Briefing Paper

A Digitally Sovereign Britain

Authored for FOTI by Megan Kirkwood and Taylor Gese

April 2026

Executive Summary

The UK's digital infrastructure - the backbone of public services, national data storage, defence operations, and more- is overwhelmingly controlled by a handful of foreign technology firms. This is a structural vulnerability that undercuts British economic security, national defence, and democratic resilience.

Digital sovereignty is the capacity of a state to exercise effective control over its technology: to ensure it operates within the rule of law, under democratic oversight, and beyond the reach of any foreign actor's ability to disable it. It also enables sound policymaking and ensures that the economic value generated by technology is retained within the UK rather than exported abroad.

Measured against that definition, the UK is not sovereign. It is critically dependent, and the cost of that dependency is rising.

This briefing outlines a portion of that dependence, assesses the risks it creates, and sets out a path forward. While dominant technology firms often characterise digital sovereignty as protectionist or impractical, we argue the opposite: it is a strategic necessity. The UK must shift from passive consumption of, and reliance on, foreign technology to the active stewardship of domestic digital capability - ensuring it retains control over critical infrastructure and economic value regardless of geopolitical change.

The UK's unique position and proven track record in technology and innovation give it a genuine opportunity to negotiate from a position of strength. But that strength depends on critical infrastructure that cannot be leveraged against us by allies or adversaries alike. Digital sovereignty is not an argument for isolation, it is the foundation for building partnerships, deals, and alliances from a position of resilience and long-term national benefit, rather than structural dependence or extraction.

Key Takeaways

- The UK's digital exposure spans every layer of the critical technology ‘stack’. Cloud infrastructure is foundational, and the most thoroughly compromised by foreign control.
- Two US firms dominate UK cloud. Amazon Web Services (AWS) and Microsoft Azure control 60–80% of the UK cloud market, per the Competition and Markets Authority's (CMA) July 2025 investigation. Government departments alone spend £6bn annually with these firms.
- Defence is highly exposed. The MOD’s contracts with Google, Oracle, AWS, and Microsoft exceed €1.099bn (£960m), with minimal diversification toward sovereign alternatives. The US CLOUD Act allows US law enforcement to compel data access regardless of where it is stored. As geopolitics shift and even longstanding partners have demonstrated willingness to use technological leverage for strategic ends, the threat of a 'kill switch' is no longer theoretical.
- More broadly, procurement has been captured by US Big Tech. Informal Memoranda of Understanding (MOU) between US Big Tech and UK government departments often bypass competitive tendering, entrenching hyperscalers before formal processes begin, and before any British competitor stands a chance.
- Current policy approaches are increasing dependence. The government is incentivising speculative data centre investment without attaching clear sovereignty conditions; it permits a revolving door between large technology firms and senior policy roles - creating the perception of undue closeness and undermining public confidence in the integrity of decision making - and it has weakened competition enforcement in ways that favour established incumbents.
- But there is a better way. Other European states have begun to reduce foreign infrastructure dependence. These approaches are operationally proven and, in several cases, cheaper. The UK can, and should, also choose to diversify.
- The immediate steps are clear: scrutinise the systems that give foreign firms - particularly hyperscalers - preferential access and influence, back the CMA to act on its own findings under the Digital Markets, Competition and Consumers Act (DMCCA), and use public procurement as a tool to shape the market. That same procurement power should be directed toward building, reserving contracts for British firms, and seeding a domestic

industry that retains value here. Where the UK cannot build alone, it should look to other European states for partnership.

Defining Digital Sovereignty & Mapping Dependencies

Digital sovereignty as we describe it has three interlocking dimensions: sovereign infrastructure, fair procurement, and regulatory independence. All are currently compromised, and each makes the others harder to achieve.

Without sovereign infrastructure, the state cannot maintain critical services in times of pressure. Without fair procurement, domestic firms cannot compete against the hyperscalers — deepening the dependencies. And without regulatory independence, the state cannot enforce the rules that protect either.

Sovereign Infrastructure

Sovereign infrastructure is the UK's ability to develop, deploy, and maintain critical digital technologies without depending on foreign supply chains.

