MAY 2026

JARED WRIGHT
OTT VELSBERG
ALEXANDER IOSAD
KEEGAN MCBRIDE

Digital Embassies and AI Sovereignty: Building Resilient States Beyond Borders

TONY BLAIR
INSTITUTE FOR
GLOBAL CHANGE

Contents

Executive Summary

Modern states increasingly depend on digital infrastructure that is both critical and physically vulnerable. Identity systems, registries, payments, legal records, administrative platforms and public-service channels now form part of the state's operational core. When these systems fail, the issue is not only service disruption, but also the continuity and credibility of government itself.

War, cyber-attacks, sabotage, terrorism and natural disasters can all affect the systems on which governments, economies and public services rely. Artificial intelligence intensifies this challenge. Governments will increasingly depend on concentrated, capital-intensive infrastructure – cloud, compute, energy, connectivity, secure data environments – that many states cannot fully build, finance or control domestically. As a result, the question is no longer whether states will depend on infrastructure beyond their borders, but how that dependence can be governed.

One concept attracting growing attention as a potential solution to these challenges is the digital embassy – a legally, technically and politically governed arrangement that allows states to preserve, restore or operate critical digital functions through trusted infrastructure beyond their territory. Building on the earlier data-embassy model, which focused on legally protected cross-border storage and recovery of critical state data and systems, digital embassies go even further. They can provide live-system continuity, service continuity and, in some cases, trusted access to cloud, compute or AI infrastructure. At their most advanced, digital embassies are designed to preserve the operational capacity of the state – including identification, authentication, access to records, legal administrative processes and communication with citizens – even when domestic infrastructure or normal administration is disrupted.

This paper argues that digital embassies should be understood as strategic instruments for resilience, security, sovereignty and capability. For guest states (those seeking to externalise elements of their sovereign digital infrastructure), they can reduce single points of failure, preserve state continuity and provide access to strategic infrastructure. For host states

(those aiming to host such systems for other countries), they can attract investment, strengthen the economy, aggregate demand for cloud and compute, deepen strategic partnerships, and position countries within the emerging global digital and AI infrastructure ecosystem. But hosting also creates political, legal and security exposure, and therefore requires credible safeguards and institutional capacity.

This paper explores these dynamics and offers a guide for policymakers that outlines what digital embassies are, the potential benefits they offer, whether they are relevant to their context, how they should be designed and what safeguards are required before critical functions are externalised. For governments interested in developing a digital-embassy strategy, the paper makes three primary recommendations:

1. MAINTAIN CRITICAL STATE FUNCTIONS

A credible digital-embassy strategy must begin with a clear understanding of what the state needs to preserve, restore or operate under stress. Governments should identify which systems, services and data sets are critical to the continuity of the state and basic societal functioning before deciding which functions should remain domestic, which should be replicated abroad and which can be operated through external arrangements. This will require policymakers to:

- **Define what is critical to state continuity and classify workloads accordingly.** Governments should formally designate the systems, data and services without which the state cannot legally, operationally or politically function, while distinguishing among public, sensitive, confidential and highly restricted workloads.
- **Set resilience requirements and externalise selectively.** Governments should establish explicit continuity requirements, including acceptable downtime and recovery thresholds, and assess whether these can be met within national infrastructure, with manageable risks, before considering externalisation.

- **Diversify dependencies where feasible.** Resilience may require diversification not only across jurisdictions but also across cloud providers, AI platforms and infrastructure suppliers to reduce exposure to single points of failure or provider-level disruption.
- **Map both system continuity and public-service continuity.** Governments should identify not only which systems must survive, but also which public services must remain deliverable to citizens, businesses and public authorities, including when users or administrators are outside national territory.
- **Define activation thresholds in advance.** Governments should establish the legal and operational conditions under which services, failover arrangements or cross-border delivery mechanisms would be activated, rather than leaving these decisions to crisis conditions.

2. PRESERVE SOVEREIGN CONTROL THROUGH INTERDEPENDENCE

The value of a digital embassy lies in helping states shape interdependence deliberately by building trusted ecosystems in which states, allies and technology providers can share infrastructure and capabilities while preserving national agency and limiting exposure to coercion or disruption. This will require states to:

- **Define non-transferable sovereign control functions.** Governments should make explicit which functions cannot be delegated to a host state or provider, including cryptographic controls, identity governance, access management, auditability and core decision-making rules.
- **Use risk-based partner and provider selection.** Jurisdictions and providers should be assessed based on legal reliability, institutional stability, geopolitical alignment, technical capability, exposure to external pressure, workload sensitivity, and the robustness of legal and technical safeguards, rather than assuming that domestic or regional provision is inherently safer.

- **Build interoperability, portability and reversibility into the design.** Systems should be capable of being moved, restored or reconstituted across environments to avoid the risk of being irreversibly dependent on a single host, provider, architecture or regulatory regime.
- **Preserve control while enabling access.** Major technology providers will often be essential to delivering scale, security and resilience, but reliance on any provider, jurisdiction or regulatory system must be appropriate to the sensitivity of the workload and supported by clear safeguards.
- **Preserve domestic accountability and public legitimacy.** Externalising infrastructure must not externalise political responsibility: citizens should have clear information on what is hosted abroad, who can access it, which law applies, what oversight exists and what remedies are available.

3. STRESS-TEST DIGITAL-EMBASSY ARRANGEMENTS

Digital embassies will only strengthen resilience if they remain credible under stress. Legal, technical and operational arrangements must therefore be designed, tested and exercised before crisis conditions emerge. This will require states to:

- **Codify enforceable access and operating rights, not just principles.** Bilateral or multilateral agreements should define jurisdiction, access rights, activation thresholds, continuity obligations, non-interference commitments, liability, dispute resolution and responsibilities during disruption.
- **Back legal guarantees with technical and operational safeguards.** These should include redundancy, segmentation, encryption, access controls, audit logs, incident-response protocols, escalation pathways and tested response procedures.
- **Define operational authority and crisis governance in advance.** Governments should clearly establish who has the authority to activate failover, coordinate incident response, communicate with providers and host states, and make continuity decisions during crisis conditions.

