

Technological Inter-Sovereignty: Preserving Sovereignty in the Age of AI and Quantum

Dr. Smadar Sonogo Itskovich^a, Shachar Farber^a

^a*AI and Quantum Sovereignty Lab*

Abstract

The capabilities underlying essential emerging technologies, such as artificial intelligence and quantum technology, are concentrated among a few states and corporations, whose power to withhold, delay or condition access to a critical capability can turn technological dependence into a de facto veto over national decisions. Since autarky across the entire value chain is unrealistic for most, and in some cases all states, the article addresses how sovereignty can be preserved when dependence cannot be eliminated.

Reviewing how technological, AI and quantum sovereignty are defined across academic research, government policy and industry, the article synthesizes them into a single prism, grounded in a state's ability to act according to its values and interests while controlling essential capabilities without one-sided dependency, with technological sovereignty as the overarching frame and AI and quantum sovereignty as parallel domains within it.

On this basis it establishes a new concept, Technological Inter-Sovereignty: a governance strategy in which trusted states, each indispensable through a critical technological specialty, grant reciprocal access to capabilities while each retains ownership, operation and oversight. A four-condition test, requiring preserved decision-making authority, a critical contribution to the value chain, reciprocal access, and lack of one-sided dependency, distinguishes genuine inter-sovereign arrangements from ordinary cooperation. Quantum Inter-Sovereignty extends this framework to the domain where substitution is least attainable.

Applied through global case studies, this uniform prism and strategy pose a distinctive opportunity for all states, and particularly for small and medium-sized ones, outlining how they can attain sovereignty that would have been unreachable with classical means.

1. Introduction

This chapter contends that the global race is not conducted solely over innovation, market position, or scientific prestige. It is conducted over control of the layers that enable states to defend themselves, grow their economies, operate public systems, and determine how their language, culture and values are represented in the algorithmic era. When these layers are concentrated in the hands of a small number of superpowers and corporations, technological dependency can turn into a strategic constraint, and even into a de facto veto held by an external actor. The challenge this article poses is not how to produce everything within the state, but how to preserve freedom of choice and action under conditions of dependency that cannot be eliminated.

1.1 The Race for the Twenty-First Century's Centers of Technological Power

Artificial intelligence and quantum technologies are no longer research fields separate from state power. Both are dual-use technologies: they can accelerate scientific discovery, productivity and public services, while at the same time transforming capabilities in intelligence, cyber, encryption, command, sensing, and weapons systems development. For this reason, the United States and China do not treat them as ordinary industry sectors. The American plan of 2025 was explicitly titled "Winning the AI Race", while China has incorporated artificial intelligence and quantum information into its long-term national planning, as part of its aspiration to secure an early advantage and reduce dependency on foreign technologies. (The White House, 2025; State Council of the PRC, 2020)

The scale of capital directed at the race illustrates the shift in magnitude. According to Stanford's AI Index (2026), global corporate investment in artificial intelligence more than doubled in 2025, reaching \$581.7 billion. Private investment in the United States stood at \$285.9 billion, compared with \$12.4 billion in China; however, the figure does not fully capture the scale of Chinese support channeled through government guidance funds. Simultaneously, the United States continued to produce more frontier models, while China led in the volume of publications, citations and patents. The race is already institutionalized In quantum as well: more than thirty countries have formulated substantive policy, and by November 2025 eighteen OECD and European Union member states had adopted dedicated quantum strategies, alongside public investment amounting to billions of dollars. (OECD, 2025a; 2025c)

Whoever holds the ability to train and operate large-scale models, manufacture chips, provide cloud infrastructure and data centers, control quantum components and know-how, and

influence standards, keys do not elicit absolute global control, but they do grant the power to determine who gains access, and on which terms, costs, and limitations. From this, follows their direct bearing on security, economic growth and national independence; and, in the field of artificial intelligence, also on the question of which languages, cultural contexts and values find expression in the systems used for education, governance and public life. (Buchser, 2025)

1.2 Concentration in the Critical Layers

Beneath the diversity of applications and products lies a far more concentrated global infrastructure. According to the [Stanford AI Index](#) (2026), a single company in Taiwan manufactures nearly all of the world's leading AI chips. The [OECD estimates](#) that the three largest cloud providers together hold more than sixty percent of the global cloud infrastructure market, and that they are also vertically integrated into model development, investment in AI companies, and the operation of the data centers on which their competitors depend. The production of advanced models likewise remains concentrated mainly in the United States and China (OECD, 2025b).