The tech stack is vast, from physical infrastructure to user-facing applications. Cloud infrastructure, sitting in the middle, is a critical layer, and also the most compromised. It is the layer of the tech stack on which many others depend, and where foreign control is most concentrated and therefore riskiest.

The UK public cloud market is substantial and set to grow rapidly. Statista projected revenues of around $35.8bn (~£28bn) in 2025. Yet this market is not a level playing field. Two US firms, AWS and Microsoft Azure, control 60-80% of UK cloud infrastructure, according to the CMA's July 2025 market investigation. Government departments alone spend an estimated £6 billion annually with these providers, a cost that will grow as cloud becomes more central to economic activity.

But the dominance of just two providers raises questions about whether the market structure is conducive to healthy competition. For most cloud customers, switching is rarely realistic: egress fees, lock-in, and multi-year committed spend agreements mean that once a department is embedded, it's costly and difficult to leave. Pricing power sits with the vendor, and the CMA found that Microsoft and AWS have sustained returns substantially above the cost of capital for years - the UK is currently being overcharged by at least £500m a year in the cloud market.

While UK businesses offer alternatives, they face extreme barriers. Former employees of UKCloud (a now-defunct British cloud company) reported to the CMA that hyperscalers exert undue influence over business decisions and government policy through direct access to senior officials — a channel unavailable to domestic competitors. Without direct intervention, a change in market dynamics remains unlikely.

This has implications for the UK's AI strategy, because cloud and AI are inseparable. Virtually all AI applications rely on cloud infrastructure, reinforcing the market power of the same firms. The hyperscalers further entrench their ecosystems by integrating AI directly into existing cloud services. The CMA's investigation into AI Foundation Models concluded that there is a growing presence across the "value chain of a small number of incumbent technology firms, which already hold positions of market power in many of today's most important digital markets, [which] could profoundly shape FM-related markets to the detriment of fair, open and effective competition." They recognise that the same firms have "strong positions in critical inputs", including compute and distribution access points. The government's ambition, laid out in the AI Opportunities Action Plan, to embed AI across public services risks amplifying dependency on US hyperscalers unless deliberately managed otherwise.

Without control over foundational infrastructure, the UK cannot guarantee continuity, security, or integrity in the face of geopolitical or commercial disruption.

Fair Procurement

Procurement is the mechanism that either reinforces or reduces dependency. In the UK, it is currently reinforcing it.

The UK AI Opportunities Action Plan states an intention to foster 'homegrown AI,' yet the government has signed non-binding MOUs with Anthropic, Nvidia, and OpenAI under its guise. These agreements skirt ordinary procurement, with no commitment to publish terms and no indication of competitive tendering. These informal agreements are expansive, giving their signatories significant influence in UK politics and conferring sweeping powers to direct policy.

The mechanics of this approach matter enormously. A DSIT official asserted that a non-binding agreement with Google Cloud involved no direct payment, classifying it as a below-threshold contract exempt from transparency obligations. Under the Procurement Act 2023, below-threshold contracts were intended to give flexibility to award contracts to *British* firms or SMEs. Yet this

appears to be having a perverse result: the largest, best-funded foreign firms are using such agreements to provide 'free' services in exchange for disproportionate access to policymaking. The use of MOUs for cloud services is, according to government guidance, intended to negotiate discounts or "mak[e] sure the contract is with a UK provider", yet all the MOUs with cloud providers listed involve foreign companies.

This is not an accident, but a pattern. As Labour MP Rachael Maskell observed, Palantir offered services to the NHS for £1 during the Covid-19 pandemic. That initial agreement expanded into a £330 million contract, and its MoD contract tripled to £240 million. The entry price is low, but the lock-in price is not.

To compound matters, formal public procurement frameworks are skewed in ways that advantage hyperscalers. Evaluation criteria reward scale and existing integration rather than sovereignty or domestic value. There is no premium for homegrown technology, and the government has limited visibility into its aggregate spend on foreign-controlled Big Tech versus British or European alternatives.