- **Test arrangements under realistic stress conditions.** Governments should conduct joint exercises and scenario planning for cyber incidents, infrastructure failures, geopolitical tensions, economic coercion, sanctions and armed conflict, so continuity is not merely a matter of principle.
- **Assess dependencies across the full delivery chain.** Governments should evaluate not only the host jurisdiction but also providers, subcontractors, support models, telecom links, software-update channels and external AI or cloud control layers that may become points of leverage or failure.
- **Explore alliance-based, two-way or distributed arrangements where appropriate.** Where political and strategic conditions allow, these models can reduce dependence on any single host and strengthen credibility under stress.

As countries become increasingly dependent on infrastructure that is capital and energy-intensive, concentrated, and increasingly difficult to replicate, digital embassies will become an essential strategic tool. They can influence where critical infrastructure is located, which allies and partners a state relies on, and how states strengthen resilience, security and sovereignty in a globally interdependent system.

01

The Importance of Digital-Infrastructure Resilience

Today's digital world depends on real-world, physical infrastructure. As developments in artificial intelligence and other emerging technologies continue to transform how economies, governments and societies function, this dependence will become greater. The growing reliance on a small number of physical assets, such as electricity supply, data centres and subsea cables, creates new points of failure for digital states. A missile strike, fire, cable cut, cyber-physical attack or power disruption can now interrupt core government services. Policymakers must therefore be proactive in mitigating these risks to ensure the security and resilience of their digital states.

There are many contemporary examples demonstrating the fragility of the current model. At the start of the war in Ukraine, government data centres were targeted by ballistic missiles to disrupt government operations.[1] In South Korea, a fire at a government data centre disrupted digital services and caused significant data loss.[2] More recently, data centres across the Middle East were targeted by drones and other munitions, causing significant damage and disruption.[3] There has also been an increase in the number of terror-related attacks on digital infrastructure.[4] The implications of this are clear: a country's, or indeed the world's, digital operations can be disrupted by war, sabotage, terrorism, natural disasters and more.

This realisation comes at the same time as countries and businesses around the world are investing trillions of dollars into building out the infrastructure required to support AI systems.[5] Countries will require their own AI infrastructure but just how much depends on their needs – compute needs vary significantly between training frontier models, fine-tuning domain-specific systems, running secure inference and operating public-sector AI services. But as recent TBI research suggests, most countries are unable to fund or sustain the buildout of all the infrastructure they need to meet their own domestic compute demand – especially for frontier-model training. As

a result, many governments will be reliant on external providers and this is why demand aggregation and trusted cross-border infrastructure could become attractive.

This reality requires leaders to confront two urgent questions. First, how can their governments improve the resilience of the digital infrastructure on which their economies, government operations and national security depend, especially given that this infrastructure is expensive and vulnerable to destruction at an ever-lower cost? Second, how can governments preserve sovereignty, resilience and security while simultaneously growing access to compute and frontier AI, often using external providers? Any solution will depend on cooperation, collaboration and the development of new strategic partnerships with both the private sector and trusted allies.

It is impossible to build the required resilience and security unilaterally. The task for policymakers is therefore to determine which functions must remain domestic, which can be shared with trusted allies, and which can be externalised under enforceable legal, technical and political safeguards.

One practical response is the emerging model of digital embassies.[6] Originally conceived as a continuity mechanism,[7] digital embassies are now increasingly part of wider debates about digital sovereignty, infrastructure concentration and access to advanced AI capabilities. This paper traces the evolution of digital embassies, explains their growing relevance and provides leaders with a clear framework for both guest states and host states to assess how they can strengthen resilience, manage new risks and determine which critical functions must remain under direct national control.

While the idea of a digital embassy has only recently entered the public debate,[8] it was preceded by the concept of a data embassy,[9] legally protected cross-border storage or backup of critical sovereign data and systems, primarily for preservation and recovery. In contrast, digital embassies describe a broader, emerging category of arrangements, as outlined in Figure 1. These concepts can be understood along a spectrum, ranging from the backup and preservation of critical data assets to enabling states to operate, serve and scale beyond their physical borders, especially amid disruption and change.

FIGURE 1

The spectrum of "embassy" models

Concept	Meaning
Data embassy	Legally protected cross-border storage or backup of critical sovereign data and systems, primarily for preservation and recovery.
Digital embassy	A broader arrangement that may include live systems, operational continuity, trusted cloud environments and, in some cases, AI or compute workloads.
Sovereign cloud/sovereign hosting	Protected hosting under legal/technical safeguards, but not necessarily an embassy model.
External AI/compute access	Access to compute and advanced infrastructure, which may support digital-embassy objectives, but is not automatically a digital embassy.

Source: TBI

The defining feature of a digital embassy is not simply that infrastructure is located abroad. Governments already use foreign cloud providers, cross-border backups and international technology services. What makes the digital-embassy model distinct is the combination of sovereign purpose, legal protection, trusted host arrangements, technical control, operational continuity and political accountability.