In quantum technology, concentration stems from a physical, material facet no less than from financial. Quantum systems depend on specialized equipment, manufacturing processes, materials and components, software, testing facilities, and scarce talent in science or engineering. Many of these components cannot be quickly substituted or purchased on the open market in a crisis. This means that even a state working with several suppliers may in practice depend on the same bottleneck further up the value chain. In this way, commercial concentration becomes an architecture of power: a small number of states and companies hold the ability to accelerate, delay or condition the progress of others. (OECD, 2025a, 2025b)

1.3 From Technological Constraint to a De Facto Veto

External dependency is not necessarily a failure. Trade, joint research and international specialization are preconditions for progress in fields where no state alone holds every layer of knowledge and production (March, C., & Schieferdecker, I. (2023)). The character of that dependency changes, however, once access to an essential capability can be withheld, delayed, impaired, or made conditional on the unilateral decision of a foreign government, supplier, or infrastructure holder. The [export controls imposed by the U.S. Bureau of Industry and Security in 2024](#) on quantum computers, quantum equipment, components, and software illustrate that the movement of critical capabilities across borders can be, and is already, subject to security and policy decisions. (Bureau of Industry and Security, 2024)

Such a veto does not require a public threat. It is enough for a state to know that a competitive disadvantage may be caused ([U.S. Bureau of Industry & Security, 2025](#)). This means a license, an update, a cloud service, system maintenance, access to a model, the supply of a component, or the transfer of specialists could be halted under certain conditions which are ambiguous. That knowledge alone may narrow the space of choice in advance: affecting defense strategy, delaying a public service, constraining regulation, altering procurement policy, or leading to the abandonment of a use suited to local language and values, may amount to a 'Denial of Governance' ([Simon & Haklai, 2025](#)). When an external decision can alter a national decision in this way, the constraint is no longer merely technical; it becomes strategic. The risk is especially acute for small and medium-sized states, which have less capital, fewer alternatives, and less ability to rapidly establish substitute infrastructure.

The cost bears on four dimensions at once. In defense, it bears on intelligence, cyber, encryption and command capabilities (OECD, 2025a; 2025c). In the economy, it determines whether companies, researchers and public systems can access computing power, models and advanced equipment (OECD, 2025b; Buchser, 2025). In policy, it affects the state's ability to enforce its laws and operate essential services even as the interests of a supplier or source state change (OECD, 2025c) And in the cultural dimension, the concentration of data, models and expertise in the hands of a few actors may favor dominant languages and groups and marginalize local languages and contexts. (Buchser, 2025).

The discussion above establishes that technological dependence becomes strategically significant when access to critical capabilities can be conditioned by actors outside the state. This raises a more fundamental question: what, in such circumstances, does technological sovereignty require? Existing uses of the terms "technological sovereignty", "AI sovereignty", and "quantum sovereignty" provide different answers, reflecting different understandings of capability, control, and dependence.

Chapter 2 therefore examines these definitions and their limits before developing a common framework for understanding sovereignty across the three domains, as well as proposing a new terminology for the strategic framework of its implementation.

2. Defining the Terrain: Existing Definitions and Their Limits

This chapter synthesizes insights from academia, government institutions, and industry leaders into a single prism unifying Technological, AI, and Quantum Sovereignty. To operationalize this framework, the chapter proposes a new definition, Technological Inter-Sovereignty, a governance strategy in which states leverage indispensable domestic specializations to secure

reciprocal, enforceable access across interdependent technological ecosystems while preserving what is determined essential for the existence of sovereignty.

2.1 The Definitional Problem

Technological sovereignty, AI sovereignty and quantum sovereignty are each the subject of active definitional work. Within each term, academic, governmental and commercial formulations differ in scope, in the object over which sovereignty is claimed, and in the threshold set for attaining it. This lack of consensus is not only within subjects, but between subjects. Each subject is internally divided as well, a pattern visible in miniature within a single forum. The UK Parliament [debate on technology sovereignty \(2026\)](#) showcases difference of opinions between members that is a microcosmos of differences between and within governments, scholars and industries. The sources surveyed below typically develop one of the three concepts on its own, a few extend to a second, but treat it as ancillary to the concept under primary discussion rather than coordinated analysis, and none treats all three within a single, unified scope, part of the aspects in which the following article adds value to the discussion.

