

## Sovereignty by design

Security, resilience, and growth

July 2026

Matthew Feeney



## ABOUT RE:STATE

*Re:State* is established as the leading Westminster think tank for public service reform. We believe that the State has a fundamental role to play in enabling individuals, families, and communities to thrive. But our vision is one in which the State delivers only the services that it is best placed to deliver, within sound public finances, and where both decision-making and delivery is devolved to the most appropriate level. We are committed to driving systemic change that will deliver better outcomes for all.

We are determinedly independent and strictly non-party in our approach. This is reflected in our cross-party Advisory Board and our events programme which seeks to convene likeminded reformers from across the political spectrum.

*Re:State* is a registered charity, the Re:State Trust Ltd, charity no. 1103739.

## ABOUT RE:IMAGINING THE STATE

After a decade of disruption, the country faces a moment of national reflection. For too long, Britain has been papering over the cracks in an outdated social and economic model, but while this may bring temporary respite, it doesn't fix the foundations. In 1942 Beveridge stated: "a revolutionary moment in the world's history is a time for revolutions, not for patching." 80 years on, and in the wake of a devastating national crisis, that statement once again rings true. Now is the time to fix Britain's foundations.

*Re:State's* programme, 'Re:Imagining the State', puts forward a bold new vision for the role and shape of the State. One that can create the conditions for strong, confident communities, dynamic, innovative markets, and transformative, sustainable public services.

## ACKNOWLEDGEMENTS

*Re:State* would like to thank BT for kindly supporting this paper.

### Interviewees

We would like to thank all three interviewees for giving their time and candid insights to support this research paper. The list of interviewees is as follows:

- Colin Bannon, Chief Technology Officer, BT
- Alvaro Garcia Delgado, Counsellor for Digital Affairs and Space Policy, Delegation of the European Union to the United Kingdom
- Doniya Soni-Clark, Associate Director - Public Affairs, techUK
- Will McGarrigle, Head of Government Affairs, UK & Ireland, Cisco

The arguments and any errors that remain are the authors' and the authors' alone.

# Table of contents

|                                               |           |
|-----------------------------------------------|-----------|
| <b>1. INTRODUCTION .....</b>                  | <b>5</b>  |
| <b>2. THE STATE OF AFFAIRS.....</b>           | <b>7</b>  |
| 2.1 The British Government's approach.....    | 8         |
| <b>3. POLICY IN THE STACK.....</b>            | <b>11</b> |
| 3.1 The stack meets digital sovereignty ..... | 11        |
| 3.2 Full stack sovereignty risks.....         | 17        |
| <b>CONCLUSION.....</b>                        | <b>20</b> |

---

# Ideas for a digital sovereignty policy

**Idea 1:** Establish a sovereignty framework that emanates from the Cabinet Office or the Department for Science, Innovation & Technology that explains the requirements for the full range of government digital services. The framework would also set out clear guidelines related to the use of foreign digital services and the degree of insulation from foreign jurisdictions that is necessary.

**Idea 2:** Develop a tiered framework of digital government systems that ranks systems in relation to national security, law enforcement, and critical infrastructure and public services.

**Idea 3:** Clarify sovereign control point obligations for the day-to-day operation of digital government services, such as encryption-key control and domestic technical capabilities.

**Idea 4:** The Government should create a strategic programme for prioritising grid connections for significant datacentre projects, including considering additional fees or auctioning to provide further investment, and prioritising projects based on their relevance to technology sovereignty under this framework. It should prioritise capacity for particularly sensitive systems and connections related to AI Growth Zones.

**Idea 5:** The Government should ensure that the upcoming National Policy Statement for Data Centres outlines when certain data centres can be considered Nationally Significant Infrastructure Projects (NSIPs), a designation currently associated with power stations, airports, railways, and water management. The NSIP designation should be most strongly considered for data centres above a high energy capacity threshold and those aimed at hosting data concerning national security, critical infrastructure, and law and order.

**Idea 6:** Government should define DCs as a “critical national priority” in the way that low-carbon infrastructure is defined both in the National Policy Statement, and the National Planning Policy Framework. This would ensure it is given strong planning policy support. While pursuing this policy change the Government must be mindful of environmental concerns as well as the role of environmental considerations under the current policy framework. Relatedly, the Government should implement a reform proposed in the Fingleton Review amending the cost cap for judicial reviews and restrict legal challenges to Nationally Strategic Infrastructure Projects (NSIPs).

**Idea 7:** The Government should require plans for critical systems so that government systems continue to operate in the event of an attack, telecommunications disruption, the collapse of a vendor, or if access to data is otherwise disrupted. These plans should include drills and exercises, data restoration and backup plans, and naming specific officers responsible for data loss.

---

# 1. Introduction

Two features of the world present growing challenges to British technology policy: 1) intricate global supply chains underpin the creation of devices that run the modern economy, and 2) geopolitical instability risks disruption to these supply chains. These two factors combined have prompted some lawmakers and policy experts to argue for ‘digital sovereignty’ in an attempt to protect critical British technology from exogenous geopolitical shock.

While ‘digital sovereignty’ lacks a universal or agreed upon definition, most discussions of the concept focus on nation state control and regulation of significant portions of digital assets and infrastructure in a way that preserves security, resilience, and economic independence.

The term is best understood as a spectrum between “full sovereignty” (which assumes total control of the production, transport, and use of all digital assets) and “no sovereignty” across four pillars: data sovereignty (concerning data residency, transit, and encryption); operational sovereignty, which governs who has access to data and data management tools; technology sovereignty, which provides controls and limitations on the range of technologies needed in a system; and jurisdictional control over which governments and regulators can legally access data and networks.

Given the globalised state of modern markets, it is unrealistic to assume that the UK can close itself off from the rest of the technological world and build an entirely home-grown technology stack from chips to apps. But nor is it realistic for the Government to play a passive role and accept the security and sufficiency risks associated with being heavily reliant on overseas companies for digital assets and infrastructure.

Instead, the Government must take a risk-based approach to the technologies it must control, those which it does not control, and the elements of the technology stack where it needs some control and sovereignty but not full end-to-end control. Crucially, this risk-based approach needs to be clearly articulated for both public sector organisations and private companies so both can make planned investments based on a shared understanding of the policy. In addition, the Government should undertake reforms aimed at making it easier for private companies to build critical digital infrastructure, such as data centres.