Data Embassies

Estonia became the first state to conceptualise and operationalise a data embassy,[10] signing an agreement with Luxembourg.[11] At its core, a data embassy enables a state to store or back up critical government data and systems in infrastructure located in another jurisdiction while retaining sovereign control through a combination of legal, organisational and technical arrangements.[12] This is a departure from the traditional assumption that the state's most sensitive data and systems must not leave its national borders. The purpose is to create a trusted and protected extension of sovereign digital infrastructure beyond territorial borders, without transferring authority over the underlying systems and data.[13]

The Estonian model remains the most mature and operationalised example of how this arrangement functions in practice. It illustrates not only the technical architecture of a data embassy, but also the legal, institutional and strategic choices required to make such an arrangement viable.[14] What distinguishes the model is the way it combines sovereign control, foreign physical infrastructure and private-sector provision within a single continuity architecture. Estonia retains authority over its data, including encryption, access management and governance, while the infrastructure is located outside its territory in a trusted jurisdiction.

It is important that data embassies are not conflated with every form of sovereign cloud, cross-border backup or government use of hyperscalers. The distinguishing characteristic is the governance and legal-protection arrangements built in around continuity, sovereign control and political trust between states.[15] These arrangements do not fall under existing diplomatic law and frameworks such as the Vienna Convention. For example, in the case of Estonia, the main innovation was not so much the technological implementation, but the bilateral agreement that was signed to interpret the Estonian data embassy "in the spirit of the Vienna Convention … despite not being located within a traditional diplomatic mission".[16]

Data embassies therefore rely on novel legal constructs, governed by bespoke bilateral agreements that define jurisdiction, access rights and protections for digital assets. Under this model, the host state guarantees non-interference, security and continuity of access, while the originating state retains authority over its data and systems. In effect, this creates a legally protected extension of the state's digital infrastructure beyond its territorial boundaries, without transferring sovereignty over the underlying assets.

The Estonian model is therefore best understood first as a continuity mechanism, rather than as a general-purpose sovereignty solution. Its purpose is to preserve the state's digital core. Its replication in more limited form, including a similar "e-embassy" agreement between Luxembourg and Monaco,[17] suggests that the approach may be transferable, particularly for

smaller or highly digitalised states seeking to reduce systemic vulnerability. Estonia's data embassy remains the most mature operational reference point for the wider digital-embassy debate.

Digital Embassies

The move from data embassies to digital embassies marks a shift from static backup to operational continuity. Where the original model focused on preserving critical data for recovery, the emerging model asks whether the state can continue to operate, deliver services and access critical infrastructure when domestic systems are unavailable or insufficient. This shift is driven by two pressures: the growing vulnerability of digital infrastructure to physical and cyber disruption, and the increasing concentration of the cloud, compute and AI capabilities on which modern states depend.[18]

The strategic relevance of digital embassies is growing as the threat environment and the state's infrastructure requirements evolve. Attacks on digital infrastructure, government data centres, communications networks and other soft targets have shown that the physical foundations of the digital world are vulnerable to disruption. Ukraine's experience is particularly important. In the early phase of Russia's invasion, Ukrainian government data centres, networks and administrative systems were targeted as part of efforts to degrade state capacity. Ukraine's subsequent migration of data and services helped preserve digital continuity, but much of this relied on emergency partnerships with major technology providers rather than pre-existing sovereign arrangements.[19,20,21] This strengthens the case for governments to prepare legal, operational and technical continuity mechanisms before a crisis occurs.

At the same time, governments are beginning to adopt AI-enabled, increasingly agentic forms of administration and service delivery.[22] This requires secure cloud environments, high-performance compute, resilient connectivity, scalable infrastructure and access to rapidly evolving AI capabilities. These systems are capital-intensive, energy-intensive and concentrated in a small number of jurisdictions and providers. For many

states, including advanced economies, full domestic provision will be difficult, costly or strategically inefficient. The question for policymakers is therefore not simply how to build everything at home, but how to decide what must run domestically, what can be run with trusted partners and allies, and what can be externalised under clear legal, technical and political safeguards.

For states that cannot sustain frontier-scale infrastructure on their own, digital-embassy-style arrangements could help crowd in demand, aggregate sovereign workloads and make investment in cloud, compute or AI infrastructure more viable. For potential host states, this could offer a route to attracting hyperscalers and strategic technology investment that would not be justified by domestic demand alone. For guest states, it could provide access to compute or trusted cloud capacity that would otherwise be unavailable or unaffordable. In this sense, digital embassies go beyond simply protecting a state from disruption and play a key role in a broader strategy for AI sovereignty, allowing governments to preserve agency while participating in infrastructure ecosystems that no single state can fully control.

Digital embassies are therefore about more than resilience and security alone. They can help preserve the state's functioning amid disruption, support the delivery of services to citizens beyond national territory, and create new forms of cooperation between guest and host countries. Over time, they may become an increasingly important diplomatic and strategic instrument – a means to strengthen alliances, build technology partnerships and structure interdependence in a world where digital sovereignty depends not on isolation but on trusted collaboration.

The Digital Embassy Spectrum

To help understand the full spectrum – from data to digital embassies – this paper introduces a three-layered and four-tiered framework. At one end, critical data can be securely stored and recovered in the event of a disruption; at the other, digital embassies may support the operation of live

systems or provide access to compute and AI infrastructure at scale. Between these points, different models introduce varying levels of integration, dependency and governance complexity.

RESILIENCE LAYER

- Tier 1: Preservation – secure backup of critical state data and systems to ensure recovery after disruption.
- Tier 2: Technical continuity – the ability to restore and run essential state systems from abroad when domestic operations are disrupted. This tier is ultimately about systems, and whether the state can technically restore and run its essential digital infrastructure and continue operation from abroad. It assumes that normal domestic institutions can still function.

SERVICE-CONTINUITY LAYER

- Tier 3: Operational continuity – the ability to continue core state functions, even when territory, infrastructure or population location is disrupted through host-country-based infrastructure and operational arrangements, including, if necessary, through host-country information systems. This tier is ultimately about institutions and services, asking whether the state can continue to exercise core functions and deliver services even when the normal domestic administration is disrupted.

