The Digital Sovereign Stack

A Framework for Small Nations

by
Nouf Almarri

The Digital Sovereign Stack

A Framework for Small Nations

by

Nouf Almarri

Working Paper · Version 0.1
Doha, 2026

Contents

1. The Strategic Question

Small nations have always faced a different version of the sovereignty question than larger ones. Where larger states can ask *what should we control?* and afford to debate the answer at length, smaller states must ask *what can we not afford to fail to control?* — the harder question, asked under harder constraints. The digital era has not changed this question. It has sharpened it.

The conventional framing of digital sovereignty — own everything, avoid foreign dependence, repatriate critical systems — does not survive contact with operational reality. Talent is bounded by population. Capital is bounded by scale. Time is bounded by the pace of global technological change. No small state can credibly build every layer of its digital infrastructure, and most should not attempt to. Those who have tried have learned the lesson at expensive scale.

Estonia learned the lesson in 2007, when state-sponsored cyberattacks revealed how exposed its young digital infrastructure had become. The country rebuilt with sovereignty as a founding principle, and the system that emerged became the global reference case for what small-nation digital sovereignty can look like when designed deliberately rather than discovered under pressure. The question reaches every small nation eventually. The only variable is whether it arrives before or after the choice has already been made.

What small nations can do — and what this paper argues they must — is decide with precision which layers of the digital stack are non-negotiable,

which can safely depend on global partnerships, and what foundation underlies any of these choices. The framework that follows identifies five such layers, and argues that the foundation beneath them — sovereign talent capability — is the actual rate-limiting factor in this work.

The case being made here is not for total digital independence, which is impossible for small nations, nor for full integration into global platforms, which is increasingly dangerous. The case is for *layered sovereignty*: a clear-eyed assessment of what must be claimed, what can be borrowed, and what cannot be done without people. The framework — referred to throughout this paper as *the Digital Sovereign Stack* — is offered for the policymakers, leaders, and senior technologists of small advanced economies whose strategic advantage is decisiveness, whose primary constraint is scale, and whose window for these decisions is closing.

There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things.

— Niccolò Machiavelli, The Prince (1532)

---

2. The Five Layers

The Digital Sovereign Stack identifies five layers at which a small advanced nation must make deliberate sovereignty choices, and one foundation beneath them. The choice of five is not arbitrary. It reflects what a working framework requires: enough granularity to map the actual operational architecture of a modern state, few enough that the framework can be held in a single mind, and bounded such that everything outside the five layers can credibly be procured from global partnerships under the right contractual and legal terms.

The five layers are: national identity and authentication systems; payments and financial rails; critical communications infrastructure; sovereign cloud for government and critical sector data; and AI governance and regulatory capability. Each is treated, in the sections that follow, as a self-contained mini-essay: what the layer is, why it must be sovereign or partially so, what the consequences of foreign dependence look like, what counts as sufficient sovereignty, the canonical example of a small nation that has done this work, and an honest accounting of the trade-offs.

What is deliberately not included in the framework is also worth naming. Productivity software, general-purpose cloud computing for non-sensitive workloads, most enterprise tools, hardware procurement, and the vast majority of consumer-facing technology can safely be sourced from global partnerships, provided the legal architecture around the five sovereign layers is sound. The framework is not a recipe for digital autarky. It is the opposite: a structured argument for which layers must be claimed so that the rest can be confidently borrowed.

The order of the layers, from identity through AI governance, also reflects something about their relationship to one another. Identity is the bedrock; everything else presupposes it. Payments and communications are the operational substrate of daily citizen life. Sovereign cloud is where the state's own data and processes live. AI governance is the layer at which the state determines how the technologies of the present decade are permitted to act within its borders. Each builds on the credibility of the layers below it. A small nation that has built sovereignty unevenly across these layers has built sovereignty unevenly across the substance of its statehood.

Layer 1. National Identity & Authentication Systems

National identity and authentication is the cryptographic infrastructure through which citizens, residents, and entities prove who they are to digital systems — and through which those systems prove their legitimacy in return. It is the layer through which a citizen accesses health records, pays taxes, signs a contract, votes, registers a business, or receives welfare. It is also the layer through which a state recognises its citizens as juridical persons in the digital domain. Every other digital interaction with the state, and most interactions with the private sector, presuppose this layer working correctly.

This layer must be sovereign because it is the foundation of digital citizenship itself. A nation that does not control its own identity system has outsourced the most basic act of statehood: deciding who its citizens are and how their identity is recognised. The cryptographic keys, the registry

of citizens, the protocols by which new identities are issued and old ones revoked, the courts to which disputes are escalated — these are not technical decisions delegable to a foreign vendor. They are constitutional decisions in technical form.

The consequences of foreign dependence at this layer are not theoretical. A nation whose identity provider is a foreign company is one strategic decision away from losing the ability to authenticate its own citizens. A nation whose identity registry sits on infrastructure governed by another country's laws has accepted, implicitly, that another country's courts can compel disclosure of who its citizens are. A nation whose authentication standards are set by a foreign body has accepted that the gate to its own digital state is keyed by another. These dependencies have, in recent years, moved from abstract risks to live concerns for several small nations.

Sufficient sovereignty at this layer does not require domestic invention of every protocol or chip. It requires three things: control of the cryptographic keys that sign and verify identity assertions; control of the citizen registry and the rules by which it is maintained; and the legal and institutional capability to issue, revoke, and arbitrate identities under domestic law. The underlying cryptographic standards may be international; the implementations may use foreign hardware. What must be sovereign is the *operation*: the keys, the registry, the protocols, the courts.