The Government currently lacks a comprehensive approach to digital sovereignty. The lack of clarity could undermine innovation and foreign investment. A clear digital sovereignty policy would give suppliers and investors greater confidence. Alongside this policy certainty, the Government should implement a set of supply-side reforms to make it easier for both foreign and domestic companies to build in Britain – so that planning, grid connectivity, and energy supply are not barriers to infrastructure being built. The more companies of any kind that can build infrastructure in the UK, the more of a sovereign stake Britain has in the global technology economy.

Discussions about digital sovereignty present risks as well as opportunities. A digital sovereignty policy that does not account for the United Kingdom’s comparative advantages as a global trading nation and is not realistic about the State’s capacity to transform the economy risks hampering innovation and growth. But a policy that accounts for these realities while also providing robust and clear guidelines to government and the private sector related to security, procurement, and data management could contribute to the economic growth successive governments have been seeking.

This paper analyses the state of the hardware supply chain, the arguments for robust digital sovereignty, and the implications of different policy options. It then provides a categorisation scheme for the Government to employ that would allow for clarity on procurement and security requirements for government digital systems. This approach considers the relative security and privacy risks associated with a wide range of government services without insisting on a 'full stack' sovereignty approach. It also allows the government to enjoy strategic autonomy over key systems and processes.

Finally, the paper presents policy recommendations that would allow for the government to double down on the UK's comparative advantages, prompt more valuable domestic digital infrastructure construction, provide the private sector with clear mandates and procurement rules, and set out viable strategies so that departments can help to protect British security.

---

## 2. The state of affairs

Digital infrastructure is the bedrock of the modern economy. But the policy debate about how to use and regulate digital technology is often divorced from the material and economic foundations that infrastructure relies on.

Although many of the public's everyday experiences with technology – messaging a friend, hailing a rideshare, scrolling social media, tracking a delivery, retrieving a work email – give the illusion that the device in our hands houses all of the relevant data, that is not in fact the case. Much of this data, and the computational power to process it in different ways, is housed in data centres across the world. 'The cloud' is a popular metaphor, but in reality, it refers to out-of-sight data centres in physical locations containing troves of servers connected to our devices via the internet.

Data centres around the world process troves of information, and the location of this data processing often bears little relation to the location of the people or services associated with the data. When a Dutch grandmother living in Amsterdam emails her grandson in Japan using Gmail, it is possible that the content of the email travels within Google infrastructure across the world rather than in the physically straightest route across fibreoptic cables. It is also possible that an email sent between two people sitting in the same city can take an international route between sender and recipient.

Despite being ubiquitous and necessary features of the global economy, the chips that form the nervous systems of almost every modern electronic device are the result of complex international supply chains. Specific gases, chemicals, lasers, wafers, high-purity materials, and tools are required to impose specific patterns shorter than the wavelength of visible light onto material in a process with a margin of error measured in nanometres. Factories involved in this supply chain cost billions of pounds and take years to build.

Debates about digital sovereignty occur amid these intricate supply and communication chains. Contemporary concerns about Chinese and Russian cyberattacks, as well as increased concern about the potential weakening of European countries' relationship with the United States have all prompted discussions about how the British Government can be an attractive home for digital investment, while also ensuring a suitable degree of autonomy and security. At the same time, lawmakers are seeking to find ways to make the UK an attractive option for investors seeking robust technology policies that allow for strategic autonomy and resilience.

These debates are taking place at a time when global companies and services are dominant and intricately linked to the British government and British companies. In July 2025, the Competition and Markets Authority (CMA) published its final decision following an investigation into cloud services.<sup>1</sup> It found that the Infrastructure as a Service (IaaS) market, which provides customers with shared computing resources, is dominated by Microsoft and AWS, which each have a market share of between 30 to 40 per cent.<sup>2</sup> US-based companies also play a significant role in the market for Platform as a Service (PaaS) products, which allow customers to use the cloud to run, test, and develop applications.<sup>3</sup> According to the CMA, Microsoft enjoys a 20 to 30 per cent PaaS market share while AWS' share is 10 to 20 per

---

<sup>1</sup> *Cloud Services Market Investigation: Summary of Final Decision* (Competition and Markets Authority, 2025).

<sup>2</sup> Ibid.

<sup>3</sup> Ibid.



cent.<sup>4</sup> Other companies such as Alphabet, Oracle, and IBM also play significant roles in the IaaS and PaaS markets.<sup>5</sup>

In 2023, the Office of National Statistics estimated that 69 per cent of British firms with at least 10 employees use cloud computing or cloud-based apps.<sup>6</sup> Given US companies' dominance in the cloud computing, smartphone, and router markets, it is not an exaggeration to say that a significant portion of the British economy relies on US technology services.<sup>7</sup>

A number of geopolitical events and domestic developments in the United States have prompted the UK and other traditional allies of the US to consider the effects of this reliance on American technology. At the same time, Chinese espionage operations have renewed debates on the private sector and public sector use of hardware (such as that made by Huawei) developed in China. The Chinese government's foreign policy is also a concern. Taiwan is home to Taiwan Semiconductor Manufacturing Company (TSMC), which commands a significant majority of the semiconductor foundry market. If China were to invade Taiwan or otherwise disrupt its trading capabilities it would have a devastating effect on the world's technology markets.

In June 2026, the US Government, citing national security concerns, issued an export control aimed at prohibiting any foreign national from using Anthropic's Mythos 5 and Fable 5.<sup>8</sup> Anthropic ceased making the models available to anyone anywhere in the world as a result.<sup>9</sup> The US Government reversed course a few weeks later.<sup>10</sup> The US Government unilaterally issuing an effective ban on some of one of the most powerful AI models, including those many British citizens had begun to use, raises concerns about the UK's reliance on American tools.

Regardless of specific concerns about the risks generated by national actors, interest is expanding in the potential for a more systematic approach to British digital sovereignty strategy, not least because of the potential for a clear policy to provide the regulatory certainty required for increased investment into long-term digital assets and infrastructure.

## 2.1 The British Government's approach

In comments during an oral evidence session with the Joint Committee on Human Rights, Parliamentary Under-Secretary of State for AI and Online Safety Kanishka Narayan laid out the three pillars that he believes are the necessary conditions for technological sovereignty: 1) having enough hardware and infrastructure material, most notably chips, 2) having a diversity of supply of inputs, and 3) 'Build British' so that "we have the full-fat version of sovereign capability here in parts of the stack".<sup>11</sup>

<sup>4</sup> *Cloud Services Market Investigation: Summary of Final Decision*.

<sup>5</sup> *Management Practices and the Adoption of Technology and Artificial Intelligence in UK Firms: 2023* (Office for National Statistics, 2025).