CAPABILITY LAYER

- Tier 4: Capability – trusted access to external compute, cloud or AI for workloads that a state cannot build or run domestically at scale. For example, a government operating large-scale AI-enabled public services may rely on compute infrastructure that cannot be easily rebuilt domestically in the event of disruption. If domestic AI infrastructure is damaged, degraded or insufficient, trusted external compute environments may allow critical sovereign workloads to continue operating while preserving legal, operational and security safeguards appropriate to the workload's sensitivity.

These tiers are not exhaustive or mutually exclusive and will often operate in combination. They nonetheless provide a practical framework for aligning policy choices with strategic intent by clarifying the distinction between resilience measures (redundancy and continuity) and more advanced capability-building investments. As states move from resilience to continuity and increasingly to capability, the costs, risks and governance requirements increase.

While Tier 1 is relatively well-established, Tiers 2 to 4 remain less tested and involve more demanding legal, operational and technical arrangements. Tiers 2 and 3 require stronger legal, institutional and operational arrangements because they move beyond backup to live operations and service delivery. Tier 4 introduces a distinct category of strategic exposure because capability at scale often depends not only on host states but also on trusted technology providers. As a result, host-state legal guarantees alone may not fully address risks related to provider access, embargoes, compute allocation or platform governance. Not all states will need – or be able – to operate at the highest level. A structured approach allows governments to align ambition with risk, and to expand incrementally as confidence, capability and trust develop.

FIGURE 2

The tier framework in practice

Tier	Core question	Main purpose	Main risk
1. Preservation	Can critical data and systems be recovered?	Backup and recovery	Data integrity, access, legal protection
2. Technical continuity	Can essential systems run from abroad?	System restoration and operation	Failover, interoperability, connectivity
3. Operational continuity	Can the state still serve people and exercise authority?	Service and institutional continuity	Legal authority, access, citizen trust
4. Capability access	Can the state access cloud/AI/compute capacity?	Strategic capability	Provider dependence, export controls, lock-in

Source: TBI

02

Different Strategic Roles: Guests and Hosts

Decisions on how digital embassies fit into a country's overall strategy vary widely. Their importance and risks depend on what role a country chooses in a global system of digital infrastructure and governance. Assuming that all countries face the same choices masks key strategic differences. One country might outsource parts of its sovereign infrastructure to boost resilience, improve access or avoid single points of failure. Another might host others' systems for economic, diplomatic or strategic reasons. Countries could also do both. These setups can be bilateral, multilateral, alliance-based or spread across multiple trusted jurisdictions.

As the concept of digital embassies continues to gain traction, it will become an essential component of any country's strategy for digital sovereignty, infrastructure access and technological capabilities. For guest states, the question is how and where digital-embassy-style arrangements fit within their broader resilience, security and AI-capability strategies. For host states, the question is how they can credibly provide trusted environments for sovereign workloads, whether doing so aligns with their strategic and economic objectives, and what forms of influence or risk such arrangements entail.

These arrangements are most likely to emerge first among trusted partners. Because digital embassies depend on legal reliability, political trust, operational cooperation and confidence under stress, it may make sense for states to begin within existing institutions, such as NATO, AUKUS or the EU, before broadening their resilience architecture. Over time, these arrangements could evolve from bilateral continuity mechanisms into wider networks of trusted sovereign infrastructure.

However, the practical models for digital embassies are likely to differ significantly across regions. States with advanced digital infrastructure, mature cloud ecosystems and strong alliance structures may approach digital embassies differently from regions where connectivity gaps, financing

constraints, energy availability or institutional capacity remain more uneven. In some contexts, the priority may be continuity and resilience; in others, it may be collective access to compute, cloud infrastructure or shared digital capability through regional cooperation and demand aggregation.

Digital-embassy strategies also require clear governance inside government. States will need to decide who owns the risk, who classifies systems as eligible, who negotiates and manages host-state relationships, who oversees providers, who approves activation, how incident escalation works, and how audit, assurance and accountability are maintained over time. Without this, digital embassies risk becoming infrastructure projects rather than sovereign-resilience arrangements.

The technical architecture should be designed from the outset for control, reversibility and operational continuity. This requires clear arrangements for key management, identity and privileged access management, recovery procedures, logging, monitoring, failover triggers, operational playbooks, and portability across providers or hosting environments. The objective should be to ensure that the state can retain control, restore services, switch environments and verify system integrity even during disruption, dependency failure or under geopolitical pressure.

Whether a country decides to use or host a digital embassy will be shaped by its geography, regulatory environment, energy availability, security posture and geopolitical alignment. For host countries, digital embassies may offer a way to position themselves within the emerging architecture of global digital and AI infrastructure by attracting investment, aggregating sovereign workloads and deepening technological partnerships. But this cannot be a one-way source of leverage. Credible arrangements must be based on mutual guarantees in which host states provide legal protections, non-interference commitments, continuity of access and technical safeguards, while guest states commit to long-term partnership, shared standards and reciprocal cooperation. Done well, digital embassies can strengthen strategic relationships by creating shared stakes in resilience, security and technological capability.

The following sections assess these roles in turn, outlining why states may choose to use or host digital embassies, and what opportunities, risks and constraints each pathway creates.

Guest States

For guest states, there are two primary reasons to use digital embassies abroad. The first is to improve resilience, manage vulnerability, and ensure continuity for critical state systems and public services. This desire is driven by the growing criticality of digital infrastructure, combined with an increasingly unstable geopolitical environment defined by rising conflict, crises and instability. Externalised, legally protected and geographically distributed infrastructure can help reduce single points of failure, spread risk and strengthen resilience.