Estonia is the canonical example because it built sovereignty at this layer deliberately, after the lesson of 2007. Today, the Estonian e-ID system issues every citizen a cryptographic identity from birth, governed by Estonian law, operated on infrastructure under Estonian control, and

recognised across the European Union through reciprocity rather than dependence. The system has been continuously operational for over twenty years, has survived multiple geopolitical pressures, and has become the substrate for nearly every other digital service the Estonian state provides. Its design was neither cheap nor fast — Estonia invested in the institutional capability before the technical infrastructure, recognising that the operation of identity is harder than its issuance.

The trade-offs are real and worth naming. Sovereignty at the identity layer requires long-term institutional commitment of a kind few small nations have demonstrated outside the security domain: continuous funding, deep technical capacity within the public sector, legal frameworks that evolve with the technology, and political stability across electoral cycles. Identity infrastructure built in a single political term and then neglected becomes a vulnerability rather than a strength. The choice to make this layer sovereign is therefore not a single decision but a standing commitment — one that several nations have made successfully, and one that several others have abandoned partway through, leaving expensive infrastructure orphaned. The lesson is that sovereignty at this layer cannot be retrofitted under pressure. It must be built before the pressure arrives.

Layer 2. Payments & Financial Rails

National payments and financial rails are the infrastructure through which money moves within a country: between banks, between citizens, between businesses, between government and the public. This layer includes the real-time gross settlement system at the central bank, the inter-bank

clearing rails, the consumer-facing instant transfer schemes, the merchant acceptance standards, and the cross-border linkages by which the domestic system reaches the rest of the world. It is the layer that operates beneath every salary deposit, every bill payment, every welfare disbursement, every tax collection, every retail purchase.

This layer must be sovereign because the ability to move money domestically is constitutive of the modern state itself. A government that cannot pay its employees because its payment processor is unavailable is no longer functionally governing. A central bank that cannot settle inter-bank claims has lost the ability to conduct monetary policy. A retail economy that depends on a single foreign card network to process daily transactions is one strategic decision away from systemic disruption. Payments sovereignty is the technical expression of monetary sovereignty — which most nations consider non-negotiable when expressed in legal terms but treat as optional when expressed in technical terms. The two are the same.

The consequences of foreign dependence at this layer are visible in recent history. Nations that have relied on foreign card networks have seen those networks withdraw service in response to sanctions, sometimes overnight. Nations that have outsourced their core clearing infrastructure to foreign vendors have found those vendors subject to legal regimes outside their control. Nations whose retail merchants depend exclusively on foreign acquirers can find a significant portion of their economy temporarily uncollectable. These are not edge cases. They are the operating environment of the present decade.

Sufficient sovereignty at this layer requires three capabilities. First, a domestic real-time settlement system operated by the central bank, through which all major financial institutions ultimately settle. Second, domestic instant-transfer schemes that allow citizens and businesses to move money to one another without routing through foreign processors. Third, the regulatory and legal framework to define the rules of the system, including who participates, on what terms, and under what oversight. International standards may underlie these capabilities; foreign technology may be used in implementation. What must be sovereign is the operation, the oversight, and the legal regime — not the protocols.

Singapore offers the most instructive case of long-arc payment sovereignty among small advanced nations. The Singaporean architecture has been built across four decades and is now being consolidated for the next. GIRO, the inter-bank direct debit and credit system, has been operational since 1984. FAST, the real-time inter-bank transfer rail, launched in 2014 and uses the ISO 20022 messaging standard. PayNow, launched in 2017, built a proxy-addressing layer on top of FAST that allows citizens to transfer funds using a phone number, identity card number, or business identifier rather than a bank account number. The Singapore Quick Response Code standard, introduced in 2018, unified merchant acceptance across all schemes. Settlement flows through MEPS+, the Monetary Authority of Singapore's real-time gross settlement system. In 2025, recognising that fragmented governance of these schemes was itself becoming a sovereignty risk, MAS and the Association of Banks incorporated a single governing entity, the Singapore Payments Network, to consolidate administration of the country's eight national payment schemes. Cross-border integrations — the PayNow-UPI linkage with India in 2023, the multilateral Project

Nexus signed with four other regional central banks in 2024 — are deliberately structured as interoperability between sovereign systems, not as dependence on a foreign one. The architecture demonstrates a principle worth naming: payment sovereignty is built layer by layer over decades, and is sustained by continuous institutional consolidation.

The trade-offs are substantial. Domestic payment infrastructure requires sustained investment in technology that does not generate revenue in any direct sense. It requires a regulatory body with the technical competence to supervise it. It requires participating banks willing to invest in shared infrastructure rather than purely competitive systems. And it requires the political discipline to resist the apparent efficiency of outsourcing the layer to a foreign provider — an efficiency that disappears the moment the foreign provider's incentives diverge from the nation's. Singapore's success at this layer is, in part, the success of an institutional culture that treats payment infrastructure as public infrastructure of the same kind as water or electricity. Nations that treat payment infrastructure as a commercial service to be procured will struggle to build sovereignty here, regardless of investment level. The first sovereignty choice is institutional. The infrastructure follows.

Layer 3. Critical Communications Infrastructure

Critical communications infrastructure is the physical and logical foundation of a nation's connectivity: the fibre backbone, the submarine cable landings, the mobile network core, the satellite ground stations, the inter-exchange points, and the regulatory and contractual relationships

that determine who operates what and under whose authority. It is the layer that carries voice and data inside a country, between a country and its neighbours, and between a country and the wider internet. When this layer fails, identity systems cannot authenticate, payments cannot settle, government cannot communicate with its citizens, and economic activity contracts to whatever can be done in-person.