The structural access this deference to Big Tech creates is material. For instance, OpenAI's previous governance lead now serves as AI adviser to the Prime Minister and heads the UK's AI Security Institute. Microsoft UK's chief executive chairs the UK Industrial Strategy Advisory Council while Microsoft simultaneously supplies cloud and productivity software to public organisations. Doug Gurr, former UK Managing Director of Amazon, was appointed Interim Chair of the CMA in 2024 and made permanent in 2026, raising legitimate questions about the regulator's ability to oversee an industry he previously led. Each of these appointments may be individually justifiable. Cumulatively, they create an appearance of institutional capture that is difficult to defend, and that public confidence in independent regulation cannot survive indefinitely.

This is only exacerbated by access and lobbying power. Tech giants outspend domestic competitors by orders of magnitude, effectively buying influence over the legislative agenda before the public debate has even begun. The UK does not publish a lobbying register comparable to the EU's, so the precise figures spent influencing Westminster are unknown. But the EU data is illustrative: analysis by Corporate Europe Observatory and LobbyControl found that the tech industry now spends a record €151 million annually lobbying the EU. Just ten companies account for one-third of that total, with Meta the top spender at €10 million, followed by Microsoft, Apple, and Amazon at €7 million each. The number of tech lobbyists now exceeds the number of MEPs, and Big

Tech averaged three lobbying meetings a day with senior EU officials and parliamentarians in the first half of 2025.

There is no reason to believe the UK picture is materially different — and some reason to think it may be worse, given the absence of equivalent transparency requirements and the placement of former Big Tech executives in key regulatory posts. When domestic competitors are spending a fraction of this and operating without the same access to senior officials, the outcome is not a level playing field.

Regulatory Independence

Regulatory independence is the state's ability to set and enforce law without external constraint. In practice, that independence is constrained when infrastructure is foreign-controlled.

The US has increasingly used trade leverage to undermine UK digital enforcement. Negotiations last summer saw US stakeholders mischaracterise the UK's Online Safety Act and Digital Markets, Competition and Consumers Act as trade barriers. Just this month, President Trump again threatened a 'big tariff' on the UK and to walk back commitments under the trade agreement, should the UK retain its Digital Services Tax on US Big Tech.

A government that depends on foreign infrastructure for core public services may struggle to enforce domestic law against monopolies that hold the keys to its digital economy – at least not without consequences it may not be willing to accept. When states have repeatedly demonstrated a willingness to use their infrastructural leverage to extract concessions or distort law enforcement in other jurisdictions, investment in sovereign technology infrastructure becomes more than a resilience play. It reduces the risk that a government's enforcement decisions (on competition, on data protection, on platform conduct) are held to ransom for unrelated economic or geopolitical reasons.

The Risks of Reliance

Economic Risks

The UK's digital economy is operating, in significant part, as a system of value extraction rather than retention. A substantial share of the value generated here is captured by foreign firms and transferred overseas, rather than reinvested in the UK. This reflects a structural issue: much of our

core digital infrastructure is not domestically owned. As a result, British ideas and talent are often acquired, and while UK citizens' data is monetised, the returns are largely realised offshore.

In doing so, hyperscalers rarely pay their fair share. In fact, analysis by TaxWatch suggests seven major US technology firms generated approximately £60 billion in UK revenues in a single year but paid only £753 million in corporation tax, implying a shortfall of around £2 billion relative to expected liabilities. This is just one small sample of Big Tech firms - the full figure of hyperscaler tax deficit will be much larger.

Data centres, frequently presented as evidence of inward investment, illustrate the next phase of this extractive model. Foreign-owned, foreign-operated, and foreign-profitting, they will process data generated by UK citizens and underpin AI systems central to the UK economy, while revenues are repatriated abroad. Research shows large-scale data centres typically generate fewer than 100 permanent jobs per site once operational. They will also consume an extraordinary share of our already strained energy supply. Data centres account for 2.5% of UK electricity consumption today, a figure expected to quadruple by 2030. British households, already cash-strapped, are set to foot at least part of the bill.

The talent picture is equally concerning. The UK faces brain drain, where skilled workers are absorbed by multinationals and successful startups are acquired, transferring intellectual property (and future value creation) overseas. For instance, analysts have pointed out that there is a "tsunami of overseas acquirers" buying UK firms at a record high. They have found that "overseas buyers have consistently accounted for 40-45% of all tech deals in the UK", though this jumped to 56% of all deals in Q4 last year, the highest on record. While foreign direct investment is often lauded as beneficial to the UK economy, it is also responsible for the loss of economic control. As Viscount Hanworth put it in a recent Lord's debate on foreign direct investment, "we have experienced a loss of economic sovereignty. We no longer own our airports, seaports, energy industry, water industry, rolling stock and much else besides."