<sup>6</sup> *Management Practices and the Adoption of Technology and Artificial Intelligence in UK Firms: 2023*.

<sup>7</sup> Ibid.

<sup>8</sup> Hadas Gold, 'Anthropic Suspends All Access to Mythos Model after US Government Bans Foreign Nationals Use', *CNN*, 13 June 2026.

<sup>9</sup> 'Statement on the US Government Directive to Suspend Access to Fable 5 and Mythos 5', Announcement, Anthropic, 12 June 2026.

<sup>10</sup> Osmond Chia, 'Anthropic Says US Lifts Export Ban on Its Advanced AI Tools', *BBC News*, 1 July 2026.

<sup>11</sup> *Uncorrected Oral Evidence: Human Rights and the Regulation of Artificial Intelligence*, HC 1262 (Joint Committee on Human Rights, 2026), Q105.

A speech delivered by the Department for Science, Innovation & Technology (DSIT) Secretary Liz Kendall in April 2026 failed to provide much more clarity.<sup>12</sup> According to Kendall, AI sovereignty is not about isolation, but about “reducing over (sic) dependencies and increasing resilience in key national strategic priorities” by backing more British AI companies and working with international partners on AI standards.<sup>13</sup> While it would be a mistake to conflate AI sovereignty and digital sovereignty, AI sovereignty policy and digital sovereignty policy have overlapping concerns such as resilience, control, and security.

While the Government does not have a comprehensive view of sovereignty, it is clear that the Government is trying to provide a sovereignty vision that embraces markets and trade with necessary guardrails while rejecting outright protectionism. The challenge the Government faces is resolving the tension between embracing increased domestic capability and portraying the UK as an attractive venue for global investment with sovereignty controls in place.

On chips, the UK occupies a small but specialised section of the global semiconductor market. Companies in countries such as South Korea and Taiwan are central players when it comes to mass semiconductor fabrication, and American companies are working hard to boost American fabrication capacity. Companies in other countries, such as the Netherlands, Japan, and China also play significant roles. It is unrealistic to believe that the UK will be able to catch up to these companies on mass semiconductor fabrication any time soon.

However, the UK is well placed in some key areas. As the then government pointed out in 2023, the UK enjoys strengths in IP and design as well as compound semiconductors and R&D.<sup>14</sup> The South Wales compound semiconductor cluster, known as CSconnected, is the world’s first compound semiconductor cluster that connects high-quality research with construction facilities and wafer fabrication capabilities.<sup>15</sup> South Wales is also home to IQE, a compound semiconductor company.

Elsewhere in the UK research and development clusters are found in and around Oxford, Cambridge, Bristol, and London. When it comes to intellectual property and design, British companies such as Arm, XMOS, and Aion Silicon (previously Sondrel) play important and internationally recognised roles in chip design.

There are presently efforts in the UK to boost domestic AI chip manufacturing, a market currently dominated by the US firm Nvidia. Fractile, a UK-based chip designer focuses on reducing the energy intensive and time-consuming hurdles that occur when many chips designed before the proliferation of Large Language Models (LLMs) move data from memory to compute.<sup>16</sup> Fractile chips will reportedly not be ready for data centre deployment until next year, but if its claims to be able to run LLMs up to 100 times faster than existing models while reducing operating costs by up to 90 per cent are accurate, its chips promise to be one of the most significant semiconductor developments in recent years.<sup>17</sup>

<sup>12</sup> The Rt Hon Liz Kendall, ‘Speech: Rebuilding Britain for the New World’, Royal United Services Institute (RUSI), 28 April 2026.

<sup>13</sup> Ibid.

<sup>14</sup> ‘National Semiconductor Strategy’, Policy Paper, Department for Science, Innovation and Technology, 19 May 2023.

<sup>15</sup> ‘Who We Are’, CSconnected.

<sup>16</sup> Saskia Koopman, ‘Fractile vs Nvidia: Can a UK Startup Undercut AI’s Chip Darling?’, *City A.M.*, 6 May 2026.

<sup>17</sup> David Manners, ‘UK AI Chip Startup in Talks to Raise \$200m’, *Electronics Weekly*, 7 May 2026.

The Government has taken some steps to signal a more robust “Build British” approach.<sup>18</sup> Some of these predate the present-day concerns widely cited in modern sovereignty debates. In 2015, the British company Ark Data Centres and the Cabinet Office established Crown Hosting data centres, a joint venture that would provide public bodies with “a physical space to host their computer servers and systems that aren’t in the cloud”.<sup>19</sup> The latest framework agreement for the venture states that the venture is 74.9 per cent owned by Ark Data Centres and 25.1 per cent owned by government.<sup>20</sup> The venture allows for many public bodies such as NHS trusts as well as some local authorities to rent server and connectivity services. This ensures that departments do not need to build and maintain their own servers. The venture is not only convenient but a money saver, with Crown Hosting reporting billions of pounds worth of savings since 2015.<sup>21</sup>

Yet while Crown Hosting shows one way for government to work with the private sector on data storage, it is important to place the initiative in the broader data centre environment. According to Crown Hosting, “only around 3 per cent of on-premises IT currently sits in Crown Hosting”.<sup>22</sup> As noted above, a significant portion of government data is housed, shared, and protected by US-based hyperscalers. But it would be a mistake to pursue policies that consider the use or housing of hyperscaler services and infrastructure as incompatible with a digital sovereignty agenda. With the right policies and controls in place, foreign hyperscalers have the potential to play an important role in a digital sovereignty agenda.

The Government has made other policy decisions consistent with a “Build British” goal.<sup>23</sup> In April 2026, the Government announced Sovereign AI, a £500 million fund dedicated to investment in UK-based AI companies.<sup>24</sup> These efforts may well yield results that will allow the UK to more robustly deploy domestic AI skills and products, but it is too early to make that assessment.

Now is an ideal time for the Government to supplement its AI investment plans and sovereignty rhetoric with an approach to digital sovereignty that seeks to provide policies for the full stack. The Government should implement policies that acknowledge the state of global supply chains, the UK’s comparative advantages, and the diversity of risks facing the UK. Such policies would boost strategic autonomy by establishing clear tiers of government digital services and products separated by their importance to national security, critical infrastructure, and public services.

---

<sup>18</sup> *Uncorrected Oral Evidence: Human Rights and the Regulation of Artificial Intelligence*, HC 1262.

<sup>19</sup> ‘Government Creates New Business to Save up to £105 Million in IT Costs’, Press Release, HM Government, 19 March 2015.

<sup>20</sup> ‘CROWN HOSTING DATA CENTRE COLOCATION SERVICES: Framework Agreement with Crown Hosting Data Centres Limited’, Crown Commercial Service, July 2020.