This layer must be sovereign because the alternative is having one's national communications operate at the discretion of actors whose interests do not always align with one's own. A foreign-owned mobile network operator answers ultimately to its home regulator, its home shareholders, and its home government's foreign policy. A submarine cable system whose landing rights, repair contracts, and operational control rest with foreign vendors is one geopolitical change away from being unable to repair a fault. A 5G core supplied by a foreign vendor — whose software updates, security patches, and operational telemetry are governed by that vendor's home jurisdiction — is sovereign in name only. Sovereignty at the communications layer is not about ownership of every cable or tower. It is about authority: who decides what runs on the infrastructure, who can be excluded from it, who answers to whom when something goes wrong.

The consequences of insufficient sovereignty at this layer have become legible across recent years. Submarine cables have been damaged, deliberately or accidentally, in ways that revealed how dependent some nations are on a single physical route. Foreign mobile network vendors have been removed from critical infrastructure under sanctions regimes, leaving operators with expensive and slow replacement processes. Satellite constellations have been withdrawn from specific theatres at the discretion

of their commercial operators, demonstrating that connectivity is no longer treated as a neutral utility but as a strategic asset by those who control it. Each of these events forced nations into a sovereignty conversation they had postponed for years.

Sufficient sovereignty at this layer does not require national ownership of every physical asset. It requires three institutional capabilities. First, ultimate authority over the operators of critical communications infrastructure — through ownership, contract, license, or law — sufficient to ensure that critical decisions are taken under the nation's jurisdiction. Second, regulatory and security oversight competent enough to evaluate the technical and geopolitical implications of foreign equipment, contracts, and partnerships. Third, the legal capacity to exclude specific foreign actors from critical infrastructure projects when national security requires it, without rendering the entire telecommunications sector hostile to international investment. The infrastructure may be built and operated by private companies. What must be sovereign is the framework of authority within which they operate.

Switzerland offers a particularly instructive case among small advanced nations because its sovereignty at this layer is institutional rather than physical. Swisscom, the incumbent telecommunications operator, is 51% owned by the Swiss Confederation — a majority stake structured to function as a de facto golden share, giving the federal government direct influence over strategic decisions, board appointments, and any transaction that might dilute its control. The Federal Department of Finance supervises Swisscom against federal policies on universal access, network security, and critical service continuity. In February 2014, the

Federal Council took the more direct step of excluding foreign-held companies from bidding on critical infrastructure projects with a strong information and communications dimension — a decision widely interpreted to cover defense, railways, the energy grid, and the Swiss National Bank's communications. The regulatory architecture has continued to develop. From 1 April 2025, operators of critical infrastructure must report cyberattacks to the Federal Office for Cyber Security within twenty-four hours. The universal service license, which guarantees affordable basic telecommunications across all Swiss regions, was awarded to Swisscom for an eight-year term beginning in 2024. And in 2025, Swisscom launched beem, the world's first telco-delivered sovereign secure access service, operated and governed entirely within Swiss jurisdiction. The Swiss model demonstrates that small nations can maintain communications sovereignty without national champions in every layer of the technology stack — provided the institutional framework is unambiguous about who governs the infrastructure, on what terms, and under whose law.

The trade-offs at this layer are different from the others in the stack. Communications infrastructure is capital-intensive and natural-monopoly-prone; pure market provision tends to concentrate in a small number of operators regardless of national preference. Sovereignty here requires either accepting state ownership of strategic incumbents, constructing strong public-interest licensing regimes around private operators, or building parallel public-sector communications capacity for the most sensitive applications. Each approach involves political and economic costs — state ownership constrains commercial flexibility; strict licensing slows investment; parallel public networks are expensive to

operate at scale. None of these costs is avoidable. The choice is which form of cost a nation is willing to accept, and the worst answer is to refuse to choose, which produces an infrastructure that is neither fully sovereign nor fully market-disciplined. Sovereignty at this layer is the deliberate choice of which constraints to live with.

Layer 4. Sovereign Cloud for Government & Critical Sector Data

The cloud layer is where the data that governs a nation actually lives. It includes the infrastructure on which government services run, the data of citizens held by public agencies, the records of regulated industries — healthcare, finance, defense, energy — and increasingly the operational systems through which states themselves function. Unlike the layers below it, the cloud layer is overwhelmingly delivered today by a small number of global hyperscale providers (Microsoft Azure, Amazon Web Services, Google Cloud), supplemented by national and regional providers of varying scale.

This layer must be partially sovereign because complete cloud sovereignty is, for most small nations, neither achievable nor desirable. Building a domestic hyperscale cloud from scratch would cost billions of dollars and decades of engineering effort, and even if achieved would likely lag global hyperscalers in capability for the duration. At the same time, the layer cannot be entirely surrendered to foreign providers, because the data it holds — citizens' identities, health records, taxation, defense, criminal justice — is the operational substance of statehood itself. A nation that has

placed all of this data on infrastructure governed by another country's laws has accepted, in effect, that another country's courts can adjudicate access to the most sensitive data of its own citizens.

The consequences of this dependency are not theoretical. The Microsoft warrant case, which ran from 2013 to 2018, became the canonical example of the problem: the United States government sought, by domestic warrant, to compel Microsoft to disclose customer emails physically stored in its Dublin data centre. The legal question — whether U.S. law could reach into a foreign jurisdiction through a U.S. company — was answered, before the Supreme Court could rule, by the passage of the CLOUD Act in March 2018, which expressly authorised exactly such reach. The decision did not resolve the underlying conflict between national sovereignty and the operational architecture of global cloud computing. It made the conflict permanent. Every nation hosting data under the control of foreign cloud providers must now reckon with the possibility that the laws governing that data are not its own.

Sufficient sovereignty at this layer therefore requires explicit, layered design rather than physical residency alone. First, the most sensitive categories of data — those that constitute the core of state operation and the most sensitive records of citizens — must reside on infrastructure governed unambiguously by domestic law. Second, the remaining categories may reside on global cloud infrastructure, provided the legal architecture is explicit about what jurisdiction applies, what foreign legal access is possible, and what the contractual and technical mitigations are. Third, the line between these two categories must be drawn deliberately, in policy, with the technical implementations following — not the reverse.