The second is a capability constraint. Many states will not be able to build enough AI infrastructure domestically at a meaningful scale.[23,24] For them, the attraction of digital-embassy-like arrangements may extend beyond continuity to access; in other words, trusted data-processing environments, secure cloud capacity, or compute resources that would otherwise be too costly or slow to establish at home. Together, these factors can push states towards some level of externalisation.

However, they also introduce challenges. Political durability is a central concern. These arrangements depend on trust between states at a time of growing competition and distrust. While risks are often framed in terms of crisis scenarios such as sanctions, more routine pressures may also matter. In a trade dispute, tariffs, regulatory delays or compliance checks could be used to influence access or cost. In such cases, continuity may persist but on less certain terms.

Externalisation also creates new dependencies. Relying on a single host, provider or regulatory system can shift rather than remove risk. Diversifying across locations can reduce physical exposure, but it introduces additional

complexity and cost, along with new dependencies on host jurisdictions, local law, foreign providers, energy systems, and political relationships that may behave differently in times of crisis than in peacetime.

Domestic political legitimacy will be essential. Externalising sovereign systems can be perceived as a loss of control unless governments can explain what is hosted abroad, why it strengthens resilience, what remains under national authority and how citizens' rights are protected.

There is also a lack of clear norms. If a physical embassy is attacked, there are established diplomatic responses. If a digital system hosted abroad is disrupted, the line between a technical failure and a political act is less clear. This raises the question of whether more formal international rules are needed, rather than relying only on bilateral agreements.

Geography also matters. Not all workloads are equally suitable for distant hosting. Backup and recovery functions may tolerate greater distances, but live systems, service delivery and time-sensitive AI or compute workloads may be affected by latency, connectivity resilience and data-transfer constraints.[25] This suggests that states should not treat digital embassies as purely jurisdictional choices. Where operational continuity is important, they may need to begin with trusted partners in closer geographical proximity or within existing regional and security alliances, before scaling outward to more distributed arrangements for less latency-sensitive workloads.

Alongside these risks, there are practical barriers to consider. Legal agreements are often bespoke and take time to negotiate. Technical integration can be difficult, especially where systems and standards differ. Domestic politics may also be a constraint, as externalising core functions can be perceived as a loss of control. Cost is another factor, as these arrangements require investment and ongoing coordination.

External infrastructure cannot replace domestic capability. Cyber-security, regulation and system management still need to be in place at home. Without this, externalisation may increase risk rather than reduce it. For guest states, the central policy question is therefore not whether

externalisation is good in the abstract, but which systems justify it, what must remain under direct national control, and which dependencies are acceptable under today's geopolitical conditions and potential risk scenarios.

Finally, guest states must also determine who has the authority to activate failover or cross-border service delivery during a crisis. If activation depends on ad hoc decisions under stress, continuity may fail when it is most needed.

Host States

For host states, digital embassies are not primarily about their own resilience but about strategic positioning and strengthening domestic capabilities by attracting infrastructure investment, deepening cloud and compute ecosystems, and building stronger public-private operational capacity. Ultimately, the decision to host one or more digital embassies will be driven by a mix of economic and geopolitical ambitions.

For countries with structural advantages, such as cheap, abundant energy, a secure environment and ample land, developing a hosting strategy for digital embassies may be logical. However, hosting digital embassies can also help deepen partnerships, strengthen geopolitical relevance and improve domestic access to cloud, compute and AI infrastructure. For example, in countries where the domestic market is too small to justify major hyperscaler investment, becoming a trusted host for sovereign workloads may be one of the few viable ways to aggregate demand at sufficient scale.

By combining domestic demand with workloads from partner governments, host states can attract investment in cloud, compute and AI infrastructure that would otherwise not materialise. Given the inherently political nature of digital embassies, any country acting as a host must work to build trust and credibility, as guest states are likely to favour jurisdictions with stable political systems, reliable legal frameworks, and mature relationships among government, regulators and industry. This can be done, for example, by establishing clear protections, non-interference commitments and

continuity guarantees to reassure guest states that hosting will strengthen resilience rather than create a new point of dependence. Host states will also need the institutional capacity to manage these arrangements over time, including oversight of providers, incident-response coordination, security assurance and clear points of contact with guest governments.

The more effectively host states attract digital embassies to their territory, the greater the risk that they could be drawn into the political and security dynamics of the countries they support. A host state is not merely providing infrastructure; it is accepting a role in the continuity architecture of another state. That creates diplomatic, legal, operational and security obligations that must be understood before such arrangements are offered. During conflicts or periods of heightened mistrust, host countries may face competing pressures from other partners, allies or internal political forces. Host countries cannot assume that existing defence guarantees will automatically extend to sovereign data or systems located on their territory. If a hosted digital embassy is attacked or disrupted, the legal and political response may be unclear, particularly where the guest state, host state and relevant alliances do not overlap. Host states should therefore ensure that agreements clearly define legal status, protection obligations, escalation pathways and mutual-assistance arrangements in advance.

Being an effective host country for digital embassies will not be easy, and there are significant barriers to entry. Hosting at scale requires substantial investment in infrastructure, energy and connectivity, as well as the ability to meet high technical and security standards. Much of the underlying infrastructure is likely to be built, operated or maintained by private industry, meaning that host states will need strong public-private partnerships, clear accountability between government and providers, and an ecosystem of trusted technology providers capable of delivering secure, high-availability infrastructure. These partnerships should define not only delivery responsibilities but also requirements for security, resilience, auditability, incident response and operational control.

Hosting can therefore generate influence, but also liability. The strategic question for potential hosts is whether they are prepared to convert infrastructure, law and trust into a long-term sovereign service offering, and whether doing so aligns with their wider security, economic and foreign-policy objectives.