<sup>21</sup> ‘Crown Hosting’, NHS England, NHS England, 29 January 2026.

<sup>22</sup> ‘Where Does Your IT Live? Moving beyond Server Rooms to Smarter, Greener Estates’, 15 October 2025.

<sup>23</sup> *Uncorrected Oral Evidence: Human Rights and the Regulation of Artificial Intelligence*, HC 1262.

<sup>24</sup> Sam Trendall, ‘Seven AI Firms Receive Support via New Government Tech Venture Capital Unit’, *Public Technology*, 16 April 2026.

## 3. Policy in the stack

Most digital technologies can be understood as fitting into different parts of the ‘stack’, a metaphor describing where a particular application, cloud service, piece of infrastructure, or model fits in relation to others. Many discussions on digital sovereignty hinge on how public policy should apply within the stack which underpins cloud computing, AI, and the Internet. The metaphor is helpful in part because it helps illustrate the risks, opportunities, and trade-offs associated with control and regulatory leverage at each level of the stack.

At the bottom of the stack are its physical building blocks: the chips and processors. The next level includes pieces of infrastructure such as servers, data centres, energy connectivity hardware, and under sea and over land fibre-optic cables. Cloud services and AI models sit at the layer above this, as do databases and Application Programming Interfaces (APIs). Machine learning and tool development occur in the next layer, where foundation models and model deployment tools sit.

The final application layer, which is where the vast majority of users interact with the stack, includes the interfaces customers use to access apps and websites. In this layer, the UK enjoys many home-grown competitive players such as Wise, Rightmove, and Monzo.

Many technology companies based in the UK are also involved in providing or supporting government services as part of the application layer. The security and resilience of a company such as Rightmove raises different questions than those raised by a technology company that lists private sector and government entities as clients.

If a company provides the public sector with an application to boost productivity such as a DWP chatbot, Home Office visa application tracker, or portal for Ministry of Defence procurement applications, then there are privacy and security concerns at play even if the concerns are higher in the stack than the hardware infrastructure.

Any sovereignty policy that is designed to provide security, regulatory stability, and opportunities for investment and growth must consider the diverse ways in which technology companies interact across the stack and the diversity of their customers. Some companies will rely almost exclusively on app-level maintenance and management because they rely on their customers using a mobile app.

Others provide hardware and software products to private sector customers as well as government services. Given this diversity, digital sovereignty policy must consider the sensitivity of particular government services while also acknowledging which layers of the stack affect different technology companies. This is especially important given that many services often rely on cloud services located in foreign jurisdictions.

### 3.1 The stack meets digital sovereignty

The stack should inform a digital sovereignty policy because it provides lawmakers with a framework that helps gauge the security, privacy, and economic risks associated with different portions of the digital infrastructure. But before mandating specific technologies and behaviours, the Government must set out a clear digital sovereignty policy in order to provide investors with a clear set of principles and objectives.



To that end, the Government should establish a sovereignty framework, produced by either the Cabinet Office or DSIT. The lack of clarity within the digital sovereignty debate is one of its most notable features – the debate is almost entirely abstracted from specific technologies and the public sector’s risk appetite at each level. The lack of clarity is also likely to be one of the digital sovereignty debate’s most costly features. At a time when hyperscalers are looking around the world for investment and growth opportunities, and domestic operators are hungry for predictable conditions within which to make plans for growth, regulatory clarity and predictable rules could be highly valuable.

One of the Government’s key roles within digital sovereignty policy is to provide one central framework of definitions and clarifications. While providing civil servants and regulators with clear guidance, the framework would also give investors and developers a welcome set of predictable, stable, and clear guidelines necessary for reliable investment and economic growth.

The framework should explain the requirements for the full range of public sector digital services. It should also set out clear guidelines related to the use of foreign digital services and the degree of insulation from foreign jurisdictions that is necessary.

The Government should provide a clear set of requirements that digital service vendors must satisfy to be considered for purchase or use by government. The first step of this process would be to consolidate the currently dispersed guidance and codes that govern how the government buys and builds technology.<sup>25</sup>

The government should also require that vendors designing, building, and supporting the most sensitive systems have extra obligations associated with future cost pricing, interoperability, and data restoration exercises. It is critical that the government have a full understanding of the pricing and reliability of systems critical to public services and national security.

A tiered approach to determining the sensitivity of a system would help the government assess what obligations are appropriate. The following system would achieve that goal:

**Tier 1:** Low-risk software that is used to organise events, schedule communications, or collect feedback. Image editing tools, surveys and feedback polls, and social media scheduling programmes would be included in this tier.

**Tier 2:** Important government systems that are not associated with critical infrastructure, national security, healthcare, welfare, or law enforcement. Examples of such systems include the Civil Service’s recruitment website, internal department wikis and customer relationship management tools. An archive on ministerial speeches and statistical bulletins would also appear in this tier.

**Tier 3:** Systems associated with important public services such as the NHS, DWP, HMRC, and some local authority systems where failure would be harmful to individuals but are not primarily associated with national security, law enforcement, or critical infrastructure.

---

<sup>25</sup> ‘Make Use of Open Standards’, Guidance, Government Digital Service and Central Digital and Data Office, 6 November 2017; ‘The Technology Code of Practice’, Government Digital Service and Central Digital and Data Office, 14 July 2021; ‘G-Cloud Buyer’s Guide’, Guidance, Crown Commercial Service, 24 September 2013; ‘API Technical and Data Standards’, Guidance, Government Digital Service and Central Digital and Data Office, 7 February 2018.

**Tier 4:** Critical infrastructure, national security, and law enforcement systems. Tier 4 would include energy and water systems as well as specific systems associated with the Home Office, the Armed Forces, the Ministry of Justice, and the Secret Intelligence Service.