Sufficient sovereignty here is not about where data sits but about which authority adjudicates access to it.

Ireland offers an instructive case precisely because its position is paradoxical. Ireland is, by some measures, the largest single host of European cloud infrastructure: Microsoft, Amazon, Google, and Meta all operate major data centres in or near Dublin, and the Irish Data Protection Commissioner serves as the lead supervisory authority under the General Data Protection Regulation for many of the leading U.S. technology companies operating across Europe. At the same time, Ireland has been building deliberate sovereign cloud capacity for its own state functions, structuring landing zones with foreign hyperscale providers under contracts and architectures designed to preserve Irish and European jurisdictional control. The model that has emerged is not pure isolation nor pure dependence. It is a layered architecture in which data of the highest sensitivity sits in Irish-governed environments, while less sensitive workloads operate on hyperscale infrastructure under contractual arrangements that anticipate jurisdictional conflict. The hyperscale providers, recognising the strategic imperative, have responded: in 2025, both Microsoft and Amazon Web Services launched expanded sovereign cloud offerings for Europe — separately operated infrastructure within Europe, staffed by EU residents and EU citizens, designed to be structurally insulated from foreign legal reach. Whether these offerings deliver on their promises remains to be tested over time. The Irish model anticipates that they may not, and continues to maintain sovereign infrastructure for the cases where they cannot.

The trade-offs at this layer are the sharpest in the stack. National sovereign cloud infrastructure, built from scratch, is prohibitively expensive for most small nations and tends to lag global hyperscalers in capability for the duration of its operation, which means government services become measurably worse than their private-sector counterparts. Hyperscale-delivered sovereign cloud offerings are new, evolving, and unproven across multiple political cycles. Pure hyperscale dependence, as the Microsoft warrant case demonstrated, leaves a nation's most sensitive data subject to foreign legal regimes. There is no clean answer. Each small nation must construct its own layered approach, recognising that sovereignty at this layer is achieved through legal architecture, contractual design, and the explicit classification of data — not through any single technical decision. The work is institutional more than infrastructural, and it must be continuously maintained, because both the legal landscape and the cloud landscape are in active motion.

Layer 5. AI Governance & Regulatory Capability

National AI governance is the legal, regulatory, and institutional capability to determine what artificial intelligence systems are permitted within a nation's borders, on what terms, and with what accountability when they fail. It is the layer at which a nation decides which AI applications its citizens are exposed to in healthcare, hiring, welfare, education, criminal justice, and public administration. It is also the layer at which a nation decides what redress its citizens have when an algorithm decides wrongly about them.

This layer must be sovereign because the alternative is to accept that the AI systems shaping the lives of one's citizens are governed by the choices of foreign companies and the regulatory regimes of foreign governments. A nation that has no domestic AI regulatory authority has, by default, delegated to other jurisdictions the rules that will determine how AI affects its population. Unlike the other layers in this framework, AI governance is not primarily about owning infrastructure or even about national champion firms. Small nations cannot build frontier AI models and most should not attempt to. What they can build, and must, is the regulatory and institutional capability to govern the use of AI within their territory — capability that exists independent of who built the underlying models.

The consequences of insufficient sovereignty at this layer have already begun to materialise. AI systems trained on data from foreign populations and optimised for foreign contexts are now deployed across welfare administration, hiring, lending, healthcare diagnostics, and criminal justice in nations that have no institutional capacity to evaluate their fitness or accountability. When such systems fail — and they have failed, including in advanced economies — the legal and regulatory architecture to investigate the failure, assign responsibility, and remediate the harm is often absent. The capability gap is not theoretical. Several recent high-profile algorithmic failures in welfare administration and public-sector decision-making have demonstrated what happens when AI is deployed at scale in the absence of institutional governance.

Sufficient sovereignty at this layer requires three institutional capabilities. First, a regulatory body with the statutory authority and technical competence to evaluate AI systems against the nation's laws, including its

anti-discrimination, due-process, and data-protection frameworks. Second, mandatory transparency mechanisms — such as public registers of high-impact algorithms used in the public sector — that make AI deployment legible to citizens and other regulators. Third, the legal capacity to require redress when AI systems decide wrongly, including the right of affected citizens to obtain an explanation of an automated decision that has affected them and to appeal it. The underlying models and infrastructure may come from anywhere. What must be sovereign is the regulatory authority itself: who decides what AI may be used, how its harms are remediated, and how its operators are held accountable.

The Netherlands offers the most developed case among small advanced nations because its AI governance architecture has been built deliberately, in part as a response to institutional failure. Following a major scandal involving algorithmic decision-making in the administration of childcare benefits — a system that wrongly flagged thousands of families, predominantly of immigrant background, as fraudulent — the Dutch government built one of the first national AI governance regimes in Europe. The Strategic Action Plan for AI, launched in October 2019 alongside the Dutch AI Coalition, established the country's approach across three pillars: adoption, research, and responsible deployment. The Algorithm Register, launched in December 2022, requires Dutch government organisations to publicly disclose information about the algorithms they use, including high-risk AI systems; by the end of 2025, all central government bodies were required to register their high-risk AI systems in the central public register, which now holds over six hundred entries. The Dutch Data Protection Authority took on the role of algorithm regulator in January 2023, with a dedicated Directorate for Coordination

of Algorithms and the obligation to publish public algorithmic risk reports twice a year. The Court of Audit and the Central Government Audit Service provide additional oversight. The model is being extended: the Netherlands is preparing to expand the Algorithm Register, initially voluntarily and eventually as a mandatory requirement, into critical private-sector industries such as energy and telecommunications, and the legislature is debating a statutory right to explanation in the General Administrative Law Act. The Dutch approach has influenced European Union AI Act implementation across the bloc, demonstrating that a small nation can shape governance at the regulatory layer even when it cannot compete at the infrastructure or frontier-model layer.