This chapter proceeds in four steps. It first surveys the existing formulations for each term, organized by the type of actor advancing them. It then examines the concepts that describe similar arrangements under other names. On that basis it proposes a definition for each of the three terms: Technological Sovereignty, AI Sovereignty and Quantum Sovereignty, and situates them within a hierarchy. Finally, it identifies a configuration that is entailed by the surveyed definitions but never explicitly named, and proposes a term for it – Technological Inter-Sovereignty.

2.2 Technological Sovereignty

No single definition commands general assent. The most frequently cited academic formulation is that of [Edler, et al. \(2023\)](#), first set out in [2021](#), which defines technological sovereignty as "the ability of a state or a federation of states to provide the technologies it deems critical for its welfare, competitiveness, and ability to act, and to be able to develop these or source them from other economic areas without one-sided structural dependency." Two elements of this wording bear on what follows. The definition turns on **the ability to provide critical technologies**, whether by developing them domestically or sourcing them externally, rather than on domestic ownership of production. And the constraint is not dependency but one-sided structural dependency, which permits reliance on others provided that no single supplier can convert that reliance into leverage.

[March and Schieferdecker \(2023\)](#) derive their definition from the challenges that key technologies pose to political and economic sovereignty, defining technological sovereignty as "the ability of a polity to self-determinedly shape the development and use of key technologies

and technology-based innovations, which impact its political and economic sovereignty." They locate research, education and innovation policy at the center of sovereignty aspirations, and conclude that autarky is detrimental to technological sovereignty rather than conducive to it. Their argument for that conclusion is developed in four parts: technological capability creates comparative advantage; it reduces the information asymmetries that raise the cost of trade, enabling what they term trade "on eye level"; it generates the absorptive capacity required to make use of imported technology; and international trade in turn strengthens technological capability. On this account cooperation and sovereignty are mutually reinforcing rather than opposed.

[Crespi et al. \(2025\)](#) reach a similar position from industrial strategy, proposing *coopetitive technological sovereignty*, "a structural and longitudinal strategy in which states compete for technological leadership while deliberately collaborating, in an informed way, with other countries to generate essential critical technologies through the use of complementary knowledge." They rest this on [Huang and Soete \(2025\)](#), who hold that solving specific scientific and technological problems now requires going beyond the capacities and expertise available to individual companies or states, and that global challenges including the development and governance of artificial intelligence can be addressed more effectively through cooperative effort.

Governmental formulations follow comparable lines. On 3 June 2026 the [European Commission](#) adopted its [Technological Sovereignty Package](#), built around the capacity to develop, control and scale critical technologies, infrastructures and data, and responding to a dependency stated by the Commission and originating in the 2024 Draghi report: the Union relies on non-EU providers for more than eighty percent of its key digital products, services, infrastructure and intellectual property. An earlier Commission formulation described technological sovereignty as the capability to "make its own choices, based on its own values, respecting its own rules." The [European Parliament \(2025\)](#) preserves Europe's freedom of action while recognising the role of "trusted non-EU countries and entities," distinguishing between dependencies that are trusted and dependencies that are not. Germany's [BMFTR \(2026\)](#) incorporates democratic values into the definition itself, treating the ability to understand, apply and produce key technologies as connected to the political order those technologies serve.

Commercial and consulting sources use the term in varied ways, and no single industry position can be extracted from them. [Deloitte \(2026\)](#) states that technology sovereignty rests on "the ability of countries and regional blocs to independently develop, control, regulate, and fund digital technologies such as cloud, quantum computing, AI, semiconductors, and digital communication infrastructure," extending to requirements governing data flows and "where physical facilities are, who owns them, who governs them, who operates them, and who

provides the hardware, software, and services that power them." It observes that the shift toward sovereignty "will likely quicken in 2026," with significant investment expected over the next decade in cloud, semiconductors, data centers, AI models, connectivity and satellite communications, and concludes that in an interconnected world, total sovereignty is unlikely to be achieved by any country or region, but many aim to become at least more sovereign. [McKinsey \(2026\)](#) projects that between thirty and forty percent of global AI spending to 2030 will be shaped by sovereignty considerations.

