Capgemini
RESEARCH INSTITUTE

Digital Sovereignty

The New Tech Order

Conversations FOR TOMORROW

N°11 — 2026

Executive Conversations

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?

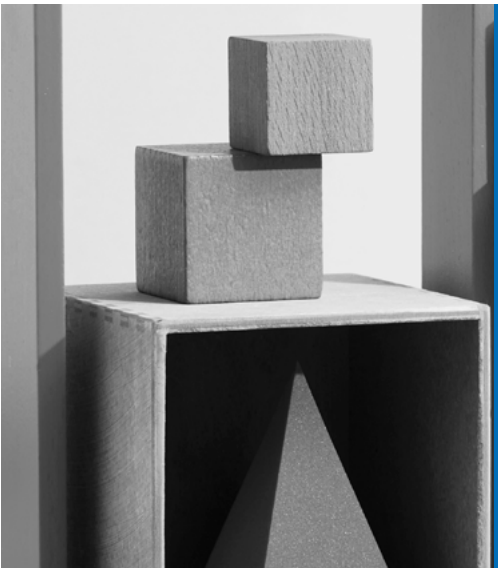
Jean Coumaros: Yes, particularly around digital resilience. In France and across several other European markets, including Germany, the debate has in some cases become irrational and almost caricatural. Some people have started to conflate digital resilience with digital autarky, expecting cloud providers 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.

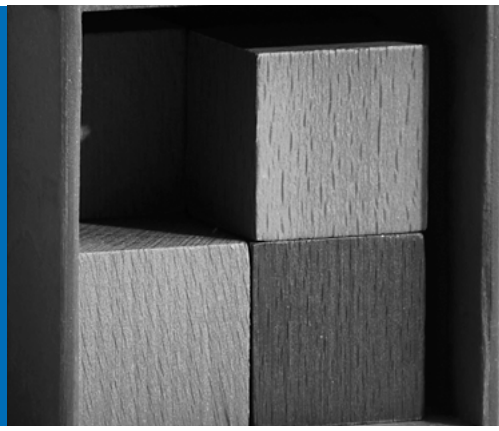
What is your advice to CEOs and senior executives navigating the digital sovereignty challenge?

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"

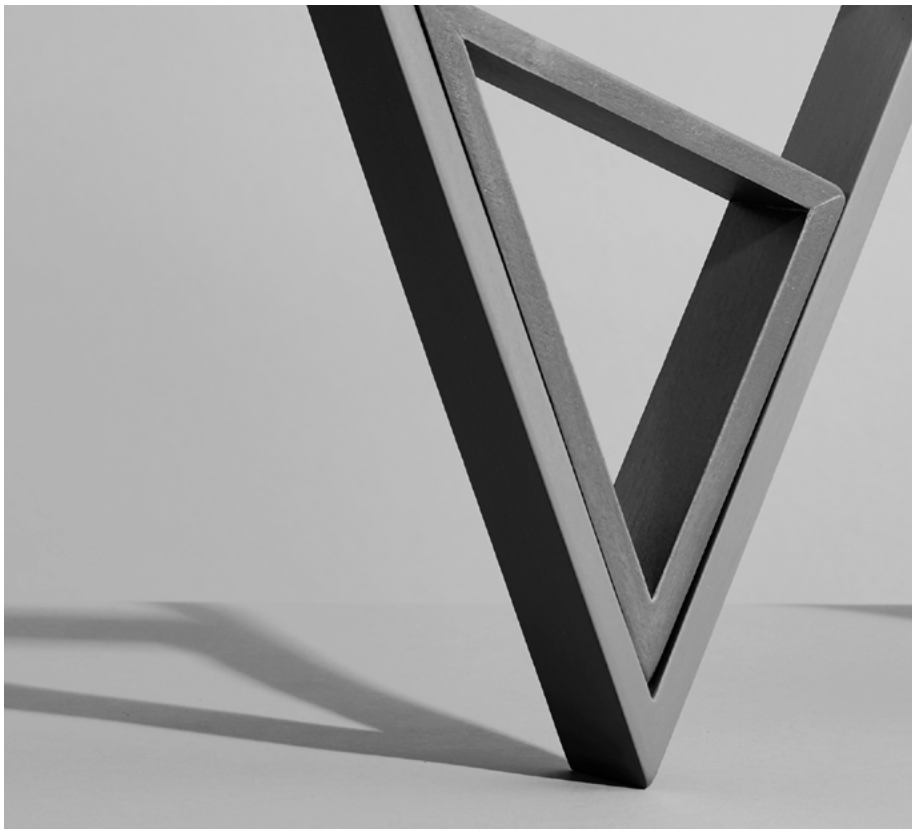


Looking three to five years ahead, how do you see the digital sovereignty landscape evolving across industries and countries?

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."

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/