The trade-offs at this layer are particular. Building genuine AI governance capability requires senior technical and legal talent of the kind that small nations struggle to recruit and retain — talent that can credibly evaluate machine learning systems against constitutional protections, anti-discrimination law, and procedural fairness. Mandatory transparency regimes can slow government adoption of beneficial AI applications and place a real administrative burden on agencies. Statutory rights of redress against automated decisions create new legal exposure for the state. And regulatory capacity cannot be acquired quickly in a crisis; it must be built before the crisis arrives, then continuously maintained through political cycles in which AI policy is often subordinated to AI investment promotion. None of these costs is avoidable, and the cost of not paying them is higher than the cost of paying them. The lesson from the Netherlands is that AI governance sovereignty is most credibly built by nations willing to learn from their own failures — and that the institutional architecture matters more than the policy declarations.

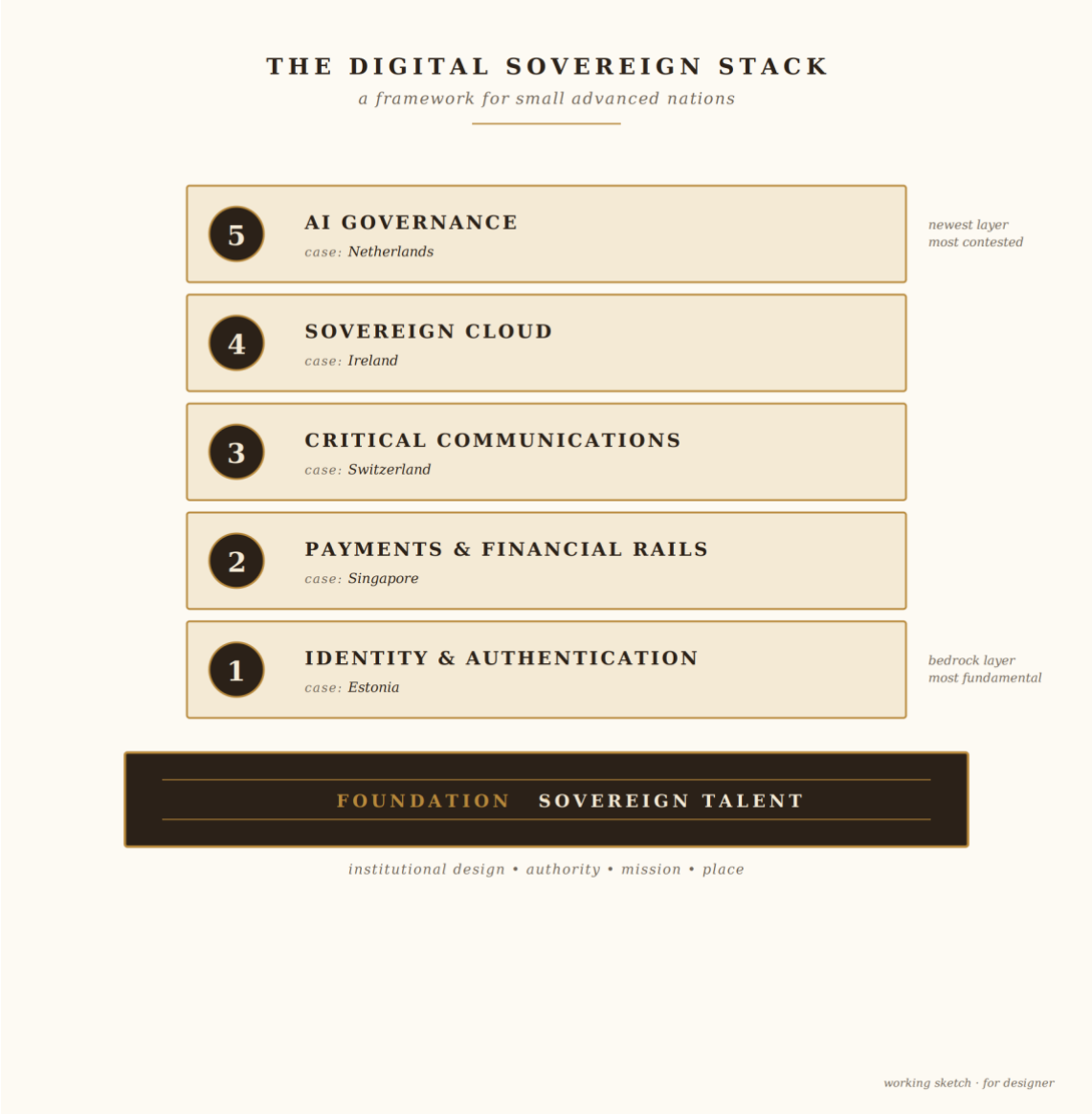

Figure 1. The Digital Sovereign Stack — five layers and one foundation.

Power corresponds to the human ability not just to act but to act in concert.

— Hannah Arendt, On Violence (1970)

---

3. The Foundation — Sovereign Talent

The five layers of the Digital Sovereign Stack all rest on something the framework has so far named only in passing: the human capability to design, operate, regulate, and continuously maintain them. Sovereignty at each of the five layers requires senior technical and institutional leadership — people who can make the consequential decisions, take the consequential risks, and own the consequential outcomes. Without this foundation, sovereignty at any layer is provisional, however well-designed its technical architecture and however well-funded its capital budget. The foundation is talent — but not talent in the recruitment sense.