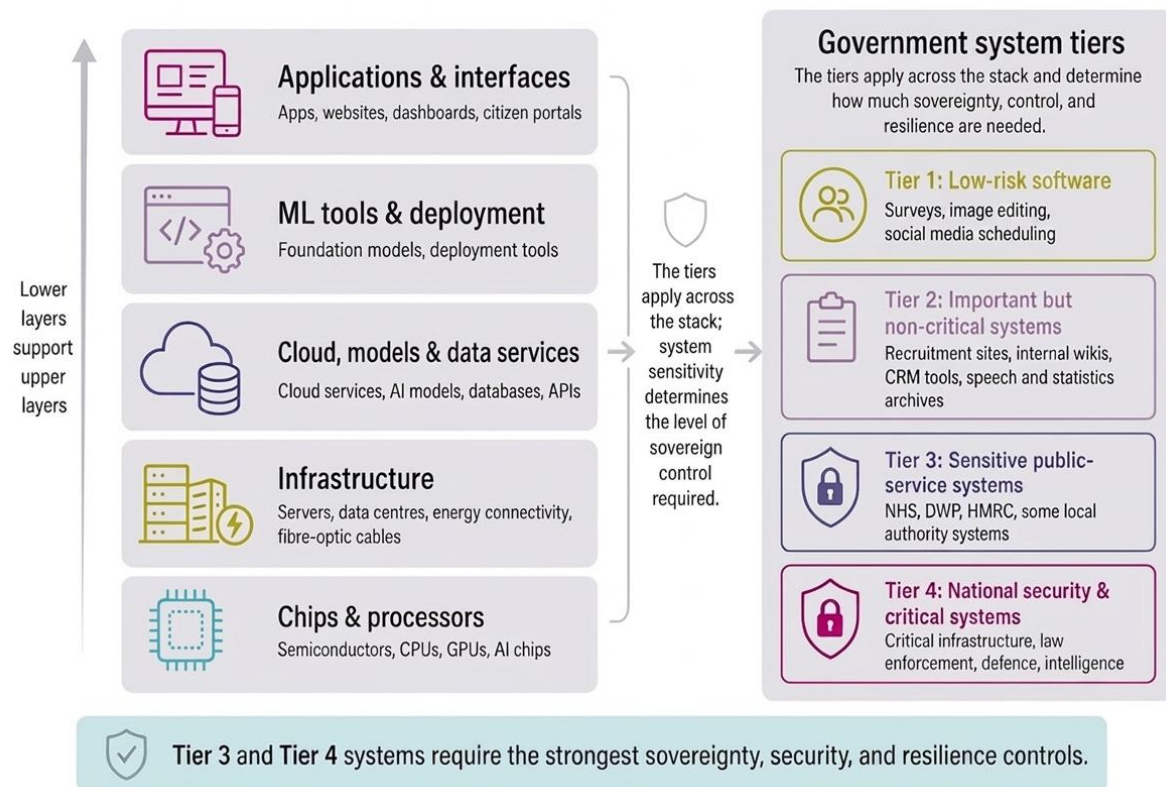
**Idea 1:** Establish a sovereignty framework, produced by the Cabinet Office or DSIT, that explains the requirements for the full range of government digital services and sets out clear guidelines related to the use of foreign digital services and the degree of insulation from foreign jurisdictions that is necessary.

**Idea 2:** Develop a tier framework of digital government systems that ranks systems in relation to national security, law enforcement, and critical infrastructure and public services.

**Idea 3:** Clarify sovereign control point obligations for day-to-day operation of digital government services, such as encryption-key control and domestic technical capabilities.

Tier 3 and Tier 4 systems should be the focus of specific security and control requirements. These requirements need not mandate that these systems be British or built by the government. Large global hyperscalers such as Google and Microsoft do offer sovereign products that allow customers to retain control over data flows and access. But the government must outline what controls Tier 3 and 4 system operators need to have over sovereign products before deploying them. The sovereign products offered by hyperscalers differ in capabilities and security options, and some may not be suitable for some Tier 3 and Tier 4 systems.

Figure 1: The digital stack



Source: Author's illustration via Gemini

For systems in these tiers, government must not enter into an agreement without being able to verify that it will have control over access to data as well as exclusive access to encryption keys. In addition, government must be able to ensure that there is a suitable supply of UK-based technical expertise necessary for ongoing operational maintenance. These policies reduce the risk of foreign governments accessing sensitive data without the consent of the British government.

It is important that control point policy is also linked to a requirement for government to assess the access to data that may be permitted due to jurisdictional issues. For example, the government must continue to assess how much sensitive data associated with British citizens could be exposed to the US government if it is housed in data centres owned by a US-based company.

Next, the Government should develop plans for boosting state capacity and domestic innovation by pursuing supply-side reforms that would enable the private sector to more easily build and develop the infrastructure necessary to boost domestic compute and digital innovation. The UK is not as attractive as it could be to foreign technology companies or investors who could support the growth of domestic competitors thanks to a range of policy decisions made by successive governments. Among the most notable are policies affecting energy and planning.

The UK's industrial electricity costs are among the highest in Europe and well above the International Energy Agency (IEA) average.<sup>26</sup> These costs affect the UK's domestic technology industry in a number of important ways. Data centres are large industrial buildings that require significant land and electricity. Reducing the costs of data centre energy consumption while also lowering barriers to building data centres would help make the UK more attractive to foreign investors.

There are changes the Government could make in order to improve the state of the UK's energy grid and the availability of grid connections. Grid connections in the UK occur on a "first come first serve basis".<sup>27</sup> This unfortunately means that some of the connections necessary for critical services, such as datacentres, are not always met. The Government is aware of this issue and is taking steps to increase data centre connection speed, with the Office of Gas and Electricity Markets (Ofgem) having consulted on ideas to reduce the delays earlier this year.<sup>28</sup>

Several potential solutions have been discussed, including an auction system, introducing a deposit and fees regime, and amending legislation from the 1980s so that customers, such as companies running datacentres, know that they can run their own high voltage connections to substations.<sup>29</sup>

Given the variety of policy options available, the Government should create a strategic programme to prioritise grid connection for significant datacentre projects, bringing together multiple different options for reducing the grid delays for datacentre connections. This should include considering additional fees or auctioning connections to provide further investment, and prioritising projects based on their relevance to technology sovereignty under this framework.

Among the policies the Government should implement is allowing data centres above a certain national significance threshold (defined by required energy capacity) or which have dedicated hosting capacity reserved for Tier 3 and Tier 4 systems to use a Development Consent Order. This would allow the government to categorise certain data centres as Nationally Significant Infrastructure Projects (NSIPs), a designation currently associated with power stations, airports, railways, and water management.<sup>30</sup> The NSIP designation would allow for the streamlining of data centre construction approval and send a clear signal to investors that the UK is keen on boosting its digital infrastructure.

Last October, the Government made the welcome change to allow for applicants wishing to build laboratories or data centres under the NSIP designation, to ask the Secretary of State for an expedited process.<sup>31</sup> However, the NSIP designation is still discretionary. The Government does have the opportunity to make the NSIP designation for data centres above

<sup>26</sup> 'International Non-Domestic Energy Prices', Statistical data set, Department for Energy Security and Net Zero, 28 May 2026; Hannah Smith, *Does the UK Have the 'most Expensive' Electricity in the World?* (Full Fact, 2025).