The core of the concept is not contested: sovereignty is a capacity to act rather than a quantity of domestic production. The disagreement concerns its boundary. The scholarly literature positions the concept against autarky, while much legislative and procurement practice moves toward it.

2.3 Digital Sovereignty and the Scope of This Article

Digital sovereignty is treated in the operational literature as layered control over digital systems. The [World Economic Forum \(2025\)](#) and [ECDPM \(2024\)](#) divide it into physical, code and data layers, and the [Joint Research Centre \(2025\)](#) adds governance and people. Vendor formulations are narrower: [Microsoft \(2026\)](#) builds it from data control, operational control and technological independence, and [Google Workspace \(n.d.\)](#) reduces it to where data resides, who accesses it and which software runs it. A distinct position holds that the concept is misapplied to the digital domain: the [United Nations High-Level Panel on Digital Cooperation \(2019\)](#) argues that no state can achieve full digital independence given the global character of the internet, and proposes *digital interdependence*, managed mutual dependence through shared global governance, in place of sovereignty rather than as a version of it. A comparable position has been expressed at state level, the United States Ambassador at Large for cyberspace testifying that "there is no room for digital sovereignty" and proposing *digital solidarity* instead ([BISI, 2025](#); [Elliott, 2024](#)).

This article does not develop digital sovereignty further, for two reasons drawn from the literature surveyed above. First, [March and Schieferdecker \(2023\)](#) observe that technological sovereignty overlaps with digital sovereignty, data sovereignty and information sovereignty, and state that they "consider technological sovereignty to encompass these concepts." Second, the domains examined here are not exclusively digital. Quantum technologies rest substantially on cryogenics, materials and fabrication, and the constraints identified in Section 2.5 are physical rather than informational. A framework organized around the digital layer would not capture them. This ordering is not uncontested: [Robles-Carrillo \(2023\)](#) holds digital sovereignty to be the broader concept, with technological sovereignty a component within it focused on infrastructure and production chains. The choice made here is therefore a taxonomic one, adopted for its fit with the technologies under examination rather than as a

resolution of that disagreement, and digital sovereignty is treated as an adjacent field outside the scope of this article.

2.4 AI Sovereignty

Two terms circulate in this field and are often used interchangeably. *Sovereign AI* denotes a productive capability, namely a state's capacity to build and operate artificial intelligence using resources under its own control. *AI sovereignty* denotes an authority relation, namely a state's capacity to govern how artificial intelligence is developed, deployed and used within its jurisdiction. The first concerns industrial capacity, the second legal and political control. This section addresses AI sovereignty, and refers to sovereign AI only where a source uses that term specifically.

Diverse perspectives are showcased by hardware suppliers, and NVIDIA supplies the clearest example of how such a formulation moves from an executive's public argument to a stable corporate position. Co-founder Jensen Huang first argued that states should own the infrastructure through which intelligence is produced, on the grounds that models encode the language, culture and accumulated knowledge of the societies whose data trains them ([Bernama, 2024](#)). [NVIDIA \(2026\)](#) later states this as the corporate formulation proper, narrower than Huang's own claim: a nation's capability to produce AI using its own infrastructure, data, workforce and business networks. Both instances, the founder's public argument and the company's subsequent corporate position, address sovereign AI rather than AI sovereignty, a productive capability rather than an authority relation, and neither frames the concept as a question of who governs AI's deployment once built. AI sovereignty would target the essential goal of the sovereignty of the state, based on governance. The distinction bears on Definition 2 in Section 2.6, where AI sovereignty is treated as an authority relation rather than a productive capacity.

Dario Amodei, chief executive of Anthropic, locates sovereignty at the level of a coalition rather than the individual state, beginning from the position that democratic states should remain at the frontier of AI development ([Amodei, 2025](#)). In [Policy on the AI Exponential](#) (2026) he proposes a democratic coalition combining coordinated risk regulation, mutual defense in the technological domain and the rejection of AI-enabled repression, resting "on coordination among sovereign states, with each nation retaining full authority over its own affairs." Sovereignty is thus exercised collectively without any member relinquishing it.

