Digital Intelligence & Land

BAE SYSTEMS

Beyond sovereignty: Building resilient digital nations



Executive summary

Why are we thinking about digital sovereignty now?

In March 2026, a House of Commons Library briefing on digital sovereignty defined the concept as "the agency and capacity of any organisation to make intelligent, informed choices to shape its digital future by design". Digital sovereignty is the ability for a nation to maintain effective control over its digital assets, services and critical technology dependencies, while continuing to operate autonomously and without external interference. The current debates on digital sovereignty are driven by two developments, which are evolving the perspectives on sovereignty requirements from those over previous decades.
At a national level, one driver is growing scrutiny around long-term strategic dependencies. For example, recent shifts in international foreign policy and security priorities have prompted a number of nations to re-examine their dependence on externally controlled capabilities, accelerating discussions around strategic resilience and digital sovereignty.

The second driver is the heightening prominence of hyperscalers, AI and software service providers, which each have leveraged greater compute capacity to create a step-change in mission capability – primarily through pace and efficiency of operations, data fusion and intelligence analysis. Concern can arise when critical national capabilities become highly dependent on technologies operating under legal, regulatory or governance frameworks outside of a nation's direct control. The level of concern typically increases when that dependency could limit freedom of action, reduce flexibility or create uncertainty about long-term access to critical capabilities.

Digital or tech sovereignty applies to the entire digital stack, with a current focus on cloud infrastructure, software platforms and AI. Sovereignty requirements, however, can also apply to hardware components, the supply chain and security enforcing functions throughout the stack.



"The challenge of selective sovereignty is to understand where greater control delivers meaningful reduction in risk..."



While digital sovereignty is a hugely topical debate in 2026, history suggests sovereignty is rarely the objective in itself. Governments pursue sovereignty measures in response to specific risks, whether to ensure continuity of service, freedom of action, supply chain security or control over sensitive assets. The underlying goal is resilience: ensuring that critical national infrastructure and services can continue operating through disruption, geopolitical change and strategic uncertainty - and to be assured of that control.

So, we must reframe the questions. It is commonly understood that full sovereignty is unrealistic. A literal interpretation would be to have domestic capabilities at all levels of the stack, which would be unfeasibly expensive, unlikely to match the maturity and sophistication of existing technologies, and fail to leverage any economies of scale offered by global markets and competitive advantage. The balance between cost and control is clearly more nuanced, leading to questions such as "How sovereign do we need to be?" and, more importantly, "Where do we need sovereign capability most?". The challenge of selective sovereignty is to understand where greater control delivers meaningful reduction in risk and where resilience can be achieved through alternative measures.

This paper makes two central arguments. First, the digital sovereignty debate is fundamentally a question of risk management. Second, decisions should be driven by the outcomes governments seek to achieve, particularly resilience. By starting with desired outcomes and then assessing the controls, capabilities and investments needed to deliver them, organisations can take a more proportionate approach to sovereignty, and a long term view to realistically reflect strategic investment in sovereign capability.

Introduction

Sovereignty: From risk to resilience

The debate around digital sovereignty has become increasingly prominent as governments reassess their exposure to geopolitical uncertainty, technology concentration and supply chain dependence. Across government, critical infrastructure and regulated industries, leaders are asking fundamental questions:

- Who controls our technology?
- Where does our data reside, and where does it flow to?
- What happens if strategic circumstances or access to critical capabilities change?

These are important questions, but sovereignty itself is not the end goal.

Modern digital systems are built upon interconnected global ecosystems of hardware manufacturers, cloud providers, software vendors, communications networks and specialist suppliers. Complete technological independence is neither realistic nor desirable for most nations. The more useful question is not whether a nation is fully sovereign, but whether it is resilient to change, disruption or denial.

From this perspective, sovereignty becomes one of several levers available to improve resilience. In many cases, resilience may be achieved through supplier or technology diversification, assurance regimes, contractual controls, open architectures, interoperability standards, or trusted international partnerships. In others, sovereign ownership or domestic control of capability may be unavoidable.

"Complete technological independence is neither realistic nor desirable for most nations. The more useful question is not whether a nation is fully sovereign, but whether it is resilient to change, disruption or denial."

Chapter 1

Case studies from the past

Analysis of historical sovereignty requirements through the digital stack helps illustrate a recurring pattern: sovereignty capabilities are typically introduced to address a perceived risk – which could relate to security, supply chains, operational continuity or strategic dependence.

Sensitive and classified assets

Historically, a key driver for sovereignty requirements has been the protection of sensitive and highly classified assets. Higher assurance networks and systems generally required cleared nationals for support roles, and domestic data centres for infrastructure hosting – in other words, keeping both physical and logical access within the boundaries of the home jurisdiction[1], as opposed to offshore arrangements.