Security Risks

The UK's reliance on foreign-owned digital infrastructure creates systemic national security vulnerabilities.

One point of exposure is citizen data. Under the US CLOUD Act, US authorities can compel access to data held by American companies regardless of where it is stored. In 2025, Microsoft

acknowledged before the French Senate that it could not guarantee resistance to a lawful US government request for European data. While tensions have long existed between American security priorities and European privacy protection, several European member states and EU institutions have responded to increasing threats to sovereignty from the current US administration by moving toward sovereign providers. The UK has not. In fact, when asked what assessment it had made of the CLOUD Act's implications for UK government data held by Microsoft, Google Cloud, and AWS, the Department for Science, Innovation and Technology admitted it had made none. This means that sensitive UK data, including NHS records and government communications, sits within potential reach of a foreign state.

This dependence extends into defence. Our 'Cloud Defence: An Exposed European Flank' rates the UK MoD as among the most reliant countries in Europe on US cloud, with over €1.099 billion (£960m) in contracts with Google, Oracle, AWS, and Microsoft. The UK is classified as 'high risk', with critical defence systems either directly contracted to US clouds or lacking effective separation from US-controlled infrastructure.

The prospect of a 'kill switch' threat is becoming more plausible, and governments are beginning to prepare accordingly. Recent years have shown that even allies and close partners will use available leverage when interests diverge, and technology is a key leverage point. The precedents for this are recent and concrete. In March 2025, the Trump administration suspended Ukrainian military access to the Global Enhanced GEOINT Delivery program, cutting off Maxar satellite imagery used to track Russian troop movements in real time as a tool for negotiations. That same year, US sanctions against ICC chief prosecutor Karim Khan resulted in him losing access to his email account (Microsoft has since then denied being responsible for the disruption). The ICC's response was to replace its Microsoft infrastructure entirely with OpenDesk, an open-source European alternative.

But the risk is not limited to the hyperscale cloud providers. The UK's reliance on Palantir Technologies presents a specific and acute risk to sovereignty - particularly for data sovereignty. A US firm with deep ties to the US intelligence community and more recently to ICE raids, Palantir holds significant contracts with the UK Ministry of Defence, the Home Office, the NHS, and, as of early 2026, the Financial Conduct Authority. Palantir's platforms ingest vast amounts of sensitive data through software architecture designed for intelligence fusion and surveillance, where data processing logic remains opaque to UK auditors. With Palantir's CEO openly advocating for the use of AI in warfare and maintaining close alignment with US defence strategy, the firm's integration into

UK critical infrastructure is not a typical vendor relationship. It creates a channel for external influence over UK defence and policing, and a live risk to sensitive citizen data.

Finally, the concentration of critical systems in foreign-owned infrastructure creates above all else a practical operational risk: a single point of failure at the national scale. We witnessed this firsthand when AWS suffered a major outage in 2025, when government websites, emergency services, schools, and banking were disrupted simultaneously. The country and systems that power it were momentarily offline. This could just as easily happen again by accident, or as part of political leverage in the form of a 'kill switch'. Should the US cease its 'special relationship' with Britain, it holds an alarming amount of control over our critical systems. 'Sovereign cloud' offerings from hyperscalers do not resolve this, as the infrastructure remains under their control and subject to their jurisdiction.

Democratic Risks

The platforms through which UK citizens consume news, engage in political debate, and form opinions are overwhelmingly controlled by US-based firms. Consequently, the rules governing the UK's public sphere (what is amplified, what is suppressed, etc) are set by foreign actors and shaped by algorithms designed to maximise engagement and shareholder value. Those algorithms increasingly reflect the political interests of US leadership rather than British democratic norms.