Three contributions qualify both positions. [Cellucci and Singh \(2026\)](#) disaggregate the concept into training-data, model, infrastructure and interaction sovereignty, the last requiring that prompts and outputs remain within sovereign boundaries. [IBM \(2026\)](#) defines AI sovereignty as control over the AI stack across all its layers, comprising IT infrastructure, data, models and operations, while distinguishing such control from ownership: "AI sovereignty isn't owning

the stack. It's staying in control when conditions change." [CNAS \(2026\)](#) finds that most states conceive of sovereignty at the model layer less as exclusive development than as the ability to run, modify and govern a model domestically without depending on a foreign firm.

[Balston \(2026\)](#) offers the most operationally specified definition, as the degree to which a state "can make and sustain independent operational choices about AI systems despite external dependencies," assessed across four control mechanisms: contractual, technical, model possession and operational. He concludes that no state possesses end-to-end AI sovereignty, since the stack is geographically distributed: a single chip may combine Chinese raw materials, a Japanese wafer, Dutch lithography built on German optics and American light-source technology, Taiwanese fabrication, Korean memory, American design and British instruction-set intellectual property. [Kurosaki \(2026\)](#) adds a legal register, defining AI sovereignty as "a state's capacity to develop, deploy, and control AI systems, including the data corpora, compute infrastructure, and model weights that constitute the AI supply chain, free from foreign dependence or manipulation," and noting that the legal positions preserving the leading states' latitude for extraterritorial cyber operations also leave their own AI infrastructure without a clear basis for protection.

2.5 Quantum Sovereignty

Quantum sovereignty is the least institutionally settled of the three terms, and the available definitions originate with industry analysts rather than with governments or the peer-reviewed literature. [Ivezic \(2026a\)](#) describes the term as capturing "the idea that nations must control their own quantum technologies – from ultra-powerful quantum computers to unhackable quantum communications – or risk dependence on others." In a subsequent article in the same series he treats sovereignty as a spectrum rather than a binary condition, distinguishing *hard quantum sovereignty*, meaning full-stack domestic control, from *sovereign optionality*: "staying integrated with global innovation while engineering the ability to pivot, verify, and swap dependencies when geopolitics turns them into liabilities" ([Ivezic, 2026b](#)). He identifies the second as the feasible objective for most states and industries.

The grounds for that assessment are material. Partial quantum capacity does not yield proportionate benefit in the way that a domestically substituted cloud or telecommunications service does, and the supply chain is correspondingly narrow: dilution refrigerators are produced by a small number of firms concentrated in Finland and the United States, and the field depends on doctoral-level specialists who are globally scarce. A second consideration is cryptographic. Quantum computing bears directly on the encryption underlying existing systems, which is why the United States [Executive Order of June 2026 on post-quantum cryptography](#) sets transition deadlines for federal systems and contractors. Quantum sovereignty therefore concerns defense against another state's capability as well as possession of one's own.

These constraints bear on the other domains examined here. Where a capability depends on inputs that no single state can supply, the question becomes not whether to depend on others but on whom, and on what terms. Section 2.2 identified the same problem in technological sovereignty, where the European Parliament distinguishes trusted from untrusted dependence, and Section 2.4 identified it in AI, where states secure the capacity to govern models they did not develop. Quantum presents it in the most acute form, because domestic substitution is largely unavailable. In each case the operative variable is the reliability of the relationships through which capability is obtained, based on trust, a point developed in Section 2.7.

Quantum computing is “the next trailblazing innovation in the computing field”, postulates the [Draghi Report \(2024\)](#). The [European Commission's Quantum Strategy \(2025\)](#) uses this premise in The European Union's Strategy on Quantum, claiming Quantum “represents some of the most transformative developments in technological history,” positioning it alongside semiconductors and AI as their top priority. The institutional description below, as well as this framing, situates quantum sovereignty as a component of technological sovereignty, as proposed in Section 2.6.

Governments have not adopted the term as a defined concept. The Quantum Europe Strategy uses the vocabulary of sovereignty without defining it, committing the Union to “fostering a resilient, sovereign quantum ecosystem” and to integrating “secure, sovereign quantum capabilities” into its space, security and defense strategies. The associated policy program frames the objective as unifying efforts, pooling resources and coordinating investments across Member States, and the Strategy is housed under the Executive Vice-President for Technological Sovereignty ([European Quantum Act, n.d.](#)). The two United States Executive Orders of June 2026 are similarly reticent, addressing leadership, security controls and post-quantum cryptography, and directing agencies to engage international partners, without defining sovereignty in this domain. The term is accordingly in use as a policy objective while remaining undefined in policy instruments.