Furthermore, government security policy in some nations has historically mandated the use of sovereign technologies for security-enforcing functions, such as cross-domain solutions and cryptographic systems. In these cases, the technology must be assured by the government or a trusted partner. This is fundamentally a question of trust in the technology's provenance, integrity and availability, whether that trust derives from established suppliers operating within recognised assurance frameworks or through independent evaluation and certification[2]. Some governments, including the US and UK, have sought to maintain a domestic commercial capability in critical security functions such as cryptography and cross domain to support national requirements. Such an approach should also shape investment in domestic technology markets to foster sovereign alternatives where assurance and trust are considered strategically important.

Core components

Concern about the provenance of components can extend to hardware and software products considered critical to the security and operation of a service.

The debate surrounding Huawei's role in UK telecommunications infrastructure illustrates how assessments of technology risk can evolve over time. While technical assurance and evaluation mechanisms may provide confidence in product security, concerns can also extend to supply chain resilience, strategic dependence and broader operational considerations. As reported by the UK Government, the subsequent decision to remove Huawei equipment from UK telecommunications networks demonstrated that technical assurance alone may not be sufficient when evaluating technologies used within critical national infrastructure. Trust is also shaped by confidence in a supplier's long-term reliability, the wider assurance framework within which it operates and the degree of control that can be exercised over strategically important technologies.

Supply chains

Supply chain risk is relevant to the above concerns, and has emerged as a major factor given the degree of embedding, inter-dependency and inheritance that exists in the digital stack. The discovery that a critical software component originated from a supplier operating outside recognised assurance, regulatory or governance frameworks could raise concerns about integrity, trustworthiness and the potential for compromise - particularly when that software supports essential national infrastructure.



> "Supply chain resilience depends on diversity, substitutability and the ability to reconfigure services or source alternative providers when circumstances change."

The dependency and resilience aspects of supply chain risk are illustrated by recent concerns regarding semiconductor manufacturing. For many years, the efficiency of global supply chains enabled the United States to rely heavily on overseas semiconductor production, particularly in Taiwan. However, growing concerns about supply-chain concentration and the implications of geopolitical tensions led policymakers to view semiconductors as a strategic national security capability. This, in turn, drove substantial investment in domestic manufacturing and supply chain resilience through the CHIPS and Science Act.

The resilience challenge is therefore not simply a question of where a capability originates, but whether viable alternatives exist if access becomes constrained. Supply chain resilience depends on diversity, substitutability and the ability to reconfigure services or source alternative providers when circumstances change.

Cloud and hyperscalers

While debates about hyperscalers often focus on data access and jurisdiction, they are equally debates about resilience. Cloud services can significantly improve resilience through scale, redundancy and rapid recovery capabilities. At the same time, concentration of services within a small number of providers can create strategic dependencies that themselves become resilience risks.

The ongoing journey to cloud adoption has been a cautious one for government organisations, presenting a new set of sovereignty requirements that emerged from a shifting risk paradigm - from on-premises to virtual infrastructure. The concern surrounding cloud and the access it affords to its tenants' data reflects one of the risks identified above: in some jurisdictions, cloud providers may be compelled under national security or law enforcement legislation to provide access to customer data.



Organisations may have different risk appetites regarding how legal access powers could be exercised across jurisdictions, which can include decisions about where sensitive data is stored and processed. Cloud providers have worked with governments and regulated industries to develop deployment models and controls designed to address sovereignty and resilience requirements, including advanced encryption and jurisdictional safeguards. Some try to offer a degree of sovereignty by providing both local and global deployments. Where support is provided by non-nationals, technical controls, such as just-in-time access and least privilege, can be used to reduce the risk.

Data residency

In a more modern context, this concern over data residency and access persists in numerous national contexts and is reflected by the concerns of the Ukrainian government. Following Russia's 2022 invasion, Ukrainian authorities allowed critical government data to be moved to cloud environments hosted outside of the country, gaining immediate benefits in terms of continuity and resilience from cyber attacks and outages during multi-domain conflict.



By 2025, beyond the immediate operational requirement, discussions had begun to focus on digital sovereignty and how critical national data could remain under greater Ukrainian control. This would not necessarily require data centres to be located within a conflict zone, but it could involve alternative hosting arrangements, jurisdictional safeguards or other controls over data access.

The Ukrainian experience illustrates that resilience and sovereignty objectives can sometimes compete in the short term. Faced with an existential threat, resilience priorities drove the rapid migration of critical data and services to cloud environments outside national borders. Longer-term sovereignty considerations only became relevant once continuity and survivability had been secured.

What does this tell us?

