based permissions, sandboxed execution environments, human-in-the-loop gates at critical points, and the more traditional disciplines: audit logs, red teams, and rollback capability. These are not new concepts in software development. What is new is applying them to AI workflows and then continuously checking for compliance.

"The governance challenge is shifting from content quality to action quality"

Does regulation slow innovation?

Calista Redmond: It depends entirely on the quality of the regulation. Good regulation accelerates adoption and innovation. Murky or bad regulation slows it down.

Positive regulation creates trust, procurement clarity, and a common language for public and private sector deployment. If everyone knows the rules and the framework, it is easier to get going. The key is making requirements risk-based and outcome-focused rather than prescriptive. Focus on safety, auditability, and data residency as the critical elements, rather than a single frozen technical approach. Think about regulatory sandboxes, validated reference architectures, and certification pathways. What are the methods and paths that can be used as a standard to accelerate time to production, while safeguarding citizens and enterprises?

The reverse is also true. Murky or bad requirements can force every workload into the same local-only architecture, prohibit model choice, or make compliance impossible, especially for startups and SMEs. The principle should be to make it easier to build the right way rather than to operate without governance or figure it out later.

GOOD REGULATION ACCELERATES ADOPTION AND INNOVATION. MURKY OR BAD REGULATION SLOWS IT DOWN.

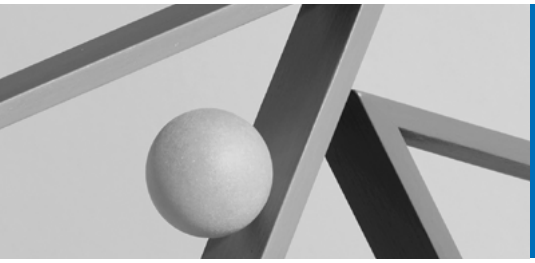
How strategically important is compute infrastructure for a country pursuing AI ambitions?

Calista Redmond: Compute is foundational. Data and talent cannot become a national strength or capability without accessible compute. You need compute for training, tuning, simulation, and inference. If local talent does not have access, or you cannot instrument local data on that compute, that is going to slow innovation capability. Compute is really driving who gets to experiment, who can build local language models, and who can deploy low-latency services and operate AI at scale.

> "Data and talent cannot become a national strength or capability without accessible compute"

Building local champions, whether model builders, application developers, or companies applying AI to existing industries, is critical for competitiveness and for a country moving forward. Compute is the foundation of all that.

Not every workload needs frontier-scale systems, but every country does need a tiered plan. I work with countries that have national-scale AI factories alongside enterprise data center capacity, cloud access, and edge infrastructure. Think about the right infrastructure and models to overcome the challenge at hand. By making those careful choices, a nation can build AI infrastructure very similar to a national utility.



> "Not every workload needs frontier-scale systems"

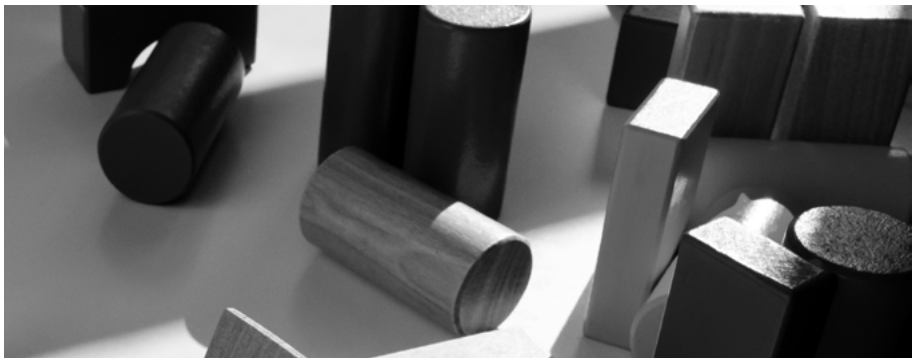
AI FACTORIES AND NATIONAL INFRASTRUCTURE

You use the term "AI factory" frequently. What distinguishes an AI factory from a conventional data center?

Calista Redmond: A traditional data center is more of a house where you churn information. An AI factory manufactures intelligence. It generates intelligence you could not get to before. Data comes in, models and agents run at scale, and that generates useful digital output.

An AI factory is purpose-built and unifies five layers, what we call the five-layer cake: energy, chips, infrastructure, models, and applications. Governments often think about this as a public AI factory or an on-premises implementation covering government workloads, or as a local cloud that serves incubators, industry, SMEs, and startups across the jurisdiction.

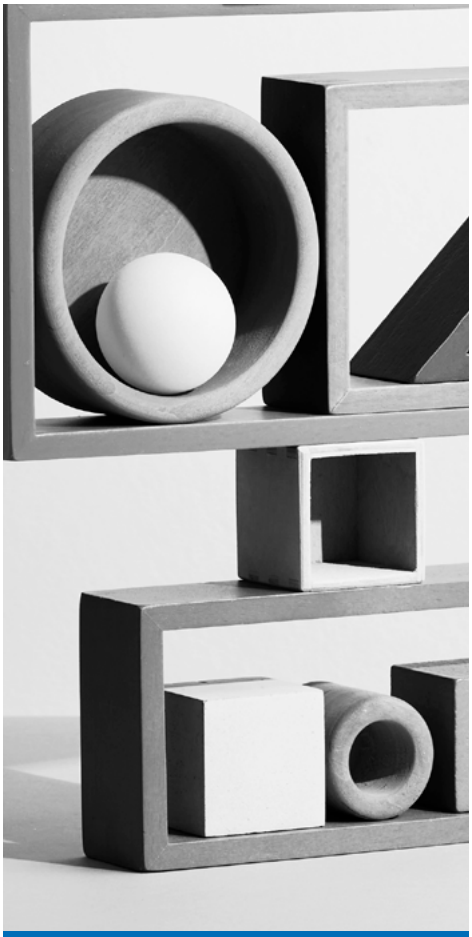
It becomes critical infrastructure when it starts to support cross-sector workloads, for example in public services, cybersecurity, healthcare, manufacturing, agriculture, or transportation. If your country has big economic drivers in manufacturing, agriculture, or textiles, you want that to be part of what the government is supporting at this level. And it is optimized differently from a data center. You are fine-tuning for a specific workflow or model, focused on energy efficiency, and operating in a secure and continuous manner.



What role do open ecosystems play in building national AI capability?

Calista Redmond: Whenever I speak with a developer, a company, or a country or city, I always encourage collaboration. At this stage, no one should work alone, and no one should start with a blank sheet of paper. In just about every industry there is a running start with AI, an application to learn from and build on, and much of this is open.

Open ecosystems fundamentally reduce single-provider dependence. Local teams can inspect, adapt, benchmark, and improve their own work. They can take open models and implement their own language, laws, culture, and industries into them, which reflects national AI capabilities. These open models and tools support local language fine-tuning, RAG, academic research, and startup experimentation.



"Open ecosystems fundamentally reduce single-provider dependence"

Countries become technically stronger when they get to collaborate with peers, learn together, and leapfrog their own technical capacity building. I do want to be clear that open does not mean free-for-all or unmanaged. Countries still need to manage licensing, provenance, security scanning, and guardrails to ensure deployment reflects their intentions. At NVIDIA, we are big proponents of broad open ecosystems. Part of that is the principle of using the right model for the right workflow. You do not need a frontier model for everything, and tuning is critical for every workload.

COUNTRIES BECOME TECHNICALLY STRONGER WHEN THEY GET TO COLLABORATE WITH PEERS, LEARN TOGETHER, AND LEAPFROG THEIR OWN TECHNICAL CAPACITY BUILDING.

What are the biggest misconceptions you encounter when leaders think about national AI strategy?

Calista Redmond: The biggest misconception is that national AI capability means building everything alone or buying a single national model. The better framework is capability and control. Data, compute, and models work within a larger ecosystem that has local components and the strength of a global community.

"The biggest misconception is that national AI capability means building everything alone or buying a single national model"

The second misconception is that AI is only software. AI at national scale is infrastructure: energy, workforce development, procurement, and operating discipline. That is a fundamental thing to consider.

The third is the claim that governance slows innovation. In fact, the right governance accelerates adoption. It gives citizens, regulators, and others the confidence to use AI in high-value workflows. We all started using AI to plan a vacation, and now we are using it to instrument business decisions and outcomes. AI is not an application you are rolling out. It is a new production system, a new platform on which you can accelerate innovation and grow economies. That is more than an app.

If you had to distill your advice to a national AI policy leader into three priorities, what would they be?

Calista Redmond: First, choose three to five high-value missions. Not applications, missions. Unpack the datasets and identify use cases with measurable outcomes such as citizen services response times, fraud detection, or supply chain resilience. Build a collaboration roadmap that identifies the major stakeholders and maps the milestones you can celebrate and the outcomes you can anticipate.