Open Questions for Policymakers

Despite growing interest and practical relevance, several open questions about digital embassies remain. First, demand remains uncertain. While digital embassies are likely to be highly useful, it is not yet clear how many governments may be willing to externalise critical sovereign workloads in practice, at what scale or for which use cases. Demand is therefore likely to vary significantly between backup and recovery, live-system continuity, public-service delivery and access to advanced AI infrastructure.

Second, the economics are not yet proven. Digital embassies require upfront investment and long-term operational spending on cyber-security, physical security, compliance and maintenance. These costs will increase as arrangements move from backup and recovery towards live systems and AI workloads. It remains unclear whether hosting sovereign workloads can generate enough durable demand to justify large-scale cloud, compute or AI-infrastructure investment.

Third, legal and political guarantees remain underdeveloped. Bilateral agreements can define jurisdiction, access rights, non-interference commitments, liability and dispute resolution, but their credibility under pressure is uncertain. The hardest questions arise during periods of political tension, economic coercion or armed conflict. Addressing these questions does not necessarily require restrictive or discriminatory regulation. In many cases, risk-based, outcome-focused and non-discriminatory approaches may be more effective, particularly where digital-embassy arrangements combine strong technical controls, provider accountability, interoperability and enforceable service obligations.

Fourth, operational viability remains uneven across use cases. Backup and recovery are comparatively well understood, but live systems, service delivery and AI workloads introduce more demanding requirements.

Operational viability will also depend on portability and interoperability. Systems that are highly bespoke, dependent on legacy architecture or locked into one provider may be difficult to replicate, migrate or restore across borders. Advanced-AI workloads add further complexity because they depend on compute availability, energy supply, model governance, export controls, platform rules and provider reliability.

Fifth, provider dependence remains a core risk. Even where arrangements are legally framed as state-to-state partnerships, much of the underlying infrastructure may depend on private providers, subcontractors, software-update channels, support teams, semiconductor supply chains, energy systems and export-control environments. Governments will need to understand where operational control actually sits and which actors could become points of leverage or failure.

Finally, the governance model is still emerging. Digital embassies require more than legal agreements and infrastructure. They depend on public-private coordination, clear accountability between governments and providers, technical safeguards such as encryption and segmentation, institutional capacity to oversee arrangements, and mechanisms for testing resilience over time. They may also require broader alliance-based, regional or international norms if bilateral agreements prove insufficient.

These uncertainties do not weaken the case for digital embassies, but they do suggest that governments should proceed incrementally: starting with clearly defined use cases, testing arrangements under stress, and scaling only where demand, economics, legal protections and operational performance are credible.

03

From Concept to Reality: Recommendations

Digital embassies are not a standard or universally applicable solution. Their value depends on their design, the conditions under which they operate, and how they fit within a state's broader digital and AI strategy. The considerations set out in the following sections are intended to help policymakers assess where and how digital embassies could be integrated into these strategies. They apply to both states seeking to use such arrangements and those considering hosting them. The underlying questions are similar, but the practical implications differ depending on the role a state plays.

It is also important to distinguish between levels of ambition. Data embassies, understood as mechanisms for secure backup and recovery, represent a more established and bounded use case. As states look beyond resilience towards live systems, service delivery and, in some cases, access to compute and AI capabilities, digital embassies may be more appropriate but the costs and risks may escalate. These choices are not binary but fall along a spectrum, with states adopting different roles and levels of exposure depending on their context. Taken together, the following considerations are intended as a guide rather than a fixed model.

Maintain Critical State Functions

Any digital-embassy strategy must begin with a strict understanding and prioritisation of which data and services are critical sovereign functions. Not every government service or data set will be mission-critical, so states should prioritise ensuring resilience and continuity for those that are.

For guest states, this requires governments to identify and formally designate systems essential to state continuity, including core registries, identity infrastructure and critical administrative platforms. Policymakers must define clear resilience requirements for these systems, including acceptable downtime and recovery expectations, and assess whether these

can be met domestically. Cross-border arrangements may strengthen resilience, particularly for systems where disruption would have systemic consequences. Externalisation should therefore be applied selectively and prioritised based on impact.

Governments will also need clearer ways to classify sovereign data, systems and workloads based on their sensitivity and operational requirements. Not all state data require the same level of protection or territorial control. Some workloads, particularly those involving confidential but non-strategic data, may be suitable for trusted external environments under strong legal and technical safeguards, while others involving highly sensitive national security, intelligence or core sovereign functions may require stricter domestic control. Developing shared classification frameworks could help governments make more consistent decisions about what can be externalised, under what conditions and with which safeguards.

For host states, the parallel judgement concerns scope and risk. Governments must define the categories of foreign sovereign systems they are willing to host, distinguishing between lower-risk data storage and more sensitive or operational workloads. These decisions carry political, legal and security implications, particularly where hosted systems may become relevant in periods of tension. Clear boundaries are therefore required to ensure that hosting strategies align with national capacity, alliance commitments and domestic political constraints.

CONSIDERATIONS

- Define what is truly mission critical. Identify and formally designate the systems essential to state continuity – such as identity, core registries and critical administrative platforms – and clearly distinguish them from broader government IT.
- Develop risk-based classification frameworks for sovereign data and workloads. Distinguish between public, sensitive, confidential and highly restricted workloads, identifying which can be externalised under trusted safeguards and which require stricter domestic control.