This analysis of sovereignty debates over the years indicates that there are different concerns at play and a range of options to mitigate them. Fundamentally the risks relate to maintaining operational continuity, along with control over access, supply chain and technology choice. These have, and will continue to be, addressed by different options, balancing outcome against cost over time. One of those options is to invest in domestically developed or controlled technology, although this must be balanced against cost, timescale, capability maturity and the benefits offered by global technology ecosystems.

[1] Clearly, software-as-a-service offerings now make this harder to achieve, as discussed later; hardware belongs to an external party and data resides within their control, and often overseas.

[2] Examples are illustrated here Schemes & Product Types | HASC - High Assurance Security Centre

Chapter 2

Understanding digital resilience risks

As outlined above, sovereignty debates often focus on ownership and control, but these are ultimately manifestations of broader resilience risks.

Risks can be grouped into availability (threatened by disruption or supplier concentration), strategic autonomy, and control over access.

Risks to availability: Disruption

Risks to availability could emanate from a variety of sources in a variety of ways. Disruption of the physical environment, including climate events, terrorism or conflict, public health or safety crises and destructive cyber attacks such as ransomware. External shocks expose the dependencies between services, and supply chain risks can be realised, in particular where suppliers are overly stretched themselves or have a concentrated footprint. If a whole sector is affected by a ransomware attack and has contracts with the same Incident Responder company, then the capacity of that IR company will constrain its availability to all its customers at once.

Risks to availability: Supply chain concentration

The above example highlights the risks associated with sectoral or national over-dependency on a single supplier, which can emerge where a single company has a disproportionate footprint in a sector. Concerns arise about its ability to support all customers under pressure or surging demand – and therefore the availability of its services to all its customers. It also spotlights the impact a failure of that supplier (for whatever reason) might have on the essential services that it supports. This reflects more of a concern about availability, and financial volatility against a backdrop of change, than the risk of access to sensitive assets.

Risks to strategic autonomy

In a context of geopolitical pressure and globalisation, fears of over-dependency on a capability or supplier further develop into risks of strategic autonomy. What if costs, commercial terms or access conditions significantly change over time, or a capability became subject to export controls? Previous decisions to leverage economies of scale and lessons across departments can, from another angle, look like over-dependency.



Dependency risk can arise from vendor lock-in, government-imposed supply constraints (for example, export controls affecting access to advanced AI models in 2026) and exposure to price rises or shocks. Nations that lose freedom of choice become vulnerable to external pressure even when services remain technically available. The Civo report defines a "Sovereignty Tax" as the costs incurred through dependency on foreign providers and the difficulty of exiting those ecosystems.

Strategic autonomy is a characteristic of resilient businesses and nations who retain their freedom of choice and ability to operate despite those pressures and shocks.

Risks to control and confidentiality

A core sovereignty concern relates to data access and control where services are subject to legal, regulatory or operational frameworks beyond the direct influence of the organisation or nation that relies upon them. This is amplified when there is a concern about over-dependency and aggregated access. Where there is a concentration of software across a government estate or across critical services, concern can arise regarding the aggregation of operational information and the resilience implications of broad dependency on a concentrated number of platforms or services.

In the current context, AI frontier models and software platforms present a combination of these concerns. AI provides an interface to vast volumes of data and knowledge, which can generate insights that may not be immediately visible to the customer. Similarly, a dependency arises on the capabilities and insights they provide, but in the case of AI models, there are multiple choices available on the market. Information and data risks similarly apply with publicly available AI models - the earliest security rule to emerge about using public LLMs was to avoid inputting sensitive information into the text field, which represented data leakage. Risks of misinformation in LLMs emerge where there is insufficient data cleansing or assurance to trust the data being worked upon.



Chapter 3

Decision-making framework

Digital sovereignty is often treated as the objective, but as the examples in this paper demonstrate, sovereignty is about technology and supplier choice in response to specific risks. The underlying objective is resilience: maintaining the availability of critical services, preserving freedom of action, and retaining control over sensitive assets and data.

There is often a trade-off between capability, cost and control. Few countries can afford complete technological independence across every layer of the digital stack. Equally, unrestricted dependence on external providers may expose critical services to unacceptable levels of risk. The most effective approach, as always, lies on the spectrum between these extremes: understanding where resilience matters most and applying sovereignty measures only where they deliver meaningful reduction to risk.

The challenge is to identify where sovereignty measures deliver meaningful resilience benefits and where other approaches may be more effective. A practical framework should therefore begin with resilience outcomes rather than predetermined sovereignty requirements.

"The challenge is to identify where sovereignty measures deliver meaningful resilience benefits and where other approaches may be more effective."