Second, develop a secure AI factory plan. Understand the tiers, the hybrid approach, and the data controls, and start implementing. Without accessible compute, you are limiting innovation, utility, and workflows.

Third, build responsible AI into the operating model from the start. This includes model evaluation, guardrails, human oversight gates, and procurement rules that demand accountability. Think about what responsible AI means for talent, workforce, and the accountability measures that accompany rollout.

And if there is one overarching message, it is this: invest locally, engage globally.

Calista Redmond
VP Global AI Initiatives | Nvidia

"Invest locally, engage globally"

Executive Conversations

KAI-FU LEE

Founder & CEO

01.AI and Sinovation Ventures

OPEN VS. CLOSED AI MODELS

Dr. Kai-Fu Lee is the founder and CEO of 01.AI, a Beijing-based artificial intelligence company focused on large language model development and enterprise AI transformation, venture-built by his tech venture capital firm Sinovation Ventures. He previously led Google's operations in China and held senior roles at Microsoft. Dr. Lee is the author of the New York Times and Wall Street Journal bestseller AI Superpowers, which examines the role of the US and China in the future of artificial intelligence, as well as its impact on society. Dr. Lee trained as a computer scientist in the United States and has spent his career at the intersection of American and Chinese technology development.

UNDERSTANDING AI SOVEREIGNTY

You have navigated the intersection of technology, culture, and geopolitics across the US and China for decades. How do you define AI sovereignty today, and why does it matter?

Kai-Fu Lee: Sovereignty means a number of things. First, it means having control over the technologies themselves. Second, it means ensuring that data, which is a critical asset to every company, does not leak. That concern is widespread across most countries, but perhaps less so in the US, given its more advanced acceptance of private cloud. But throughout the world, companies are deeply concerned about confidential data becoming an input that enriches a general model owned by another country.

There is also the question of suitability. A model trained in one country tends to embed the values of that country, and those values may not be applicable elsewhere. Having control over the model allows a company to fine-tune it, to make it fit the organization. Hosting the model in someone else's cloud limits that ability significantly.

Kai-Fu Lee
Founder & CEO, 01.AI
Chairman,
Sinovation Ventures

> **"Throughout the world, companies are deeply concerned about confidential data becoming an input that enriches a general model owned by another country."**

When Beijing, Brussels, and Washington each talk about AI sovereignty, are they talking about the same thing?

Kai-Fu Lee: Not entirely. There are layers. The first is suitability: every country wants a model that reflects its language, culture, and legal norms. In some Islamic countries, questions around same-sex marriage, alcohol, or religious guidance are handled very differently than they would be in the US. Ensuring compliance with local law, religion, and culture is a legitimate and universal concern.

The second layer is competitive ambition. Some countries feel they need to build their own model in order to have a chance at a meaningful position in this technology race. China clearly has that ambition. Japan, Singapore, Saudi Arabia, and India have all declared theirs. That is admirable. But it is sometimes overly ambitious. Training a frontier general-purpose model from scratch is not feasible for every country. The US has enormous resources. China has substantial resources. Most others do not.

The practical alternative, and I think the right one for almost all countries outside the US and China, is to take a leading open-source model and continue training it for the country's specific language, values, and regulations. Continuing training is different from fine-tuning. It treats an open-source model as a half-baked product. Think of it as buying a frozen pizza and then adding your own ingredients and baking it further per your preference. The result is something adapted to your context, whether an Indian pizza or a Japanese pizza. And, critically, the cost is only a few percent of training from scratch: a few million dollars rather than a few hundred million.

"The practical alternative, and I think the right one for almost all countries outside the US and China, is to take a leading open-source model and continue training it for the country's specific language, values, and regulations."

OPEN-SOURCE MODELS AND THE BUSINESS OF AI DOMINANCE

What has been the actual effect of US export controls on China's AI development?

Kai-Fu Lee: It is a double-edged sword, and the jury is still out. The GPU export restrictions are only one side of the equation. The other side is that Chinese companies are extremely practical. If you survey them, the great majority are not trying to beat Anthropic or OpenAI. The Chinese companies know they cannot spend fifty billion dollars on supersized model training. So, with the GPUs available to them, some domestically produced and not as scalable, they ask: what can we do excellently within these constraints?

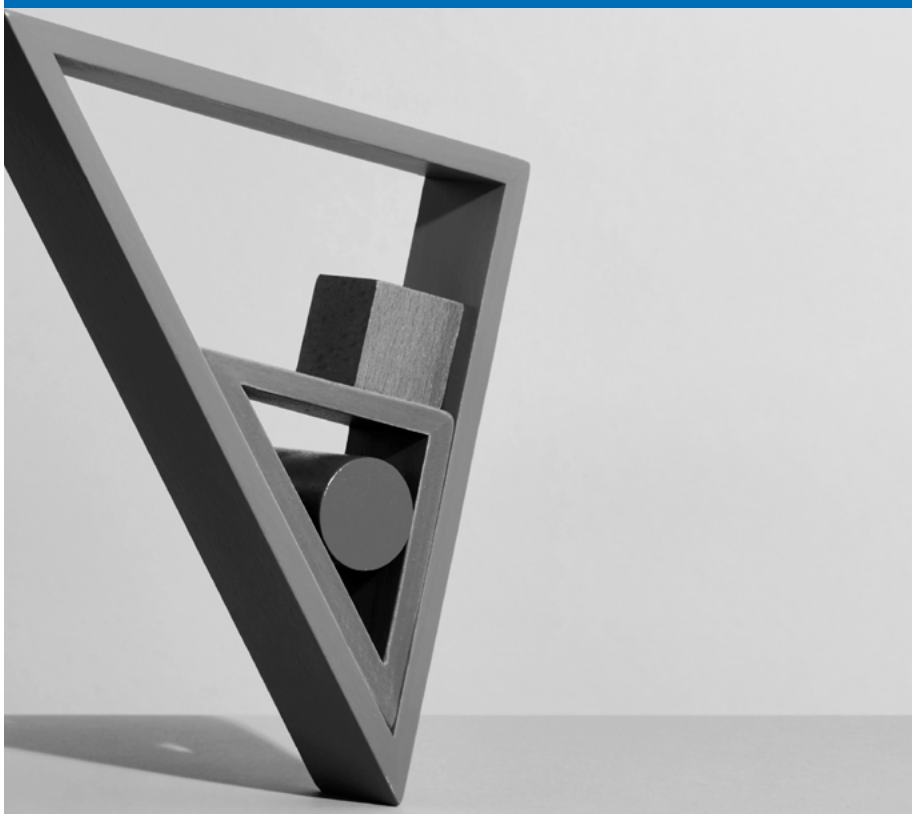
The answer has been rigorous engineering efficiency. DeepSeek is the most well-known example. When people are constrained but motivated, they innovate around the constraint. They optimize architectures, move away from CUDA dependencies, and target performance that is very good rather than definitively the best. Chinese companies are spending less than ten percent of what the top American companies spend on training, yet are producing models that are ninety to ninety-five percent as capable, running six to nine months behind their American counterparts.

"Chinese companies are spending less than ten percent of what the top American companies spend on training, yet are producing models that are ninety to ninety-five percent as capable, running six to nine months behind their American counterparts."

There is also a structural reason Chinese companies have embraced open source. They cannot win on a closed-source basis, so they share. It functions like a study group; not an explicit collaboration where people sit down together, but a dynamic where everyone builds on each other's public releases and the collective competency rises. The American companies behave more like individual researchers, each convinced they will win the Nobel Prize so keeping their know-how secretive. The Chinese companies behave like a group that knows it will not win the Nobel Prize individually, but can get closer collectively by pooling their work.

The deeper strategic question is whether the first company to reach AGI [artificial general intelligence] will dominate everything, or whether four American companies and two Chinese companies will all get there within months of one another, each serving a distinct ecosystem. If you look at the historical trajectory, open-source models have trailed closed-source models by six to nine months. Chinese models have trailed American models by about the same margin. If that pattern holds, then the race may not end with one winner squashing everyone else. But that remains to be seen.

"If you look at the historical trajectory, open-source models have trailed closed-source models by six to nine months."



What will ultimately determine the dominant model? Does being late to AI or AI sovereignty necessarily put countries or companies at a disadvantage?

Kai-Fu Lee: The "AGI-squashes-everyone" idea is unlikely, though not impossible. If American companies end up becoming dominant, my bet is that it will be because of the business ecosystems they build – not because they crossed a technological threshold that rendered everyone else irrelevant.

The first analogy is Windows. Windows did not win because no other company could have built a similar operating system. It won because applications were built on it, enterprises relied on it, and the revenue this generated funded further development, solidifying the position. That virtuous cycle is real and powerful. You see it already with something like Project Glasswing from Anthropic, which only offers exclusive access to top American tech firms to the powerful Mythos model release. Claude Code is also transforming how software is written. Companies will pay significantly for that. The revenue funds more compute, which funds better models.