<sup>27</sup> Robert Boswall, 'The Value of Connection Grid: Connection Auctions', Substack, Robert Boswall, 2 April 2026.

<sup>28</sup> 'Call for Input: Demand Connections Reform', Ofgem, 13 February 2026.

<sup>29</sup> Boswall, 'The Value of Connection Grid: Connection Auctions'; Ed Hezlet and Lucy Shaw, 'Speeding up Grid Connections to Lower Bills and Deliver Growth', Report, Centre for British Progress, n.d.

<sup>30</sup> 'National Infrastructure Planning: Data Centres', Written questions, answers and statements, House of Commons, 15 October 2025.

<sup>31</sup> 'National Infrastructure Planning: Data Centres'.



a certain energy capacity automatic and should make that intention clear in its upcoming National Policy Statement for data centres.<sup>32</sup>

Policy recommendations related to a comprehensive overhaul of the British planning and energy policies are beyond the scope of this paper. But it is nonetheless worth emphasising that a robust sovereignty policy aimed at ensuring strategic autonomy will be of limited reassurance to investors or lawmakers if it is not accompanied by policies that will make it easier to build, pay for, and maintain the data centres necessary for offering the public and the government sovereign options.

We have already seen regulatory uncertainty and high energy costs deter significant data centre plans. For example, in April 2026 OpenAI announced that it was pausing a multi-billion-pound sovereign compute data centre project in the UK, citing energy prices, grid connections, and regulation (especially related to copyright and intellectual property) as the motivating reasons.<sup>33</sup> This is deeply concerning when the aim is to boost the UK's sovereign capacity, as well as drive growth.

Comprehensive planning and energy reform will be economically and politically costly, but the government should consider the significant benefits the UK would reap if it were internationally known for a clear digital sovereignty policy and its openness to large digital infrastructure projects. As the OpenAI news shows, US companies are keen to build in the UK. This as well as the ability of domestic UK technology companies to more easily build data centres, labs, and other buildings would boost the UK's competitiveness and opportunities for British-grown innovation.

**Idea 4:** The Government should create a strategic programme for prioritising grid connection for significant datacentre projects, including considering additional fees or auctioning to provide further investment, and prioritising projects based on their relevance to technology sovereignty under this framework. It should prioritise capacity for particularly sensitive systems and connections related to AI Growth Zones.

The Government should develop plans for boosting state capacity and domestic innovation by pursuing supply side reforms that would enable the private sector to more easily build and develop the infrastructure necessary to boost domestic compute and digital innovation.

Finally, it is essential that the Government makes critical British digital systems sufficiently resilient to cyberattacks, telecommunication breakdown, natural disaster, terrorism, sanctions, legal action, or the breakdown of a vendor-government relationship. A government implementing control point obligations outlined above provides reassurance for day-to-day operation, but it is also necessary for a comprehensive digital sovereignty policy to address data access in the wake of an attack or other event resulting in potential data loss.

In order to prepare for such risks, the Government should develop resilience and security policies that ensure preparedness. These include mandating regular drills and exercises for data loss scenarios, developing backup and restoration plans, and ensuring that each Tier 3 and Tier 4 system has designated officers responsible for acting during a data loss emergency.

<sup>32</sup> Ibid.

<sup>33</sup> Ben Craske, 'Stargate UK: Why Is OpenAI Halting Its AI Data Centre Deal?', *Data Centre Magazine*, 10 April 2026.

**Idea 5:** The Government should ensure that the upcoming National Policy Statement for Data Centres outlines when certain data centres can be considered NSIPs, a designation currently associated with power stations, airports, railways, and water management. The NSIP designation should be most strongly considered for data centres above a high energy capacity threshold and those aimed at hosting data concerning national security, critical infrastructure, and law and order.

**Idea 6:** Government should define DCs as a “critical national priority” in the way that low-carbon infrastructure is defined both in the National Policy Statement, and the National Planning Policy Framework. This would ensure it is given strong planning policy support. While pursuing this policy change the Government must be mindful of environmental concerns as well as the role of environmental considerations under the current policy framework. Relatedly, the Government should implement a reform proposed in the Fingleton Review amending the cost cap for judicial reviews and restrict legal challenges to Nationally Strategic Infrastructure Projects (NSIPs).

**Idea 7:** The Government should require plans for critical systems so that government systems continue to operate in the event of an attack, telecommunications disruption, the collapse of a vendor, or if access to data is otherwise disrupted. These plans should include drills and exercises, data restoration and backup plans, and naming specific officers responsible for data loss

## 3.2 Full stack sovereignty risks

Given the potential complexity of a robust digital sovereignty policy, some may consider a full stack sovereignty policy which mandates British government control of the whole stack desirable. But while full control of the stack might achieve many of the national security goals sought by some sovereignty advocates, it is unrealistic given the UK’s size, the nature of supply chains, and comparative advantages enjoyed by many foreign market incumbents. A full stack policy would be expensive, repel many investors, and would not necessarily guarantee security.

In addition, such a policy would risk conflating sovereignty with security. Sovereign policies provide no extra security in and of themselves. Indeed, one of the main challenges in the digital sovereignty debate is that many foreign digital services do offer robust security features – global companies can bring significant investment and expertise to bear in safeguarding their products against cyberattacks, and an insufficiently thought-through policy could sacrifice security in return for notional sovereignty.

As noted above, the current supply chains that underpin the technology that fuels the global economy are so complex that it would be politically and financially prohibitive for a government to insist on full stack control. However, even if it were possible for the government to achieve full stack control, such a move would come with significant economic, rent seeking, and regulatory capture risks.

The French government, for example, has committed to replace all video-conferencing services based in the USA with its own bespoke Visio service.<sup>34</sup> The goal is for all French civil servants to be off Microsoft Teams, Webex, and Zoom and using Visio by 2027.<sup>35</sup> Such an approach is no doubt attractive to those who are concerned about the United States’

<sup>34</sup> Steven Vaughn-Nichols, ‘Why France Just Dumped Microsoft Teams and Zoom - and What’s Replacing Them’, *ZD Net*, 30 January 2026.

<sup>35</sup> *Ibid*.

occasionally erratic foreign policy and the risk of American companies being forced to hand over data associated with Europeans to the American government. However, this approach, if implemented by the UK Government, could end up resulting in significantly higher prices for the public sector and consumers in the UK. It also stands out among other European nations for being notably protectionist.