1. Identify critical outcomes:

- **What services** must continue during disruption or crisis?
- **Which assets, systems or data** are essential to national security, economic stability or public services?
- **What are we** less concerned about, and can tolerate less control over?

2. Assess resilience risks:

- **Availability and disruption:** Could services be disrupted by cyber attacks, conflict, supply chain failures or infrastructure outages?
- **Supply chain concentration:** Could over-reliance on a limited number of suppliers, platforms or regions create vulnerabilities if access, availability or pricing were to change?
- **Strategic autonomy:** Could dependency on a supplier, technology provider or foreign government limit future technology or procurement choices?
- **Control and access:** Could sensitive systems, data or decision-making be exposed to unwanted access or influence?



3. Evaluate mitigation options:



Not every risk requires a sovereign solution. In many cases, resilience can be achieved through diversity, transparency and technical controls. **Examples include:**

- **Assurance** and testing regimes
- **Supplier** and platform diversity
- **Open standards** and interoperable architectures
- **Segmentation** and redundancy
- **Governance** and contractual controls
- **Investment** in domestic or sovereign capabilities

It is, however, worth considering how strategic, commercial, regulatory and operational circumstances might evolve. The use of open authentication standards and distributed trust architectures provides a modular approach that preserves assurance, while avoiding unnecessary dependency on assumptions or operating environments that may change over time.

4. Balance capability, cost and control:

Decision-makers should assess which interventions deliver the greatest resilience benefit while preserving access to innovation, capability and value.

In the context of emerging technology, the benefits of hyperscale compute, AI and quantum offer advances in data exploitation and intelligence analysis, such that nations fear being left behind. However, this potentially leads to a short term view of risk fuelled by potential capability advances and competition. It also increases the susceptibility to snake-oil, such as unproven or overstated technology claims.

At an economic and political level, procurement decisions also present opportunities and imperatives to invest in sovereign technologies – which may present a near term cost with a time delay, but over the longer term would present more sovereign alternatives to the procuring party.

Richard Horne, CEO of the National Cyber Security Centre, has argued for a pragmatic approach to cyber resilience in an environment shaped by rapid technological change and geopolitical uncertainty. In practice, this suggests that different technologies, services and datasets will require different levels of assurance, control and resilience depending on their importance and risk profile.

Ultimately, the goal is not sovereignty for its own sake, but resilient digital capability that can withstand disruption, adapt to change and maintain freedom of action and security in an increasingly uncertain world.

Conclusion

In the current climate of concern about resilience, where shocks can come from any direction and supply chains are so intertwined as to be unpredictable, resilience needs to be a principle of design, enabling flexibility and continuity. Single disruption scenarios do not form the sole basis of flexible design. Resilient architectures should be designed to cope with changes and shocks across a whole range of scenarios.

The future of digital sovereignty should not be understood as a pursuit of technological self-sufficiency. Instead, it should be viewed as part of a broader resilience strategy. The most resilient nations will be those that understand their dependencies, maintain freedom of choice, diversify sources of risk and retain the ability to adapt when circumstances change. Sovereignty therefore becomes not an end state, but a deliberate and proportionate response to well-defined risks.

This paper has explored how sovereignty requirements have evolved in response to changing risks and dependencies. The current debate increasingly centres on AI, software platforms, compute infrastructure and supply chain; themes that we'll explore in subsequent papers in this series.

Subscribe to receive insights from this series straight to your inbox: The Digital Thread



Digital Intelligence & Land is a fast-paced hub within BAE Systems, home to 6,000 experts across 13 countries. Our advanced cyber, digital and manufacturing capabilities are dedicated to keeping vital infrastructure running, national security protected and armed forces prepared.

From transforming complex data into actionable intelligence to delivering next-generation capabilities for the battlespace of tomorrow, our agile teams leverage AI to help customers move from data to delivery at mission speed. We empower militaries, government departments and critical national infrastructure to detect risks and emerging threats, decide and plan the right course of action, and deploy mission effects with agility and precision.

BAE Systems Digital Intelligence & Land
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence & Land
Malta Office Park
ul. Abpa A. Baraniaka 88
Poznan
61-131
Poland
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence & Land
Level 2
14 Childers St
Canberra
ACT 2601
Australia
T: +61 (0) 2 9053 9330

BAE Systems Digital Intelligence & Land
Level 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur
50450
Malaysia
T: +60 327 309 390

BAE Systems, Surrey Research Park,
Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com
W: baesystems.com/digital

linkedin.com/company/baesystemsdigital
@BAESystemsDigi

Copyright © BAE Systems plc 2026. All rights reserved.

BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc.

BAE Systems Applied Intelligence Limited registered in England & Wales (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ.

No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Digital Intelligence & Land.