Being late to AI or to AI sovereignty does not automatically put countries or companies at a disadvantage. In fact, open source models create a meaningful late-mover advantage.

The second analogy is iPhone versus Android. The tension emerges when AI reaches the mass market globally. American models are priced for wealthy markets. When you run advanced tools on closed infrastructure, the costs are significant. Chinese models, by contrast, can cost a sixth to a tenth as much. So, when the technology reaches populations in China, India, and other emerging markets, the American closed source model may simply be priced out of much of that demand.

The outcome may look very similar to iPhone versus Android. Apple captures extraordinary profit, perhaps more than all Android manufacturers combined, but Android has a far larger global footprint in user base. Open source may win on reach and adoption, while closed source wins on margin and ecosystem control. In that world, being late does not mean being irrelevant. It means choosing the right path based on your resources, objectives, and markets.

Should companies and countries be worried that a small number of platforms will dominate everything?

Kai-Fu Lee: I do not think we will end up with just one choice, and that is largely because open source is now unstoppable. History suggests we will see one or two dominant closed-source platforms alongside a large-footprint open-source ecosystem. Linux versus Windows. iPhone versus Android. I predict that AI will follow a similar pattern.

What is important to recognize is that this dynamic may play out differently across layers. The model layer is one competition. The agent layer is another. Open ecosystems like OpenClaw are becoming a platform of choice at the agent level, and they fundamentally change the economics of access and adoption.

OpenClaw, combined with open source models, allows companies and developers to build powerful AI driven workflows without being locked into a single proprietary stack. That is especially important for countries, companies, and developers that cannot afford closed platforms at scale.

I think the likely outcome is not full concentration, but coexistence: one or more closed ecosystems with strong business models, and a large open ecosystem with much wider global reach. The open approach may be less profitable. However, it will be more accessible, making it very difficult to stop. Concentration becomes dangerous only if there is a single choice. Open ecosystems like OpenClaw ensure such a monopoly does not happen.

"Open ecosystems like OpenClaw are becoming a platform of choice at the agent level, and they fundamentally change the economics of access and adoption."

PHYSICAL AI AND CHINA'S EMERGING EDGE

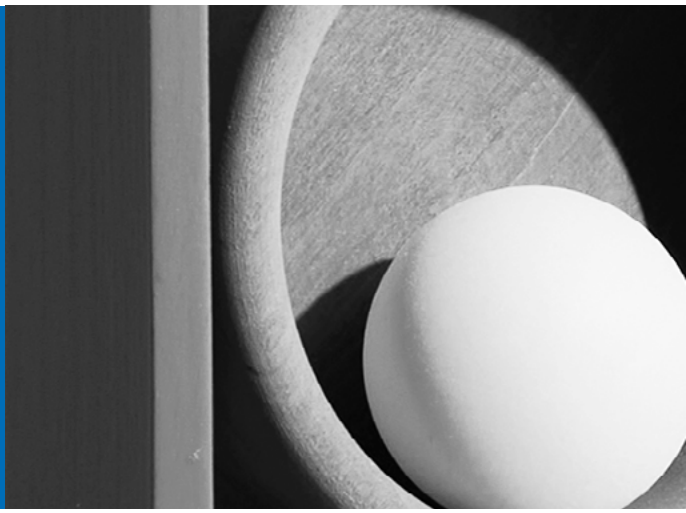
You have argued that China has structural advantages in physical AI, devices, and manufacturing. How durable are those advantages?

Kai-Fu Lee: Hardware is a completely different game from software. When the iPhone launched, American companies held nearly every advantage: design, software engineering, market reach. China's role was centered on manufacturing. Foxconn made money, but only a fraction of what Apple made.

That is no longer the situation. China now has the supply chain and ecosystem to build virtually any hardware product. China also builds at substantially lower cost than the US – from phones and PCs to robots, manufacturing devices, and new form factors such as glasses, watches, and wearable recorders. Huawei, Xiaomi, and ByteDance are all building devices. The barrier that once protected American hardware dominance no longer exists in the same form.

There is a related data point worth making. We are entering an era where AI will increasingly be speech-driven. The power of LLMs is that we can interact through language, and speech recognition is approaching perfection. Devices that record ambient interactions, workplace conversations, and meetings generate a fundamentally new category of data. I use a ByteDance recorder daily. Every meeting in my company is captured, transcribed, and analyzable by a large language model. I cannot attend every meeting, but I can virtually

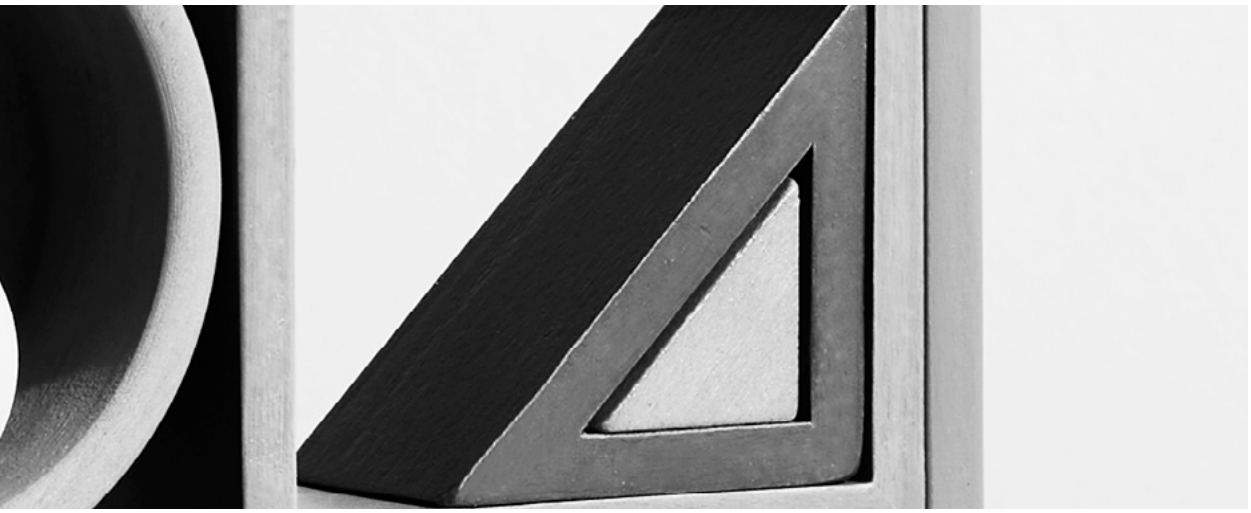
"Chinese VCs are more willing to fund hardware ventures precisely because they believe China has the edge there."



attend every meeting through that AI analysis. That is a profound operational insight tool.

The broader point is that China has a cultural advantage in data generation at scale. In AI 1.0, China had a data advantage from its vast population and usage. In AI 2.0, driven by large language models, the advantage shifted because the training data was drawn largely from the public internet, where English-language data was of particularly high quality. But now, with new data being generated through audio, video, and physical world interactions, China's advantage returns – partly from scale, and partly because there is less cultural resistance to recording and data capture than you would find in Europe or the US.

Add to that a government mandate focused explicitly on using AI to transform manufacturing. China's economy remains fundamentally manufacturing-led, rather than knowledge-based. The State Council of China's public priority is deploying AI in factories and industrial settings. That mandate creates demand, focus, and funding alignment that does not exist to the same degree elsewhere. And Chinese VCs are more willing to fund hardware ventures precisely because they believe China has the edge there, the cost of building hardware is lower, the required capital is therefore smaller, and speed is much faster.



THREE OPTIONS – NOT TWO

What are the most consequential mistakes you see countries make in how they think about AI sovereignty?

Kai-Fu Lee: For countries, the clearest error is believing that the only two choices are to accept an American model or to build one from scratch. Those are not the right two options. The real choices are: first, to adopt a leading closed-source American platform, with full awareness of the sovereignty trade-offs involved; second, to take an open-source model and continue training it for your language, values, and regulatory requirements – at a fraction of the cost and with a realistic chance of success. Building from scratch to compete with the US and China is a third path, but it requires going in with eyes fully open to the fact that, for most countries, it is unlikely to succeed.

Kai-Fu Lee
Founder & CEO, 01.AI
Chairman,
Sinovation Ventures

"Open source may win on reach and adoption, while closed source wins on margin and ecosystem control."