For example, the German government has adopted a version of sovereignty that does not shy away from hyperscalers. The German Delos Cloud is a sovereign cloud structure for public services operated by a German company but built with Microsoft Azure technology.<sup>36</sup> The state of the current foreign sovereignty policies should be reassuring to lawmakers who are committed to developing a sovereignty policy but are unpersuaded that protectionism is the best way to achieve it. Germany shows one possible source of inspiration: a sovereign policy that ensures domestic control alongside the use of hyperscale technology.

Microsoft, AWS, Alphabet, and other American hyperscalers are very popular in large part because they are efficient. They have built massive data infrastructure while competing to offer the most attractive cloud storage, video conferencing, and email suite tools they can. These attractive (and relatively affordable) products may come at the expense of security risks governments do not want to expose themselves to, but they should nonetheless develop sovereignty policies with these trade-offs in mind. Depending on the specific UK sovereignty policy, it is possible that British consumers or taxpayers would incur the higher costs of funding native British and bespoke sovereign technology that relies on domestic infrastructure and supply chains.

The political implications could also be significant. Faced with a ban on foreign technology companies hosting or facilitating government data, governments would have to consider domestic suppliers.

Governments could opt for an open-source approach similar to that seen in Denmark. Last year, reporting revealed that the Danish Ministry for Digitization is planning a phased introduction of Linux operating systems and LibreOffice tools to replace Windows and Office 365.<sup>37</sup> Such an approach will save on licensing fees, but there will be costs associated with migrating to an open source system, ensuring civil servants are adequately trained, and ensuring the new open source system is secure.

The EU Cloud and AI Development Act will reportedly aim to triple EU data-centre capacity. Such an increase would boost the ability of EU firms and governments to train AI models and secure data under European legal regimes. It would be a significant step towards the EU sovereign cloud objectives laid out in the European Commission's Cloud Sovereignty Framework.<sup>38</sup> The bill would also lay out ancillary planning and energy policies aimed at boosting sovereignty, including fast-track approval of data centre construction. Among the most notable possible policies included in the bill are requirements for EU-made software and hardware for public tenders.<sup>39</sup> Although the bill would not prohibit non-EU companies from bidding for EU contracts, it would make it much harder for non-EU companies to secure

---

<sup>36</sup> Douglas Phillips, 'Microsoft Strengthens Sovereign Cloud Capabilities with New Services', Blog post, 4 November 2025.

<sup>37</sup> Efosa Udimwen, 'Denmark Wants to Replace Windows and Office with Linux and LibreOffice as It Seeks to Embrace Digital Sovereignty', *TechRadar*, 15 June 2026.

<sup>38</sup> 'Cloud Sovereignty Framework: Version 1.2.1', European Commission: Directorate-General for Digital Services, October 2025.

<sup>39</sup> Foo Yun Chee and Toby Sterling, 'Exclusive: EU Cloud Rules to Curb Big Tech's Access to Strategic Tenders, Draft Document Shows', *Reuters*, 1 June 2026.

contracts, especially those associated with critical systems and supply chains.<sup>40</sup> It remains to be seen how many of these early reported policy proposals will make their way into the final version of the bill, but they nonetheless show how many EU officials are thinking about digital sovereignty.<sup>41</sup>

---

<sup>40</sup> Chee and Sterling, 'Exclusive: EU Cloud Rules to Curb Big Tech's Access to Strategic Tenders, Draft Document Shows'.

<sup>41</sup> Ibid.

---

## 4. Conclusion

A robust digital sovereignty policy need not require isolationism or autarky. The nature of global supply chains underpinning the economy makes such an approach disproportionately costly and would result in the British public enjoying fewer of the goods and services necessary for the UK to achieve economic growth, resilience, and security. The Government should, however, implement digital sovereignty policies aimed at making British digital infrastructure more resilient and secure. Doing so would not only boost security but would also make the UK a more attractive country for foreign investment and talent.

Political concerns associated with current geopolitical tensions tend to dominate conversations about digital sovereignty, but policy in this area should be seen as an economic and security necessity, rather than a point-in-time political challenge. The UK enjoys enviable comparative advantages such as its home-grown technology sector talent, sovereign network infrastructure, operational capability, elite academic institutions, an established global financial sector, and respected legal institutions that make it exceptionally well-placed when compared to other nations to seize this opportunity.

A clear tiered framework based on risks to national security and critical public services associated with procurement, security, and data control requirements at each stage would allow for government to use digital services, whether homegrown or provided by US-based hyperscalers, with confidence that they have control over critical data and are able to migrate to different systems if necessary.

Crucially, this approach would allow a wide range of digital services to enjoy regulatory certainty, whether they are app-based companies or large technology companies with a diverse portfolio of software and hardware services and global supply chains.

Alongside the framework, as part of a broader sovereignty policy, the Government should also take steps to reform planning and energy policy. These would make data centre construction easier for domestic manufacturers and more attractive for foreign investors. This would not only unlock investments which are currently unviable for investors to make in the UK, it would also ensure that the UK improves its reputation as a reliable home of digital investment and innovation – particularly in emerging technologies like AI.