- Set resilience standards and test domestic limits. Establish explicit continuity requirements, including acceptable downtime and recovery thresholds, and assess whether these can be credibly met within the national infrastructure before considering externalisation.
- Externalise selectively and within clear boundaries. Use cross-border arrangements only where they materially strengthen resilience for high-impact systems, while defining strict limits on what can be hosted, aligned with national security, political constraints and institutional capacity.
- Distinguish between system continuity and service continuity. Identify not only which systems must survive, but which public services must still be deliverable to citizens, businesses and public authorities, including when users and administrators are outside national territory.
- Plan for continuity of the state–citizen relationship. Ensure that the systems prioritised for continuity support essential functions such as identification, authentication, records access, payments and communication with citizens abroad or in displacement.
- Define activation thresholds in advance. Establish the legal and operational conditions under which services, failover arrangements or cross-border delivery mechanisms would be activated, rather than leaving these decisions to crisis conditions.

Preserve Sovereign Control Through Interdependence

Digital embassies should be seen as a tool to help shape interdependence and increase resilience. This requires deliberate effort to build trusted ecosystems in which states, allies and technology providers can share infrastructure and capabilities while preserving national agency and limiting exposure to coercion or disruption. Success will depend on the choice of partners, the credibility of legal guarantees, the interoperability of systems, and the technical controls that determine who can access, operate and secure critical functions.

For guest states, governments must select host partners and technology providers based on clear criteria, including legal reliability, institutional stability, geopolitical alignment, technical capability and exposure to external pressure. Major technology providers will often be essential to delivering the scale, security and resilience these arrangements require. The policy challenge is not to avoid them, but to ensure that reliance on any provider, jurisdiction or regulatory system is appropriate to the sensitivity of the workload and supported by clear safeguards. Where critical functions are involved, this should include requirements for interoperability, portability, continuity planning and credible exit options.

For host states, the challenge is to provide credible assurances of non-interference while retaining sufficient control to meet domestic legal and security obligations. This requires legal and institutional frameworks that clearly define rights and responsibilities, ensure enforceability under domestic law, and provide confidence to partner states. Oversight mechanisms are also required to monitor infrastructure, providers and compliance, ensuring that hosting arrangements do not create unmanaged risks within the domestic system.

Poorly structured arrangements risk exposing host states to political, legal or security liabilities beyond their control. Conversely, well-designed models can enable host states to convert infrastructure, law and trust into a credible sovereign service offering, while ensuring that hosting strengthens rather than undermines their domestic resilience, alliance commitments and security interests.

CONSIDERATIONS

- Define non-transferable sovereign control functions. Make explicit which elements must remain under direct national authority at all times, including cryptographic controls, identity governance, access management, auditability and core decision-making rules.

- Use risk-based partner and provider selection. Assess jurisdictions and providers based on legal reliability, institutional stability, geopolitical alignment, technical capability, exposure to external pressure, workload sensitivity, and the robustness of legal and technical safeguards, rather than assuming that domestic or regional provision is inherently safer.
- Build interoperability, portability and exit into the design. Ensure systems can be moved, restored or reconstituted across environments so that resilience does not become locked in to a single host, provider, architecture or regulatory regime.
- Design for stress, not stability. Make explicit which dependencies are acceptable under normal conditions and which become intolerable in a crisis, and back this up with enforceable guarantees, oversight mechanisms and operational safeguards that remain credible under political, economic or security pressure.

Stress-Test Digital-Embassy Arrangements

Too often, debates about resilience and technological sovereignty assume that more onshoring equates to greater security. Yet in today's digital world, strong partnerships are a core component of resilience. Going it alone can produce a weaker, less secure and less efficient digital ecosystem. For many functions, trusted externalisation can provide greater redundancy, optionality and resilience than keeping everything at home. The issue is therefore not externalisation itself, but whether the arrangements governing it can withstand the conditions in which they are most likely to matter. Digital embassies must be designed, governed and tested for moments of disruption, including cyber incidents, infrastructure failures, geopolitical tensions, economic coercion and armed conflict.

For guest states, this requires moving beyond formal agreements to practical assurance. Bilateral arrangements must clearly define jurisdiction, access rights, non-interference commitments and responsibilities in the event of disruption. However, legal provisions alone are insufficient. Arrangements should be regularly tested through exercises and scenario planning to assess how they would function under realistic stress conditions.

Without this, there is a risk that continuity exists in principle but fails in practice. For some states, particularly those operating within close security partnerships, this may also argue for exploring alliance-based or distributed models rather than relying solely on a single bilateral arrangement. Two-way partnerships, or wider distributed arrangements across trusted jurisdictions, may offer greater resilience and political credibility under stress than dependence on a single host.

For host states, credibility depends on the ability to sustain trust under pressure. Legal frameworks must be robust, enforceable and capable of operating under political or economic strain, including clear commitments on non-interference and continuity of access. This must be matched by investment in cyber-security, monitoring and incident-response capabilities that are proportionate to the sensitivity of the systems being hosted. Clear governance structures are required to define roles and responsibilities across public and private actors, and, where appropriate, joint testing with partner states can help demonstrate reliability and build confidence over time. For hosts operating within alliance structures, there may also be value in embedding digital-embassy arrangements within wider security and political relationships, rather than treating them as stand-alone technical agreements.

CONSIDERATIONS

- Codify enforceable access and operating rights, not just principles. Bilateral or multilateral agreements should define jurisdiction, access rights, activation thresholds, continuity obligations, non-interference commitments, liability, dispute resolution and responsibilities during disruption.
- Back legal guarantees with technical and operational safeguards. These should include redundancy, segmentation, encryption, access controls, audit logs, incident-response protocols, escalation pathways and tested response procedures.