Conversations FOR TOMORROW

Executive Conversations

SHARAD SRIWASTAWA

Co-CEO, Rakuten Mobile
President, Rakuten Symphony

OWNING THE NETWORK: WHY SOVEREIGNTY IS THE NEXT FRONTIER FOR TELECOMS

Sharad Sriwastawa serves as co-Chief Executive Officer and Chief Technology Officer of Rakuten Mobile and President of Rakuten Symphony, a Rakuten Group company spearheading the global adoption of open, cloud-native platforms. Sharad joined Rakuten in 2018 to lead the deployment of Rakuten Mobile, Japan's newest and most modern mobile network. He was appointed to his current positions in 2023. Sharad has held global executive roles in India, the Middle East, Australia, the US, and Asia, working with major mobile operators and vendors including Reliance, T-Mobile, Telstra, Siemens, and RAN technology vendor Airspan Networks.

THE ORIGINS OF RAKUTEN'S OPEN PLATFORMS APPROACH

Can you briefly explain Open RAN and how Rakuten Mobile built its network?

Sharad: In 2018, we could have followed the traditional telecom path, selected an incumbent vendor, and built the network the traditional way. We chose a very different route.

We built the Rakuten Mobile network on four pillars. First, complete disaggregation of hardware and software, using off the shelf commodity servers, rather than proprietary equipment. Second, full virtualization and cloudification of every workload, not just the RAN but also the core, BSS, load balancing, everything. Third, AI and automation from day one. We were competing against established operators in Japan and had to control our cost structure closely. Fourth, we embedded security from the start through a DevSecOps approach.

Open RAN, as we define it, goes beyond simply virtualizing software. It is about fully disaggregating the hardware and software stack and moving away from black box systems toward a software defined architecture. That shift gave us far greater flexibility and delivered significant capex and opex savings, which we can now pass on to customers in the form of lower cost connectivity.

Sharad Sriwastawa
Co-CEO at Rakuten Mobile | President at Rakuten Symphony

> **"In 2018, we could have followed the traditional telecom path, selected an incumbent vendor, and built the network the traditional way. We chose a very different route."**

UNDERSTANDING NETWORK SOVEREIGNTY

What does network sovereignty mean to Rakuten?

Sharad: Network sovereignty means you own the infrastructure; you control what runs inside your network; and you control your own software roadmap based on the needs of your geography.

> "Network sovereignty means you own the infrastructure; you control what runs inside your network"

At its core, network sovereignty is the end of permission based innovation. For decades, operators had to wait for vendor release cycles to introduce new capabilities. Sovereignty means you control your own destiny. You are not just operating technology. You are the owner of your technology investment.

We also see governments shifting their focus from data sovereignty to infrastructure and software sovereignty. In parallel, geopolitical pressures are pushing many governments to impose restrictions on, or mandate the removal of, high risk or untrusted vendors. That combination is fundamentally reshaping how operators think about their networks.

> "Open RAN makes sovereignty economically viable and operationally affordable"

Is Open RAN a technology choice, or a sovereignty choice?

Sharad: It is both. Open RAN makes sovereignty economically viable and operationally affordable. You can talk about sovereignty, but if it is too expensive, operators will not pursue it, especially given the pressure on ARPU [average revenue per user], capex, and opex.

Open RAN provides a path to sovereignty that operators can actually afford. It allows them to control their destiny without compromising financial sustainability.

What is your view on fragility vis-à-vis open and closed systems?

Sharad: Fragility in a network comes from two things: single points of failure, and the inability to respond quickly when something goes wrong.

Open RAN addresses both. Because hardware and software are decoupled, you can change the hardware component relatively easily if there is geopolitical disruption or a security threat to a particular vendor. There are multiple options available.

In a vendor lock-in system, if something goes wrong with your sole supplier, it is extremely difficult to exit. The closed system is the fragile one.

Rakuten is one of very few organizations that have built a fully cloud-native network at scale. What has that experience taught you about sovereignty?

Sharad: The two concepts, Open RAN and cloud native, are related but should be considered separately. Each contributes something distinct to the sovereignty question. Open RAN is fundamentally about disaggregation. Cloud native – meaning Kubernetes,[1] microservices, containerized workloads – is a different dimension.

The case for cloud native rests on three things. First, the speed and ease of change. In traditional telecoms, engineers still work maintenance windows through the night to push updates. If you look at how OTT providers manage their IT workloads, change requests are serviced during the day with no downtime, because the architecture supports self-healing. Second, operational convenience flows directly from that. Third, and most importantly, security. A cloud-native network is not opaque. The visibility you gain with a cloud-native network, whether for security testing or for embedding security algorithms directly into the CI/CD [continuous integration/continuous delivery] pipeline, is far greater than anything a closed system offers.

[1]Kubernetes is an open-source system that automates the deployment, scaling, and management of containerized applications.

What are the broader implications of Rakuten's approach for operators pursuing sovereignty?

Sharad: Open RAN is gaining real traction this year. We have more than ten proof-of-concept deployments running right now, and expect four or five of those to go to scale in 2026 and 2027. Our network buildout with 1&1 in Germany is the first fully virtualized mobile network based on Open RAN standards in Europe, and it is growing well. Boost Mobile in the US is another proof point.

The technology is no longer in question. Concerns around massive MIMO [multiple-input multiple-output], power efficiency, and scalability have been resolved. What is lacking is the commercial motivation to move.

Going forward, any greenfield operator will choose Open RAN. The architecture gives them the flexibility to migrate from 4G to 5G to 6G without ever having to swap out a proprietary closed system.

OUR NETWORK BUILDOUT WITH 1&1 IN GERMANY IS THE FIRST FULLY VIRTUALIZED MOBILE NETWORK BASED ON OPEN RAN STANDARDS IN EUROPE, AND IT IS GROWING WELL

How do you see AI reshaping telecoms, and does it introduce new sovereignty dependencies?

Sharad: In telecoms, there are two distinct dimensions to consider. The first is using AI for network operations. The second is AI-native products, which are still thin on the ground. In BSS [business support systems] and OSS [operations support systems], things are beginning to take shape. But for the broader network estate, AI is layered on top of legacy infrastructure that was designed 20 years ago and is neither cloudified nor AI-native by architecture. You can achieve a certain level of automation on top of that, but the underlying architecture sets a ceiling on automation.

But the potential is enormous. The collective capex and opex burden across global telecoms is massive, and AI offers a meaningful path to reducing it. We are seeing operators begin to collaborate in this area. At the last MWC [Mobile World Congress], AT&T announced its own small language model initiative. For network operations, you do not need large language models. You need cost-effective, domain-specific small language models. For customer-facing applications, BSS, customer support, and retail interactions, the opportunity is huge and everyone is working on it.

OWN THE CONNECTIVITY FUTURE

When a country says it wants to own its connectivity future, what does that mean in practice?

> "Going forward, countries want resilient networks built on many smaller facilities"

Sharad: In a recent conflict, a small number of data centers were damaged and entire banking systems went offline. That illustrates the risk of over-dependence on a limited number of centralized assets. Going forward, countries want resilient networks built on many smaller facilities, with automation that enables seamless failover without massive capital investment.

These systems must also be simple enough to operate with local talent, rather than highly specialized experts flown in to keep the network running. Owning your infrastructure means it is available off the shelf, transparent, and free of black boxes.

"With Open RAN, you take the software, source your own hardware, operate the network, and carry no dependency on a particular vendor"

Can sovereign networks still be global and interoperable?

Sharad: Sovereignty does not mean fragmentation. The protocols are standardized. A device will not function if it does not follow the protocol. Open RAN is based entirely on 3GPP, so anyone, anywhere can deploy it. There is no inherent vendor dependency baked into the architecture. Operators can take the software, own it, and, in time, take the code and modify it themselves. That is the future I see.

For 30 or 40 years, network operators have focused on generating revenue and delivering customer satisfaction. The technical domain was someone else's problem. But the next generation of CTOs is beginning to think not just about managing technology but owning it. If you look at how enterprises treat their IT estate, they do not merely manage IT. They own it. That ownership mindset is what needs to transfer to telecoms.

With Open RAN, you take the software, source your own hardware, operate the network, and carry no dependency on a particular vendor. The same logic will extend across the stack. Where standards exist, as they do for RAN, this is relatively straightforward. Where they do not yet exist, as in infrastructure observability, those standards still need to be developed.

OPENNESS AND SECURITY

There is a perception that openness creates greater security risk. What is your view?

Sharad: An open system is not inherently less secure. If you own the system, you gain visibility, and with visibility you can make it more secure. An opaque, closed system gives you nothing to work with. When something goes wrong inside a black box, you cannot inspect it, instrument it, or respond to it effectively. We have seen cases where a vulnerability in a single vendor's platform affected operators globally, forcing widespread simultaneous upgrades. That is the risk of concentrated, opaque dependency.

Looking at the extraordinary pace at which AI-driven security capabilities are advancing, these tools work best on transparent, inspectable systems. The function of traditional penetration testing is increasingly being handled automatically, and that will only accelerate. The principle is straightforward: be cloud-native, be transparent, and ensure you have access to your own infrastructure. Without that access, you cannot make it secure.