Small nations are not short of senior tech talent in the sense that recruitment marketing assumes. Most small advanced nations have populations educated to global standards, diaspora networks of senior technologists in major global tech centres, and returning citizens who would consider sovereign or public-sector roles under the right conditions. What small nations lack is the institutional architecture in which senior tech leadership can do meaningful work. The recurring pattern is not that the people are unavailable. It is that when they are placed in roles, the authority to make decisions, the scope to build rather than procure, and the institutional protection to take risks are absent. Senior people, recognising this, leave — or, more commonly, never accept the role.

The systematic mistake small nations make is to treat senior tech leadership as a recruitment problem when it is, in operational reality, an institutional design problem. The successful small advanced nations have built deliberate institutional structures — not the people first, but the

structures first — within which senior people can do consequential work. Estonia created the position of Government Chief Information Officer in 2013, positioned within the Ministry of Economic Affairs and Communications, with explicit authority over state IT strategy, budget, procurement, and the Information System Authority of Estonia. Singapore established the Government Technology Agency in October 2016 as a statutory board reporting directly to the Prime Minister's Office, with broad authority over public-sector digital products, ICT infrastructure, cybersecurity, and procurement. In both cases, the institutional design preceded the talent. The talent — domestic, returning, and recruited — came because the institution offered a clear scope, real authority, and consequential work.

The cost of not doing this institutional work is not visible in any annual budget line. It accumulates over years, in the form of senior departures, vendor capture, project delays, fragmented decision-making, and the gradual erosion of institutional memory as each new minister inherits the previous minister's half-built initiatives. A nation that has not done the institutional design work can run digital strategies and announce digital priorities, but it cannot sustain the senior leadership required to deliver them. The result is a recurring pattern: ambitious launch, capable initial leadership, departure of those leaders within two to four years, replacement by either less senior people or expensive foreign consultants, and a gradual decay of the original ambition into ordinary procurement. The pattern is so consistent across small nations that have skipped this work that it deserves recognition as a structural failure mode, not a series of individual missteps.

The first institutional requirement is real authority to act. Senior tech leaders in small-nation public-sector roles consistently describe the same source of frustration: the inability to move at the pace the work requires. Decisions that should take a week take a year. Hires that should be straightforward become political. Vendors that should be terminated remain. The institutional architecture compatible with senior tech leadership requires that the leadership have, in writing and in practice, the authority to set strategy, to allocate budget, to hire and terminate, to procure and decommission, and to escalate to political leadership when the layer above blocks the work. Without this authority, no compensation package and no recruitment effort will sustain the role.

The second institutional requirement is mission clarity. Senior tech leaders who stay in public-sector or sovereign roles, when asked, point not to compensation but to a clear sense that the work matters at the scale of the nation. This is not abstract. It manifests in articulated strategic priorities, in budget allocations that match those priorities, in political backing that survives ministerial changes, and in a public articulation of what the technology is for that goes beyond efficiency or modernisation. A nation that frames its digital agenda as *improving public services* will not retain senior people for long; the work is too operational to absorb a senior career. A nation that frames the same agenda as building the institutional substrate of digital citizenship for the next century will retain them, even at lower compensation than the private sector offers.

The third institutional requirement, less discussed but no less consequential, is the recognition that senior people have lives. They have spouses with careers, children with schools, parents with health needs,

communities with ties. Small nations attempting to retain or repatriate senior tech leadership through compensation packages alone systematically underestimate the place dimension — the conditions of life that determine whether a senior person can imagine raising a family in a country, sustaining a marriage, being present for a parent's illness. The successful retention and repatriation programmes recognise that talent moves to and stays in places where life is possible, not just where work is paid.

The diaspora question is real but secondary to the institutional question. Small nations have substantial communities of senior tech professionals in global tech centres — citizens who left for opportunity and would consider returning under the right conditions. Repatriation programmes designed primarily as compensation matching exercises usually fail; senior diaspora professionals do not return for compensation parity, which they could obtain by staying. They return when the institutional architecture is unambiguous, the work is consequential, and the place can hold a life. The diaspora is not a recruitment market. It is a population of senior people watching to see whether the institutional conditions in their home country have become serious enough to make return rational.

A pattern visible across more than a decade in decision-making rooms: the senior people who leave are not those whose compensation is lowest, nor those whose mission they doubt. They are those who reach a moment — usually in the second or third year of a sovereign role — when they recognise that the institutional architecture cannot be made to support the work no matter how persistently they push. The senior people who stay are those who, in the same moment, conclude that the institutional

architecture is being built, however slowly, and that their continued presence is part of how it gets built. The variable that determines which conclusion the senior person reaches is not the talent market. It is whether the political leadership has chosen to do the institutional design work or has not.

The Digital Sovereign Stack rests, ultimately, on this foundation. Each of the five layers can be funded, designed, and even partially built without the institutional foundation in place — but none can be sustained. A small nation that has built sovereignty across the five layers but has not done the institutional design work to retain senior leadership has accomplished a sovereignty that will erode within a decade as its current generation of leaders ages out. A small nation that has built the institutional design but not yet all five layers has accomplished something more durable: a foundation on which the layers can continue to be built, by people who have a reason to stay and the authority to do the work. The order matters. The institution is the precondition for the talent, which is the precondition for the layers. And institutional design, more than any technical implementation, is the work that cannot be accelerated in a crisis. It must be done in advance, while there is time.

4. The Closing Window

The argument that small nations have a finite window in which to claim digital sovereignty is not a rhetorical device. It is a structural observation about the technology landscape of the present decade. Three forces are simultaneously consolidating the layers of the global digital stack into fewer hands, fewer jurisdictions, and fewer points of strategic decision. Each of these forces makes sovereignty at a given layer more expensive, more constrained, and less reversible as time passes. Together, they constitute a window — not a closed door, but a steadily narrowing aperture through which small nations must choose whether to act with intent or to find, after some years, that the choice has been made for them.