Several comments on these definitions are in order.

2.6 Proposed Definitions

The differences surveyed above differ in kind. In technological sovereignty the dispute concerns the boundary between capability and autarky; in AI sovereignty it concerns the bearer of sovereignty and the conflation of two distinct terms; in quantum sovereignty the term is used in policy without being defined. The following definitions are proposed on that basis.

Definition 1. *Technological sovereignty is the independent ability of a state, or a group of states, to control all essential components of the technological systems material to its existence and welfare, in a manner enabling it to act in accordance with its values and interests, without one-sided dependency*

Definition 2. *AI sovereignty is the ability of a state or a group of states to control the critical supply chain of artificial intelligence, in a manner enabling it to act in accordance with its values and interests, without one-sided dependency.*

Definition 3. *Quantum sovereignty is the ability of a state or a group of states to secure effective control over, and continuous access to, the essential quantum resources, technologies and capabilities, in a manner enabling it to act in accordance with its values and interests, without one-sided dependency.*

First, the three share a common structure: a capacity, exercised as control, directed toward action in accordance with values and interests, and bounded by the absence of one-sided dependency. The intentional uniformity allows the three domains to be assessed through a single criterion rather than through three separate vocabularies. Additionally, the uniformity serves the argument of Section 2.7: since the three definitions are stated in similar language, the question of whether a single relational strategy can secure all three, rather than requiring a separate solution in each domain, becomes a question the definitions themselves raise.

Second, the qualifier is load bearing. By prohibiting dependency that is one-sided, the definitions follow Edler et al. and are consistent with the findings that autarky is detrimental to technological sovereignty, as showcased in Chapters 2.2, 2.4, and 2.5 by scholars (predominantly March & Schieferdecker), governments and corporations. A state may depend on others and remain sovereign.

Third, sovereignty is located in the state, or group of states, notwithstanding that IBM and Microsoft extend the term to firms and organizations. Corporate control remains analytically central, but as an object of state sovereignty rather than as a bearer of it.

Fourth, the resulting hierarchy places state sovereignty as the overarching objective, technological sovereignty as the framework beneath it, and AI and quantum sovereignty as parallel domains within that framework. The domains do not behave identically. AI admits of incremental realization, since a state may secure the capacity to govern models it did not develop, as CNAS documents. Quantum permits less substitution, for the reasons set out in Section 2.5.

These definitions are consistent with some of the existing formulations surveyed above. They differ in two respects from all: first, each of the existing definitions specifies what a state must be able to do. Second, each of the formulations is developed for a single domain; none takes as its unit of analysis the relationship between states through which that ability is secured when the requisite components are distributed beyond the reach of any one of them. The following section addresses these gaps.

2.7 Technological Inter-Sovereignty

The sections above describe a condition common to the three domains. Technological sovereignty concerns resources that have grown in scale, as the Commission's account of an

eighty percent external dependency and Deloitte's projection of accelerating investment both indicate. AI sovereignty compounds this, since the stack is geographically distributed to a degree that leaves no state with end-to-end control. Quantum sovereignty presents the condition in its most acute form, since the inputs are concentrated among a small number of suppliers and specialists and are not readily substitutable. In each domain the resource requirement is increasing rather than diminishing.

2.7.1 Existing Definitions

Sovereignty exercised through structured interdependence is described across these literatures under different names. The terms fall into **two groups**, distinguished by what each treats as preserved when full independence is unavailable.