RECOMMENDATIONS FOR CXOS

What are your top recommendations for CTOs and CIOs building future telco networks?

Sharad: First, if sovereignty is being pursued at a country or regional level, operators must collaborate, rather than compete in isolation. The technologies chosen for the future should be standardized across the region, and operators must work together to create and own standardized technologies, rather than simply manage them, but this will take time. The industry has been dependent on a small number of vendors for decades, and the required skill sets are not yet widely available.

Second, sovereignty requires ownership not just of technology but of infrastructure, and accepting responsibility for its reliability.

Third, resilience must be baked into the design. The challenge is cost. Instead of building multiple redundant data centers, the goal should be architectures that behave as if redundancy exists, without the capital burden. That is only possible with cloud native applications.

Sharad Sriwastawa
Co-CEO at Rakuten Mobile |
President at Rakuten Symphony

"If sovereignty is being pursued at a country or regional level, operators must collaborate, rather than compete in isolation"

Perspectives from Capgemini

P.172
Karine Brunet
Chief Operations and Delivery Officer,
Capgemini

Karine Brunet

Chief Operations and Delivery Officer, Capgemini

Karine Brunet is Chief Operations and Delivery Officer at Capgemini and a member of the Group Executive Board, roles she has held since January 2026. Previously, she was CEO of Capgemini's Cloud Infrastructure Services and earlier served as COO of the business, joining the Group Executive Committee in 2023. With a strong track record in leading large-scale transformation and infrastructure services organizations, Karine brings deep operational and technology expertise from senior roles at Vodafone, Steria, and Alcatel Group. She began her career at NCR and holds master's degrees from Middlesex University London, Nantes University, and Paris School of Business.

WHY THE RACE FOR TECH SOVEREIGNTY IS A BALANCING ACT

As geopolitical tensions rise and digital interdependence deepens, tech sovereignty has become a cornerstone of economic resilience, national security and competitiveness. Yet, in a hyper-connected world, full autonomy is an illusion.

Organizations need to identify the potential risks they face and to design an affordable sovereignty strategy that will enable them to protect their businesses. Their challenge is to maintain strategic control over critical technologies, without falling into the illusion of self-sufficiency – ensuring sovereignty becomes a stimulus, not a constraint, for innovation and growth.

Tech sovereignty – the race is on

Geopolitical tensions, regulatory complexities and digital interdependencies have exposed critical vulnerabilities, notably in Europe, where more than 80% of digital products, services, infrastructure and intellectual property are imported.

In September 2025, Ursula von der Leyen called for Europe's independence moment "to take control over the technologies that will fuel our economies." Similar ambitions are evident in the US, with initiatives to secure semiconductor production, and in China, which continues to double down on self-reliance. A global investment race is, therefore, underway to safeguard sensitive data, ensure business continuity and control critical technologies.

> "In today's globally hyper-connected digital world, no nation is truly sovereign"

Tech sovereignty is now at the top of political agendas and central to public debate, yet too often, this debate lacks nuance. The paradox is that in today's globally hyper-connected digital world, no nation is truly sovereign. Digital architecture relies on rare earths, semiconductors, data centers, infrastructure, hardware, software and increasingly AI models – components which are sourced by their very nature across borders. No single country or company controls the entire value chain, and very few can afford to.

> "No single country or company controls the entire value chain, and very few can afford to"

Owning and operating data centers alone isn't the answer. In short, digital self-sufficiency does not exist; it is neither realistic nor desirable. The challenge for organizations is to decide how much they are willing to invest to gain strategic control over the critical technologies they need and mitigate risks. There is no single answer to that question.

Tech sovereignty isn't a monolithic concept; it encompasses multiple dimensions of sovereignty. These include data (control over data storage, access and governance); operational (autonomy and resilience in managing

"Digital self-sufficiency does not exist; it is neither realistic nor desirable"

and executing digital operations safely); technical (development and control, including hardware and infrastructure); and even legal sovereignty (power to establish and enforce the regulations that govern digital infrastructures, technology actors, services and data within its territory). Decision-makers need to fully comprehend how these dimensions interact to navigate the trade-offs with full knowledge of their strategic implications.

From autonomy to resilient interdependence

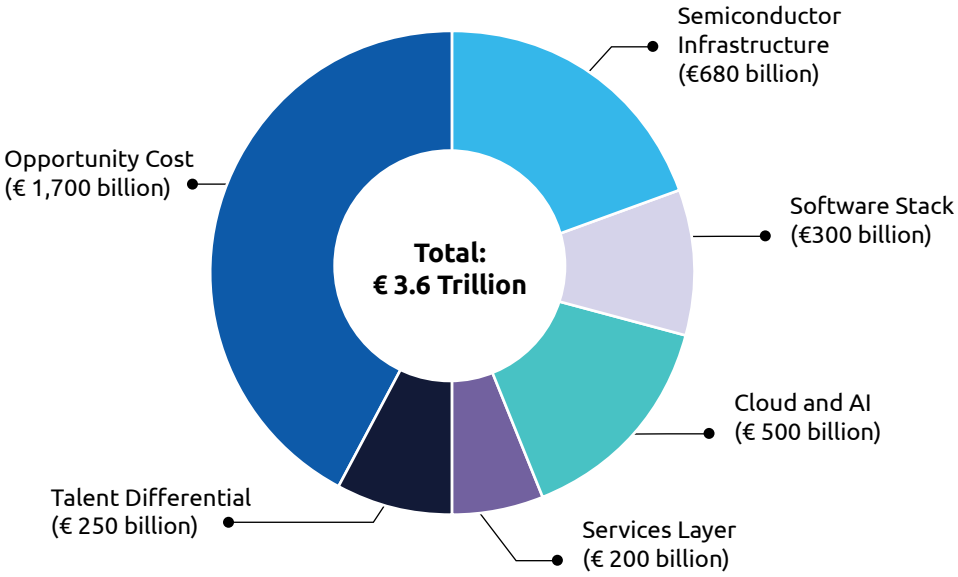
Today, the focus is shifting from full autonomy to resilient interdependence. Sovereignty now means balancing strategic self-reliance with intelligent partnerships. Economic sovereignty does not equate to isolationism – closing borders isn't the solution. Resilience and leadership will come from securing critical capabilities to reduce high-risk dependencies, while remaining open to collaboration at an affordable cost.

If it can't compete on investment, Europe – in particular – must adopt a pragmatic approach and place its bets. Sovereignty strategies should be based on a clear assessment of urgency, identifying which sectors require strategic control and where partnerships can expedite progress.

"Today, the focus is shifting from full autonomy to resilient interdependence"

Defence companies, for instance, must own and control technologies, cybersecurity and data. For many businesses in less sensitive

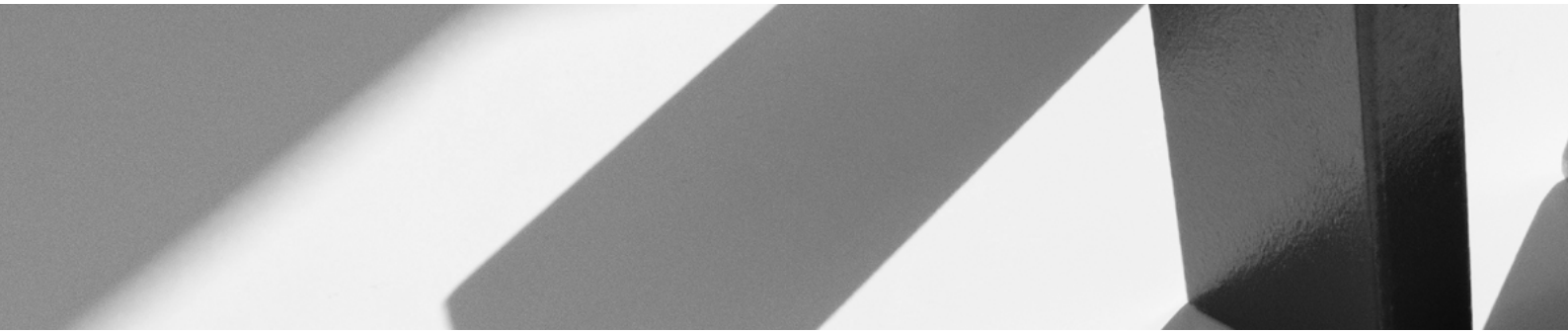
The Prohibitive Bill for European Digital Sovereignty



Source: Center for European Policy Analysis, "Digital Sovereignty: Can Europe Afford It?", October 2025

sectors, the priority is mostly data sovereignty (for example, making sure data is accessible at all times, protected from any breaches and shielded from unwanted foreign access). For others, sovereignty means avoiding dependency on a single technology provider.