The consequences are already visible in the erosion of social cohesion. Between July and August 2024, a wave of anti-immigrant riots took place across the UK, driven in part by false claims that spread rapidly on social media following the killing of three children in Southport. Ofcom found that illegal content and disinformation spread widely and quickly online, and that the riots demonstrated the role algorithmic recommendations can play in driving divisive narratives during a crisis. Research from LSE found that X amplified the fake news and conspiracy theories that helped fuel the riots, with AI-generated disinformation posts attracting nearly three times the average views of other content. The government could do little to curb it.

The political alignment of Big Tech leadership has become increasingly explicit and increasingly adversarial to democratic interests. Elon Musk, Mark Zuckerberg, and Jeff Bezos attended Trump's inauguration with prominent seats on the platform, for all to see. Musk has gone considerably further in the UK: he expressed support for far-right activist Tommy Robinson and paid his legal fees when Robinson was prosecuted under anti-terrorism law, while in December

2024, discussions took place about a potential donation of up to $100 million to Reform UK, which would have been the largest political donation in UK history.

These are not the actions of neutral technology platforms. They are the interventions of engaged political actors with the power to shape British democracy, and the infrastructure to do it. And because the UK lacks a sovereignty strategy, it is forced to tolerate this interference. Unchecked platform power is a direct threat to democratic resilience, and the UK's structural dependency prevents it from responding with the force the situation demands.

Case Studies

International examples demonstrate that reducing hyperscaler dependency is not only possible but, in many ways, profitable, safer, and a better user experience.

Europe-Wide

- EU Cloud Sovereignty Framework: The European Commission has awarded a €180 million, six-year tender for sovereign cloud services exclusively to European providers: Post Telecom (with CleverCloud and OVHcloud), STACKIT, Scaleway, and Proximus (with S3NS, Clarence, and Mistral). The framework measures sovereignty across eight dimensions, including strategic control, legal jurisdiction, operational resilience, supply chain transparency, and compliance. Four contracts were awarded in parallel to ensure diversification and prevent single-provider dependence.
- EuroStack: Co-signed by over 260 organisations, EuroStack advocates for European-owned technology across the full stack. Its framework promotes 'Buy European' (directing public procurement toward European providers), 'Sell European' (improving visibility and interoperability for European suppliers), and 'Fund European' (strategic public capital directed at sovereign solutions). Its authors frame the current situation as a 'digital colony' where value is extracted rather than created (a diagnosis that applies equally to the UK).
- openDesk: An open source productivity suite developed by Germany's Centre for Digital Sovereignty, openDesk has been adopted by the European International Criminal Court after US sanctions disrupted its Microsoft-hosted communications. This is not a hypothetical risk scenario: it is a precedent that has already been acted upon.

- Eurosky: A FOTI-backed initiative to build European social media infrastructure on the open AT Protocol. Unlike centralised US platforms, it allows users to migrate between providers while retaining their data, structurally preventing lock-in and aligning with European democratic values.
- Sovereign Tech Fund: A public investment initiative supporting open-source infrastructure such as OpenStreetMap and Fedify.

Germany

- Schleswig-Holstein Migration: The German state is migrating 30,000 civil servants from Microsoft Office to European open-source alternatives (LibreOffice, Nextcloud) by 2029, citing sovereignty as a primary driver.

France

- La Suite Numérique: A complete open-source collaboration platform for the public sector, including secure messaging, file transfer, and video conferencing.

Denmark

- Cities like Copenhagen and Aarhus have plans to or have already migrated off Microsoft services, achieving significant cost reductions (e.g., Aarhus reduced software costs by 72% in one department). The national Ministry of Digitisation is phasing out Microsoft products in favour of LibreOffice, driven by cost, competition, and sovereignty concerns.

Austria

- In 2025, Austria accelerated its digital sovereignty agenda, moving 1,200 government staff to Nextcloud, a sovereign platform, while the military has moved 16,000 workstations off Microsoft and onto LibreOffice.

The Netherlands

- The Netherlands has aligned its digital sovereignty strategy with the EU's EuroStack initiative, mandating that new public sector cloud contracts prioritise European providers with verifiable data residency. The government has established a 'Digital Sovereignty Lab' to test and certify open-source alternatives, providing a blueprint for the UK to follow.

Policy Recommendations

Given the depth and scale of the UK's dependence on foreign digital infrastructure, change cannot (and should not) happen overnight. However, there are a number of actions the government can take to move the country *toward* digital sovereignty.