The first force is the consolidation of frontier artificial intelligence. In 2025, industry produced more than ninety per cent of notable frontier AI models, and a small number of firms — three of which absorb roughly forty per cent of global AI venture investment — set the terms on which most of the world's AI capability is licensed, accessed, and deployed. Adoption is moving faster than any major prior technology cycle: generative AI reached fifty-three per cent population adoption within three years, faster than the personal computer or the internet, with Singapore among the small advanced nations already at penetration rates well above the global mean. Once AI systems are deeply embedded in welfare administration, hiring, healthcare, finance, and public-sector decision-making, the institutional cost of building governance around them rises sharply. The sequence matters: governance built before deployment is cheap; governance built

after deployment is expensive; governance attempted retroactively, in response to a public failure, is often impossible.

The second force is the concentration of the physical substrate on which everything else runs. A single foundry in Taiwan, Taiwan Semiconductor Manufacturing Company, accounts for roughly seventy per cent of global foundry market share and produces over ninety per cent of the world's leading-edge chips. The geopolitical risk this creates is widely understood; what is less often named is the strategic implication for small nations. Sovereign infrastructure at any layer increasingly depends on access to compute that flows through a small number of foundries, subject to export controls, geopolitical constraints, and capacity allocation decisions taken outside the nation's authority. As demand outpaces supply — Morgan Stanley estimates roughly three trillion dollars of AI-related infrastructure investment will flow through the global economy by 2028 — small nations that have not secured their compute strategy will find their sovereignty constrained at the most fundamental layer of all.

The third force is the consolidation of the vendor ecosystem across every layer of the digital stack. Cloud is dominated by three hyperscalers. Frontier AI is dominated by three firms. Telecommunications equipment for critical infrastructure is dominated by a handful of vendors, several of whom are subject to sanctions regimes that limit their participation in particular markets. Identity, payments, and authentication standards are increasingly set by a small number of multinational and supranational bodies whose membership is not open to all nations on equal terms. The choice to be sovereign at any individual layer is becoming more expensive

and less reversible the longer a nation waits, because the alternatives consolidate while the deferred choice ages.

What *too late* looks like is not a single dramatic moment. It is a slow recognition, usually over a five-to-ten-year period, that the sovereignty options once available have narrowed to two: accept the global default, with its embedded jurisdictional dependencies, or undertake an expensive remediation project against entrenched infrastructure, vendor contracts, and citizen habituation. Nations that have reached this point describe similar patterns: a moment in which a foreign legal or commercial decision affects domestic operations, followed by an internal review that finds the institutional and technical foundations to respond independently were not built in time, followed by years of catch-up work that costs more than building sovereignty would have cost in the first place. The pattern is now well-documented enough to be predictable.

The window for deliberate, lower-cost sovereignty work, across all five layers and the institutional foundation beneath them, is approximately five to seven years from the present moment. This is not a precise forecast. It is the period during which the forces named above are likely to consolidate further but have not yet closed the practical options available to a small nation acting with intent. Within this window, sovereignty at each layer can still be claimed at reasonable cost, on the nation's own terms, with the institutional design work done before the technical implementation. Beyond this window, sovereignty becomes a recovery project rather than a design project — possible, but at a multiple of the cost and against constraints that earlier action would have avoided. The question for the

leaders of small advanced nations is not whether the window will close. It is whether they will act while it is still open.

5. Conclusion — A Decision Framework

A framework is only useful if a senior leader can apply it on a single page, in a single sitting, with the resources already in front of him. The framework that follows is offered in that spirit: not as a prescription for what each nation must do, but as a structured way to assess where each nation currently stands, and where the gap between standing and required position is most urgent.

The framework asks six questions. The first five concern the layers; the sixth concerns the foundation beneath them.

Identity & Authentication. Does your nation control the system through which its citizens prove who they are online? Not the front-end interface — the underlying cryptographic infrastructure, the keys, the registry. If the answer requires a clarifying conversation with a foreign vendor, the answer is no.

Payments & Financial Rails. Could your nation continue to move money domestically — between banks, between citizens, between government and private sector — if a single foreign payment processor became unavailable for thirty days? If the answer is uncertain, the rails are not yet sovereign.

Communications Infrastructure. If a sub-sea cable were cut, a satellite constellation were withdrawn from your region, or a foreign telecommunications vendor were sanctioned, would your nation's critical communications continue to function? Sovereignty here is not about ownership; it is about continuity under contested conditions.

Sovereign Cloud. Of the data that governs your nation — citizens' records, health records, taxation, defense, critical sector operations — what portion resides on infrastructure governed by your laws, your courts, your auditors? Partial sovereignty is acceptable here, but the line between what is sovereign and what is not must be explicit, not accidental.

AI Governance. Does your nation have the regulatory and institutional capability to determine what AI systems are permitted within its borders, on what terms, with what redress mechanisms? Without this capability, sovereignty over the other layers can be eroded faster than infrastructure can be built.

Foundation: Talent. Do you have the senior tech leadership — present, attracted, or repatriated — to design and operate the answers to the five questions above? If the answer is no, every other answer is provisional.

A nation that can answer all six questions clearly has a sovereignty position to defend. A nation that hesitates on one or two has gaps to close in the next three years. A nation that hesitates on most has the question itself still ahead of it — and the window in which to address it is shorter than the timeline by which infrastructure can be built.

The framework is not exhaustive. It does not solve the harder political question of how to align stakeholders behind sovereignty investments, or the harder economic question of how to budget for capability that does not generate immediate revenue. Those are local questions for local leaders.

What it does offer is a shared vocabulary. Five layers. One foundation. Six questions. A common language for a conversation that every small advanced nation will have, sooner or later, with itself.

The question is no longer whether the conversation needs to happen. The question is whether it happens before or after the choice has already been made.