# Bibliography

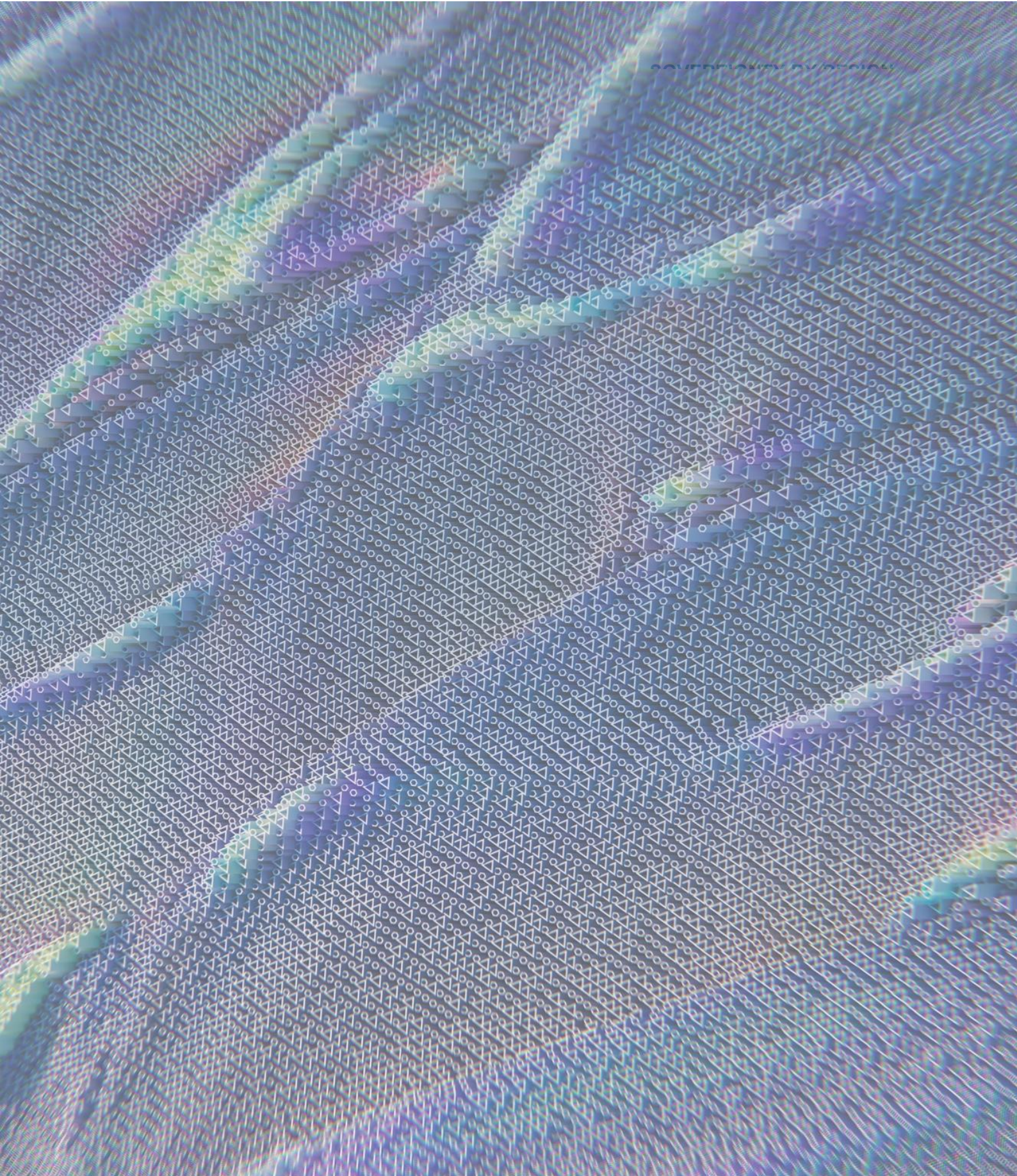
- 'API Technical and Data Standards'. Guidance. Government Digital Service and Central Digital and Data Office, 7 February 2018.
- Boswall, Robert. 'The Value of Connection Grid: Connection Auctions'. Substack, Robert Boswall, 2 April 2026.
- 'Call for Input: Demand Connections Reform'. Ofgem, 13 February 2026.
- Chee, Foo Yun, and Toby Sterling. 'Exclusive: EU Cloud Rules to Curb Big Tech's Access to Strategic Tenders, Draft Document Shows'. *Reuters*, 1 June 2026.
- Chia, Osmond. 'Anthropic Says US Lifts Export Ban on Its Advanced AI Tools'. *BBC News*, 1 July 2026.
- Cloud Services Market Investigation: Summary of Final Decision*. Competition and Markets Authority, 2025.
- 'Cloud Sovereignty Framework: Version 1.2.1'. European Commission: Directorate-General for Digital Services, October 2025.
- Craske, Ben. 'Stargate UK: Why Is OpenAI Halting Its AI Data Centre Deal?' *Data Centre Magazine*, 10 April 2026.
- 'CROWN HOSTING DATA CENTRE COLOCATION SERVICES: Framework Agreement with Crown Hosting Data Centres Limited'. Crown Commercial Service, July 2020.
- CSCConnected. 'Who We Are'.
- 'G-Cloud Buyer's Guide'. Guidance. Crown Commercial Service, 24 September 2013.
- Gold, Hadas. 'Anthropic Suspends All Access to Mythos Model after US Government Bans Foreign Nationals Use'. *CNN*, 13 June 2026.
- 'Government Creates New Business to Save up to £105 Million in IT Costs'. Press Release. HM Government, 19 March 2015.
- Hezlet, Ed, and Lucy Shaw. 'Speeding up Grid Connections to Lower Bills and Deliver Growth'. Report. Centre for British Progress, n.d.
- 'International Non-Domestic Energy Prices'. Statistical data set. Department for Energy Security and Net Zero, 28 May 2026.
- Koopman, Saskia. 'Fractile vs Nvidia: Can a UK Startup Undercut AI's Chip Darling?' *City A.M.*, 6 May 2026.
- 'Make Use of Open Standards'. Guidance. Government Digital Service and Central Digital and Data Office, 6 November 2017.
- Management Practices and the Adoption of Technology and Artificial Intelligence in UK Firms: 2023*. Office for National Statistics, 2025.
- Manners, David. 'UK AI Chip Startup in Talks to Raise \$200m'. *Electronics Weekly*, 7 May 2026.
- 'National Infrastructure Planning: Data Centres'. Written questions, answers and statements. House of Commons, 15 October 2025.
- 'National Semiconductor Strategy'. Policy Paper. Department for Science, Innovation and Technology, 19 May 2023.
- NHS England. 'Crown Hosting'. NHS England, 29 January 2026.
- Smith, Hannah. *Does the UK Have the 'most Expensive' Electricity in the World?* Full Fact, 2025.
- 'Statement on the US Government Directive to Suspend Access to Fable 5 and Mythos 5'. Announcement. Anthropic, 12 June 2026.
- 'The Technology Code of Practice'. Government Digital Service and Central Digital and Data Office, 14 July 2021.
- Trendall, Sam. 'Seven AI Firms Receive Support via New Government Tech Venture Capital Unit'. *Public Technology*, 16 April 2026.
- Udinmwun, Efosa. 'Denmark Wants to Replace Windows and Office with Linux and LibreOffice as It Seeks to Embrace Digital Sovereignty'. *TechRadar*, 15 June 2026.

*Uncorrected Oral Evidence: Human Rights and the Regulation of Artificial Intelligence*, HC 1262. Joint Committee on Human Rights, 2026.

Vaughn-Nichols, Steven. 'Why France Just Dumped Microsoft Teams and Zoom - and What's Replacing Them'. *ZD Net*, 30 January 2026.

'Where Does Your IT Live? Moving beyond Server Rooms to Smarter, Greener Estates'. 15 October 2025.





# Re:State

ISBN: 978-1-918941-03-6



@restate\_thinks



@re-state.bsky.social



www.re-state.co.uk