- Require transparency and open competition in public technology procurement. Scrutinise existing MOUs with foreign firms (OpenAI, Anthropic, Nvidia and others) that grant undue influence, data access, or policy sway outside normal procurement rules. Going forward, all technology agreements should be subject to open competitive tendering by default.
- Take action on cloud market dominance. If voluntary commitments suggested by the CMA prove insufficient, the CMA should formally designate hyperscalers (notably AWS and Microsoft Azure) as holding Strategic Market Status. Commitments should also guarantee meaningful interoperability beyond the dominant firms, enabling seamless switching and multi-cloud use with alternative providers, not just hyperscalers.
- Align data centre expansion with measurable UK value creation and retention. Planning consent should be contingent on independently verified evidence that a data centre in this location will deliver net UK economic value, from sustainable employment, to sovereign capabilities and productivity gains, to net positive environmental impacts.
- Cease entering trade agreements that undermine UK regulatory powers or mandate the adoption of foreign technology exports. Empower regulators to intervene against the harmful consequences of Big Tech products irrespective of external threats.
- Restore CMA independence to enforce the DMCCA effectively. Recent interventions show a gap between the stronger remedies suggested in market investigations and the weaker outcomes delivered under DMCCA enforcement. The CMA should be unequivocally empowered by the government to act decisively against anticompetitive behaviour wherever it has demonstrated that intervention is necessary.
- Publish a National Digital Sovereignty Strategy. The UK needs a coordinated, cross-departmental commitment to reducing critical infrastructure dependence and building sovereign alternatives. The strategy should set specific targets with named accountability and regular reporting to Parliament. Measures could include:

- Introducing 'Buy British' procurement approaches to industrial strategy by introducing non-price criteria (sovereignty, resilience, data residency) for cloud and AI procurement.
- Publishing a consolidated register of technology contracts and MOUs and an annual breakdown of spend by provider nationality so Parliament can track progress toward domestic diversification.
- Commissioning an audit of UK MoD cloud dependencies to understand genuine risk levels. Develop a phased migration plan for critical systems.
- Reserving portions of departmental budgets for domestic technology providers and prioritising open source solutions.
- Establishing a UK Tech Sovereignty Fund, modeled after the European approach. Use this to focus public investment on building an open, interoperable tech ecosystem that reduces reliance on hyperscalers and enables domestic firms to compete on fairer terms. This means prioritising open standards, portability, and infrastructure so companies can switch providers, combine services, and scale without being locked into a single vendor. The goal is not to recreate hyperscaler dominance in a UK form, but to create a resilient, multi-provider market where firms can build viable products, compete effectively, and retain more value in the UK economy.

Conclusion

The UK's digital economy is a genuine strength, but its current structure leaves the country strategically exposed. Too much of the infrastructure, data, and platform power we rely on sits beyond our control, leaving value on the table and exposing our economy, our security, and our democracy to avoidable risks.

Without intervention, this trajectory will continue. The UK will remain a place where innovation happens, but value is captured elsewhere, where infrastructure is hosted but not governed, and where markets are participated in, but not shaped.

Digital sovereignty offers a better path. It is not about isolationism or protectionism, but about rebalancing control – ensuring the UK can operate its critical systems, enforce its own laws, and negotiate from a position of strength rather than dependence.

To move us closer toward a digitally sovereign Britain, policymakers should focus on practical steps: using procurement to build domestic capability, enforcing competition law to open markets to challengers, and investing in sovereign infrastructure to diversify and reduce risk. Done well, this revived, sovereign ecosystem can deliver sustainable economic growth, stronger security, and a more resilient democracy.

And in building that ecosystem, the UK need not look to replicate Silicon Valley. It can choose a more balanced model – drawing on what European neighbours are already building, while charting a course that reflects its own strengths and interests.

About FOTI

The Future of Technology Institute (FOTI) is a pan-European think-and-do tank dedicated to building a more secure, prosperous, and fair technology future for Europe. FOTI provides research and insights to European leaders aimed at opening market chokepoints and developing sovereign alternatives. The institute is non-partisan and accepts no corporate funding.