These varied needs can be met through pragmatic solutions, not ideological, one-size-fits-all approaches. Critical dependencies have to be identified and analysed in order to build the right sovereignty plan, taking into account one's industry, customer base, country of operation, supply chain and IT architecture.



The role of regulation

> "Regulation must enable – not stifle – innovation"

Tech sovereignty has naturally become a political debate, layered on top of economic and technological concerns. It includes having the ability to shape the rules and values that govern digital systems through robust policy and regulatory frameworks covering energy, connectivity, semiconductors, AI or even talent. However, regulation must enable – not stifle – innovation.

Over-regulation, particularly in emerging technologies like AI, risks slowing adoption and undermining Europe's leadership potential. A rigid pursuit of control can create a vicious circle: limiting competitiveness and delaying digital transformation.

Likewise, compliance with ever-changing rules is a challenge in the fast-paced, ever-evolving race for innovation. Sovereignty must rest on unified, stable, forward-looking regulatory frameworks that support innovation and competitiveness. Fragmented or overly restrictive policies will only weaken the very resilience they aim to build.

Ultimately, sovereignty is not just about control – it's about resilience, performance, and competitiveness. It's about ensuring regions can lead in the technologies that matter most, while remaining agile, open and innovative. In the digital age, we must ensure that strategic autonomy is designed not as a fortress, but as a launch pad for transformation.

> "Ultimately, sovereignty is not just about control – it's about resilience, performance, and competitiveness."

INSIGHTS FROM THE CAPGEMINI RESEARCH INSTITUTE

DIGITAL SOVEREIGNTY:

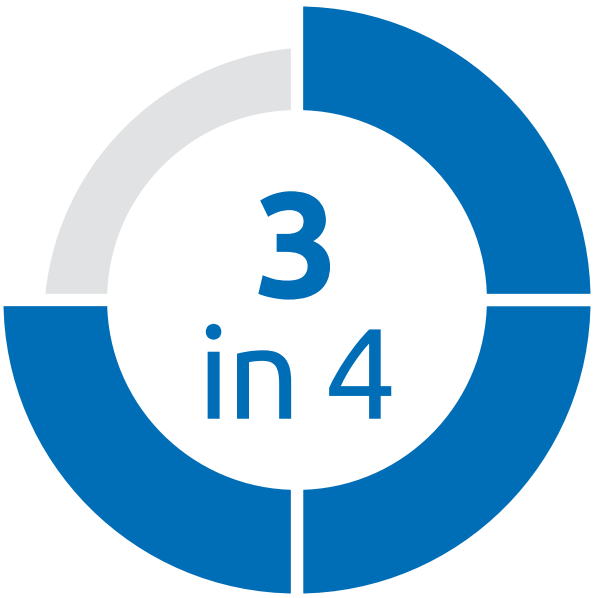
FROM POLICY AMBITION TO EXECUTIVE IMPERATIVE

For details on the research methodology and to read the full report, please visit:

https://www.capgemini.com/insights/research-library/digital-sovereignty/

Digital sovereignty has entered the mainstream

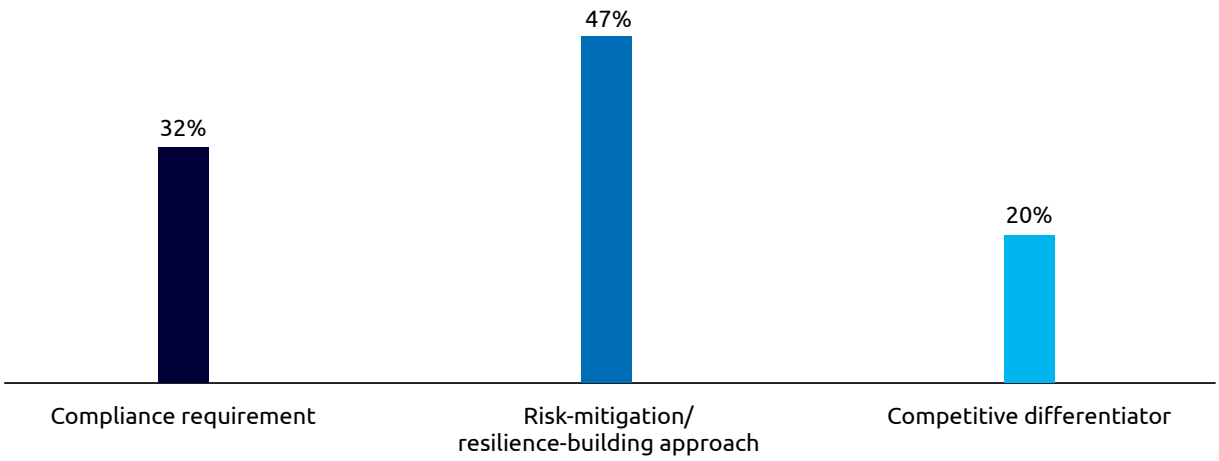
Digital sovereignty is no longer optional



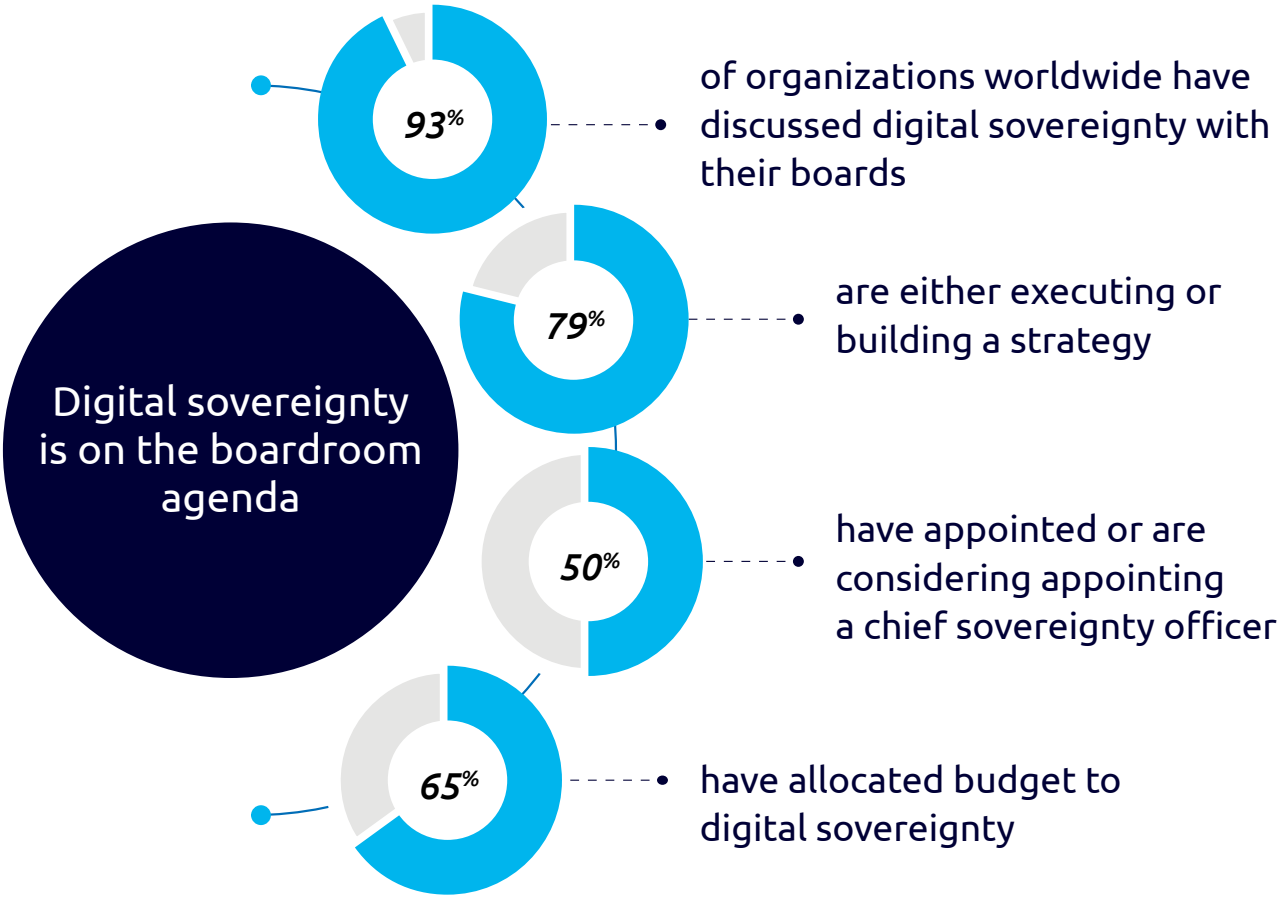
Organizations worldwide are highly *concerned about securing critical business operations* amid current geopolitical tensions