- Test arrangements under realistic stress conditions. Governments should run joint exercises and scenario planning for cyber incidents, infrastructure failure, geopolitical tension, economic coercion, sanctions and armed conflict, so that continuity does not exist only in principle.
- Assess dependencies across the full delivery chain. Evaluate not only the host jurisdiction, but also providers, subcontractors, support models, telecoms links, software-update channels and external AI or cloud control layers that may become points of leverage or failure.
- Explore alliance-based, two-way or distributed arrangements where appropriate. Where political and strategic conditions allow, these models can reduce dependence on any single host and strengthen credibility under stress.
- Preserve reversibility and guard against asymmetric dependence. Avoid arrangements that create irreversible lock-in to a single jurisdiction, provider or service model, particularly where dependency may deepen over time or create soft leverage over the guest state.

04

Conclusion

The growing interest in and importance of digital embassies are representative of the wider shift in how state power, resilience and sovereignty are organised in an era where critical digital infrastructure is capital-intensive, geographically concentrated and politically exposed. As AI systems become more deeply embedded across government and the economy, states will depend not only on data and software, but also on cloud, compute, energy, connectivity, hardware and trusted providers that may sit beyond their territorial borders.

This makes digital embassies increasingly important for both resilience and security. In their original form, data embassies addressed continuity by ensuring that critical state data and systems could survive a failure of domestic infrastructure. In their emerging form, digital embassies go further. They may support live systems, service continuity, and access to the infrastructure required to operate, govern and compete in an AI-enabled world. As states become more dependent on external infrastructure, digital embassies provide a concrete mechanism for deliberately, transparently and securely shaping these dependencies.

For most states, full technological self-sufficiency is neither realistic nor desirable; the challenge is to find a viable middle ground. Digital embassies provide one way to do this. Properly designed, they can help states distribute risk, preserve continuity, access capability and deepen trusted partnerships. They demonstrate that sovereignty is not always strengthened by keeping everything at home; in some cases, it is strengthened through carefully governed interdependence with allies, partners and trusted technology providers.

Getting this right will require action sooner rather than later. Digital-embassy arrangements cannot be improvised during a crisis. Governments need to identify which systems and services must remain operational under all circumstances, determine what must stay under direct national control, select partners carefully, build interoperability and exit options, and test legal, technical and operational arrangements before they are needed. Host

states must also decide whether they can credibly provide trusted environments for sovereign workloads, and whether doing so aligns with their economic, security and foreign-policy objectives.

Approached thoughtfully, digital embassies can become an essential component of modern digital sovereignty by offering a practical instrument for strengthening resilience, preserving agency, building alliances, and ensuring that states can continue to function in a more concentrated and contested digital order.

Endnotes

1 https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

2 https://en.yna.co.kr/view/AEN20250930001552315

3 https://www.bbc.co.uk/news/articles/cgk28nj0lrjo

4 https://icct.nl/publication/war-against-technology-analysis-recent-developments-anti-technology-violence

5 https://www.goldmansachs.com/insights/articles/tracking-trillions-the-assumptions-shaping-scale-of-the-ai-build-out

6 https://reports.weforum.org/docs/WEF%5FAI%5FInfrastructure%5Fin%5Fthe%5FAge%5Fof%5FSovereignty%5FRequirements%5FStrategies%5Fand%5Fa%5FTrusted%5FFramework%5Ffor%5FDigital%5FEmbassies%5F2026.pdf

7 https://web.archive.org/web/20190914014800/https://www.mkm.ee/sites/default/files/implementation%5Fof%5Fthe%5Fvirtual%5Fdata%5Fembassy%5Fsolution%5Fsummary%5Freport.pdf

8 https://www.g42.ai/resources/news/g42-introduces-digital-embassies-and-greenshield-make-ai-sovereignty-portable

9 https://e-estonia.com/wp-content/uploads/factsheet%5Fdata%5Fembassy.pdf

10 https://blogs.microsoft.com/eupolicy/2017/12/14/diplomatic-immunity-data-estonia-creates-virtual-embassy/

11 https://estonianworld.com/security/estonia-open-worlds-first-data-embassy-luxembourg/

12 Kotka T, & Liiv I, "Concept of Estonian Government Cloud and Data Embassies", *International Conference on Electronic Government and the Information Systems Perspective* (pp. 149–162). Cham: Springer International Publishing; 2015.

13 https://cloud.google.com/blog/products/identity-security/data-embassies-strengthening-resiliency-with-sovereignty

14 Kotka T, Kask L, Raudsepp K, Storch T, Radloff R, & Liiv I, "Policy and Legal Environment Analysis for E-Government Services Migration to the Public Cloud", *Proceedings of the 9th International Conference on Theory and Practice of Electronic Governance* (pp. 103-108; 2016).

15 https://www.riigiteataja.ee/aktilisa/2280/3201/8002/Lux%5FInfo%5FAgreement.pdf

16 Robinson N, Kask L, & Krimmer R, "The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis", ***Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance*** (pp. 391-396; 2019).

17 https://luxembourg.public.lu/en/invest/innovation/e-embassies-in-luxembourg.html

18 https://nortal.com/hubfs/gov%5Fresilience%5Fweb.pdf

19 https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data

20 https://www.atlanticcouncil.org/in-depth-research-reports/report/building-the-digital-front-line/

21 https://www.infosecurity-magazine.com/interviews/interview-microsoft-migrating-data/

22 https://agenticstate.org/

23 https://www.nytimes.com/interactive/2025/06/23/technology/ai-computing-global-divide.html

24 https://www.economist.com/leaders/2026/04/30/the-ai-supply-crunch-is-here

25 https://www.goldmansachs.com/what-we-do/investment-banking/insights/articles/powering-the-ai-era/report.pdf

TONY BLAIR
INSTITUTE FOR
GLOBAL CHANGE

Follow us

facebook.com/instituteglobal

x.com/instituteGC

instagram.com/institutegc

General enquiries

info@institute.global