Hope is not the conviction that something will turn out well, but the certainty that something makes sense, regardless of how it turns out.

— Václav Havel, Disturbing the Peace (1986)

References

This paper draws on primary sources, government documents, and policy analyses across the five layers of the Digital Sovereign Stack. The selected references below are organised by section and indicate the principal sources for the factual claims made in the paper. They are not intended as an exhaustive bibliography but as a guide to the authoritative documents underlying the analysis.

Section 1 — The Strategic Question

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). *The 2007 Cyberattacks on Estonia: Case Study and Lessons*. Tallinn.

e-Estonia. *e-Estonia: The Story Behind*. Republic of Estonia digital state briefing portal. https://e-estonia.com

Section 2 — The Five Layers

Layer 1: National Identity & Authentication (Estonia)

e-Estonia. *e-Identity*. Republic of Estonia digital state briefing. https://e-estonia.com/solutions/e-identity

Republic of Estonia, Information System Authority (RIA). *State Information System and Cybersecurity Coordination*. https://ria.ee

European Commission. *Digital Public Administration Factsheet: Estonia*. Interoperable Europe Portal, 2024.

Layer 2: Payments & Financial Rails (Singapore)

Monetary Authority of Singapore. *E-Payments in Singapore*. https://www.mas.gov.sg/development/e-payments

World Bank Group. *Case Study: Singapore FAST (Fast and Secure Transfers)*. World Bank Fast Payments Toolkit, 2021.

Monetary Authority of Singapore and Association of Banks in Singapore. *Incorporation of Singapore Payments Network Limited (SPaN)*. Joint Announcement, June 2025.

Bank for International Settlements. *Project Nexus: Multilateral Cross-Border Retail Payments Agreement*. June 2024.

Layer 3: Critical Communications Infrastructure (Switzerland)

United States Department of State. *Investment Climate Statement: Switzerland and Liechtenstein*. 2019; updated 2023.

Swiss Federal Council. *Decision of 9 February 2014: Exclusion of Foreign-Held Companies from Bidding on Critical Infrastructure Projects in Information and Communications Technology*.

Swisscom. *Annual Report and Corporate Sustainability Disclosures*. 2024-2025.

Swiss Federal Office for Cyber Security (BACS). *Cyber Incident Reporting Obligations for Critical Infrastructure Operators*, in force from 1 April 2025.

ICLG. *Telecoms, Media & Internet Laws and Regulations Report: Switzerland*. International Comparative Legal Guides, 2026.

Layer 4: Sovereign Cloud (Ireland)

Microsoft Corporation. *The Microsoft Warrant Case: Background and Documentation*. Microsoft Data Law Blog. https://blogs.microsoft.com/datalaw

United States Congress. *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*. H.R. 4943, enacted 23 March 2018.

Harvard Law Review. *Microsoft Ireland Argument Analysis: Data, Territoriality, and the Best Way Forward*. 2018.

Center for Democracy and Technology. *Microsoft Ireland Case Primer*. 2014; updated 2018.

Microsoft Corporation. *Microsoft Sovereign Cloud and Microsoft Cloud for Sovereignty: European Solutions Announcement*. 2025.

Amazon Web Services. *AWS European Sovereign Cloud Announcement and Operational Updates*. 2023-2025.

Layer 5: AI Governance (Netherlands)

UNESCO Global AI Ethics and Governance Observatory. *Netherlands Country Profile*. 2026.

Government of the Netherlands. *Algorithm Register of the Dutch Government (Algoritmeregister)*. https://algoritmes.overheid.nl/en

Dutch Ministry of the Interior and Kingdom Relations. *Strategic Action Plan for AI (SAPAI)*. Launched October 2019, with rolling annual updates.

Dutch Data Protection Authority (Autoriteit Persoonsgegevens). *Public Reports on Algorithmic Risk*. Published biannually from January 2023.

Government of the Netherlands. *ImplementatieKader for Responsible Algorithm Deployment*. Parliamentary Letter, July 2023.

Section 3 — The Foundation: Sovereign Talent

Sikkut, Siim. *Digital Government Excellence: Lessons from Effective Digital Leaders*. Wiley, 2022.

Republic of Estonia, Government Chief Information Officer Office. *Strategic Coordination of the Digital State*. Ministry of Economic Affairs and Communications.

Government Technology Agency of Singapore. *About Us: Our Role in Digital Government*. https://www.tech.gov.sg

Singapore Ministry of Digital Development and Information. *Newly-Launched GovTech to Transform Public Service Delivery*. October 2016.

Section 4 — The Closing Window

Stanford Institute for Human-Centered Artificial Intelligence (HAI). *The 2026 AI Index Report*. Stanford University, April 2026. https://hai.stanford.edu/ai-index/2026-ai-index-report

Morgan Stanley Research. *AI Market Trends 2026: Global Investment, Risks, and Buildout*. 2026.

Taiwan Semiconductor Manufacturing Company Limited. *Annual Report on Form 20-F for Fiscal Year 2025*. Filed with the United States Securities and Exchange Commission, 2026.

Observer Research Foundation. *The Global Microchip Conflict: The Semiconductor Fault Line Through Taiwan*. ORF Special Report No. 304, April 2026.

World Intellectual Property Organization. *Annual Analysis of AI Investment Trends*. 2026.

About the Author

Nouf Almarri is a Qatari technology leader. She served six years as Chief Information Officer and led the digital transformation of more than ninety government services. Her work at the Civil Service and Government Development Bureau shaped three of Qatar's national platforms: Kawader, Eskan, and Unified Data Platform — ranked first in Qatar in data maturity. She is the founder of Banan Ventures, a venture studio that backs founders building international brands of lasting cultural value. Currently advises a government bureau on technology strategy. She lives and works in Doha.