Nearly half of organizations view it as a risk-mitigation/resilience-building approach

Principal view of digital sovereignty



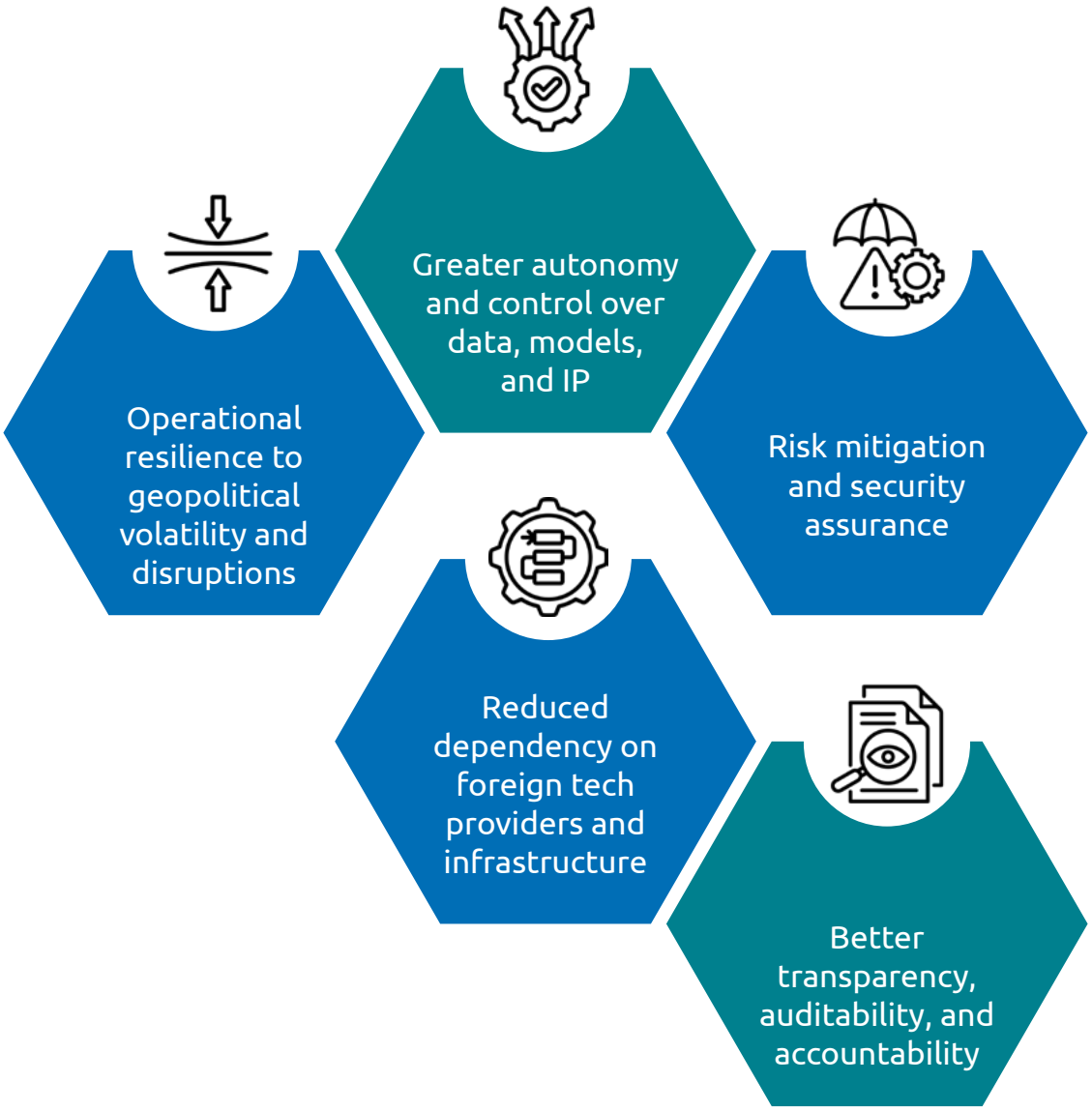
Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.



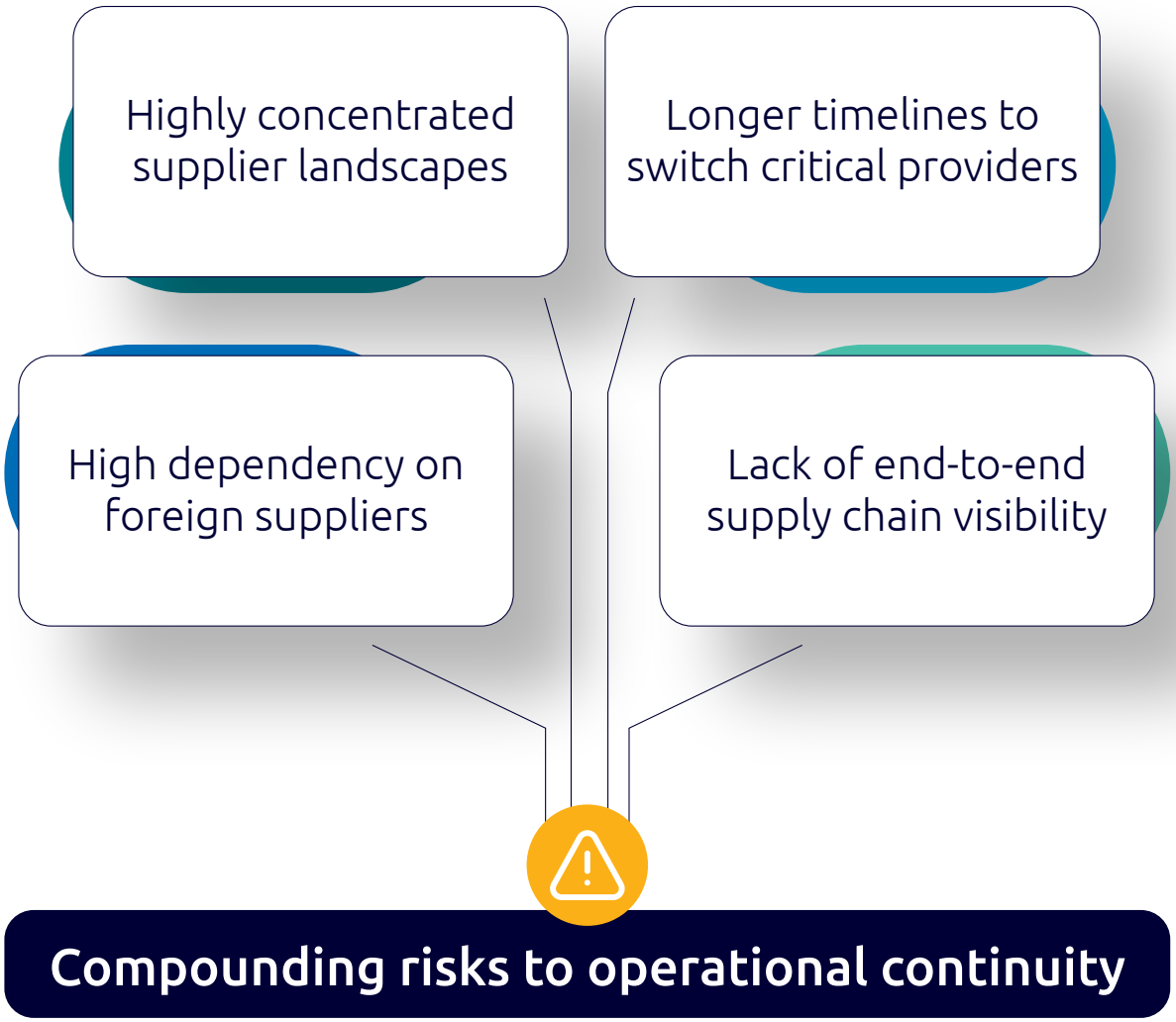
Digital sovereignty exists on a spectrum

Most (59%) organizations admit that full digital sovereignty is not a realistic goal

The strongest motivators to pursue digital sovereignty today are:



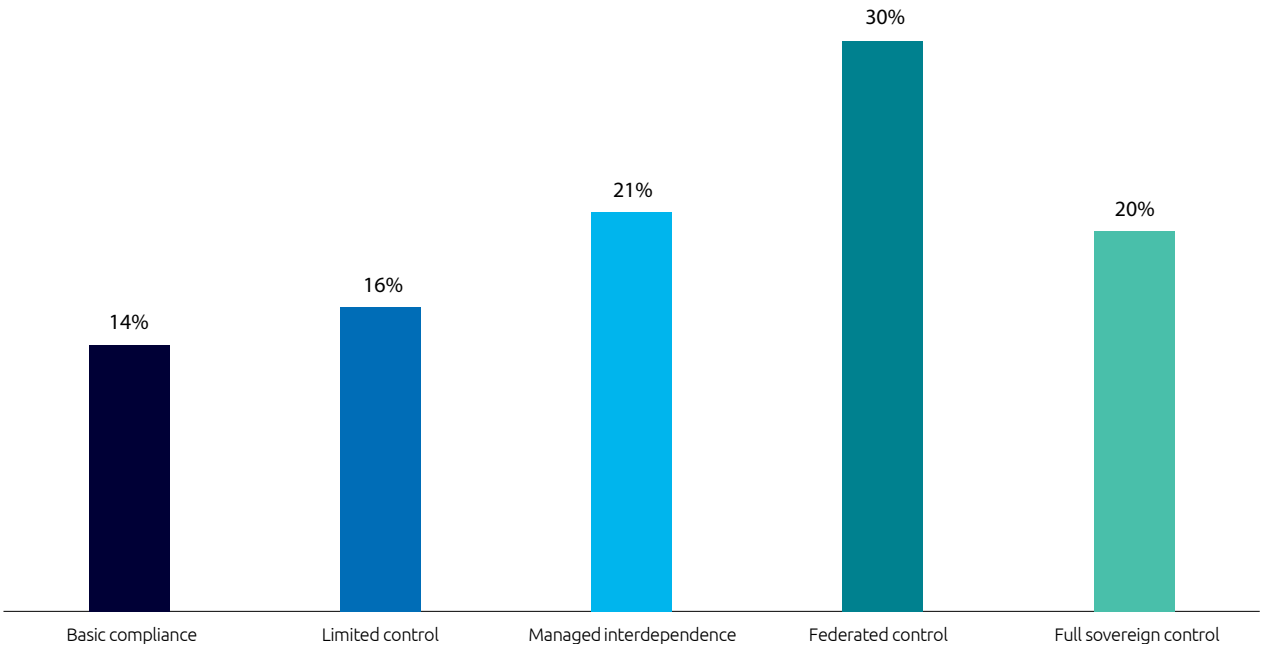
Organizations face significant technology dependency risks



Organizations are pragmatic in their pursuit of digital sovereignty

Around half of organizations pursue federated control or managed interdependence models across the dimensions

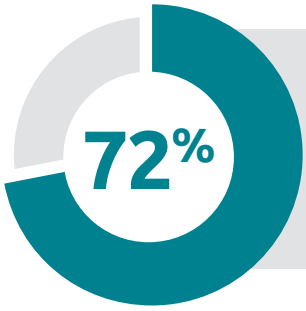
Organizations' desired level of digital sovereignty across the tech stack



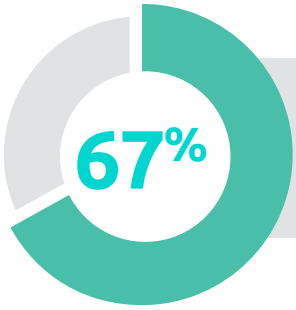
Source: Capgemini Research Institute, Digital sovereignty survey, April 2026, N = 1,300 executives.

Definitions: Full sovereign control (in-house/local; end-to-end control across the stack); federated control (shared control with certified local/regional partners; localized critical operations); managed interdependence (contractual partnerships with global providers; technical safeguards in place); limited control (policy-driven; selective controls applied on a case-by-case basis); basic compliance (only foundational security/compliance measures in place).

Most organizations are clear that they will not compromise on vendor choice or performance to reach their desired level of digital sovereignty



of organizations agree that active participation in ecosystems and/or consortia is essential to achieve digital sovereignty



of organizations believe that digital sovereignty can enable innovation

In the future, *nearly half of organizations expect digital sovereignty to become a competitive differentiator*, while 39% see it evolving into a regulated baseline requirement, and 15% view it as the cost of doing business

How organizations can begin their digital sovereignty journeys

Conversations FOR TOMORROW

Notes

Notes

Conversations FOR TOMORROW

Notes

Acknowledgments

We are grateful to all our guest contributors for sharing their experience and insights as well as to their teams, and in particular Christian Klein, Bethany Shores (SAP), Anu Bradford (Columbia University), Kai-Fu Lee, Anita Huang, Melody Xu (01.AI / Sinovation Ventures), Jai Haridas, Fotini Kaklamanou, Victoria Araujo (Google Cloud), Jean Coumaros, Melanie Pasquier (Bleu), Joakim Reiter, Kate Harris, Adam Liversage, Lawrence Abel (Vodafone), Calista Redmond, Chandler Gavin (Nvidia), Alexander Zwart, Henk Richmond, Margot Haring, Monique Middelkoop (Rabobank), Lila Tretikov, Trina Lundstrom (NEA), Sharad Sriwastawa, Chetan Wani, Mark Mowbray (Rakuten Mobile), Dirk Schrödter, Daniel Müller (State of Schleswig-Holstein) for their contributions to this edition of the journal.

We would also like to thank all our Capgemini colleagues who have been supporting this project throughout and in particular Aiman Ezzat, Fernando Alvarez, Karine Brunet, Audrey Goffi, Frederic Van Der Sande, Stanislas De Roys, Jean-Marc Gaultier, Herschel Parikh, Tracy Perez-Diana, Valerie Masson, Katerina Hubka, Edouard Morio De L'isle, Janet Smith, Johanna Sundh, Shoko Ueno, Oliver Jones, Marc Reinhardt, Laura Immonen Beatty, Wim Stolk, Victoire Grux, Florence Lièvre, Christel Lerouge-Finet, Tricia Stinton, Thomas Hirsch, Sam Connatty, Camille Marc Dura, and the Capgemini Research Institute team: Jerome Buvat, Subrahmanyam Kanakadandi, Dominique Banon, Vaishnavee A, Marissa Slatter, Neil Fernandes, Punam Chavan, Aparajita Paul, Sonali Malekar, Vibha Palekar, Suparna Banerjee, Subhadra Chakraborty, Sujoy Karmakar, Alexander Rainer, Gregory Nieuwsma and Ramendra Ahuja.

Conversations FOR TOMORROW

Please scan the QR code to explore the complete collection of
Conversations for Tomorrow interviews and in-depth research on digital sovereignty.

Discover more about our recent research

Conversations for Tomorrow: Crafting Tomorrow – Leader's perspective on technology

Conversations for Tomorrow: Gener(AI)ting the future

Conversations for Tomorrow: Breathe (in)novation – uncover innovations that matter

The resurgence of manufacturing

Physical AI

Digital Sovereignty

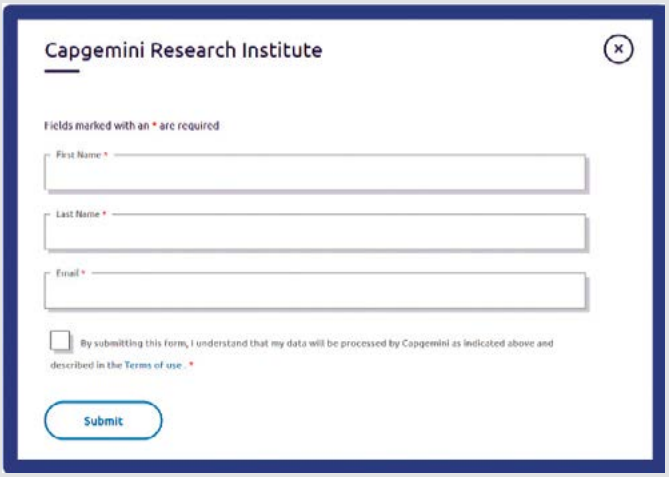
The on-demand tech paradox

Next gen supply chain

The B2B pulse for Telcos # 2

Subscribe to the latest research from the **Capgemini Research Institute**

Receive copies of our reports by scanning the QR code or visiting https://www.capgemini.com/insights/research-institute/subscribe/



About Capgemini

Capgemini is an AI-powered global business and technology transformation partner, delivering tangible business value. We imagine the future of organizations and make it real with AI, technology and people. With our strong heritage of nearly 60 years, we are a responsible and diverse group of over 420,000 team members in more than 50 countries. We deliver end-to-end services and solutions with our deep industry expertise and strong partner ecosystem, leveraging our capabilities across strategy, technology, design, engineering and business operations. The Group reported 2025 global revenues of €22.5 billion.

Make it real | www.capgemini.com

About Capgemini Research Institute

The Capgemini Research Institute is Capgemini's in-house think tank on all things digital. The Institute publishes research on theimpact of digital technologies on large traditional businesses. The team draws on the worldwide network of Capgemini experts and works closely with academic and technology partners. The Institute has dedicated research centers in India, Singapore, the United Kingdom, and the United States. It was recently ranked number one in the world for the quality of its research by independent analysts.

https://www.capgemini.com/insights/research-institute/