The first locates sovereignty in control retained despite dependence. IBM defines AI *selective sovereignty* as “the ability to apply control across data, models, and AI infrastructure in proportion to business risk and strategic value. Not everywhere. Not equally. But where the economic and operational risks justify the investment” ([IBM, 2026](#)). Balston's *controlled dependence* states the same logic operationally, as using frontier systems while the advantages outweigh the exposure to risks, while ensuring that if essential functions degrade, they do so controllably. ([Balston, 2026](#)). [Brookings' \(2026\)](#) *managed interdependence*, an “approach that relies on strategic alliances and partnerships to reduce risks throughout the AI stack,” belongs to the same group. Considering governmental perspective, the A UK minister offered a structurally similar account, defining sovereignty in a technology as “strategic leverage” secured through three pillars: holding a sufficient volume of critical inputs, diversifying their sources, and most relevant to our argument – retaining full national control over at least one critical segment of the stack ([House of Commons, 2026](#)). This last condition anticipates the role that specialization in a single segment plays in Section 2.7's account of Technological Inter-Sovereignty. The [Tony Blair Institute \(2026\)](#) states the underlying principle: “Sovereignty should not mean independence from all others. Rather, it should be viewed as the ability to act strategically, with agency and choice, in a world that is irreversibly interdependent.” Ivezic's *sovereign optionality* completes the group.

The second group situates sovereignty in the merger among sovereigns. The *pooled* and *shared sovereignty* of European law sit here, in an intra-Union register ([Poli, 2023](#)), with [Besson \(2004\)](#) supplying the theoretical basis in her account of *cooperative sovereignty*, in which entities overlap in their claims to sovereignty and powers are allocated to whichever authority is best placed to protect shared values. [Data & Society \(2026\)](#) finds that regional compute-pooling coalitions treat sovereignty as a shared capacity, and [Carnegie \(2026\)](#) proposes a *compute coalition* of allied democracies. In the quantum domain, [Ivezic \(2026c\)](#) observes that allies share technology among trusted partners to reduce individual burdens while adversaries are kept at arm's length, an arrangement documented in AUKUS Pillar 2

through a dedicated ITAR exemption operating among the three states alone ([CSIS, 2025](#); [House of Commons Library, 2026](#)). [García-Herrero and Dutta \(2026\)](#) propose *programmable sovereignty*, "soft governance anchored by a deliberately minimal degree of hard-stack control — above all pooled compute capacity — sufficient to make governance commitments credible and dependence reversible," realized through *coordinated specialization*, and show that governance capacity and production capacity are systematically non-overlapping across states, so that no single actor holds the combination their definition requires.

These two groups supply complementary components more so than competing accounts. The first establishes that sovereignty survives dependence provided that control over the dependent relationship remains with the state. The second establishes the mechanism by which multiple sovereigns secure, jointly, a capability that none holds alone, described in registers running from legal theory through defense procurement and industrial policy. No surveyed term holds both properties at once, stated as a single named strategy, nor applied across all three technological domains. The control-preserving group is stated at the level of an individual state's strategy; the pooling group is stated at the level of a particular arrangement, whether European law, AUKUS, or a proposed compute coalition; neither is offered as a general description of the relationship connecting the two. This is the gap the remainder of this section addresses: not a framework alongside managed interdependence or coordinated specialization. Rather, the strategy of which both are instances, named once and stated at the level of the technological domain as a whole.

The survey above identified two components recurring across these responses, and the arrangements surveyed there combine them independently of domain. Amodei's coalition rests explicitly "on coordination among sovereign states, with each nation retaining full authority over its own affairs" (Amodei, 2026) — the control-preserving component — while its purpose is to combine capability that no single member holds alone, the pooling component. The European Commission's Quantum Europe strategy proceeds by pooling resources and coordinating investment across Member States rather than by any one state closing its own gap, while no Member State cedes its own regulatory authority in the process. AUKUS Pillar 2, discussed further in Section 2.7.2 below, follows the same logic in a defense partnership's controlled technologies. The domains differ in what is being secured — a coalition's frontier models, a Union's quantum ecosystem, a defense partnership's controlled technologies — but not in the structure of the arrangement securing it: authority remains where it was, and access is extended selectively to named counterparties. [Kitamura \(2026\)](#) states the underlying logic directly from India's experience, observing that sovereignty in practice has become less about eliminating dependency than about choosing among competing foreign partners, while cautioning that such a choice should not be equated with democratic accountability.

Section 2.6 showed that technological, AI and quantum sovereignty share a common definitional structure. This section has shown that the arrangements proposed to secure them under conditions of resource concentration share a common structure as well: retained authority, combined with shared or guaranteed access. This article proposes a term for that configuration: Technological Inter-Sovereignty.

Definition 4. *Technological Inter-Sovereignty is a governance strategy in which states, each indispensable through a critical specialty no other entity can replace, retain their Technological Sovereignty with trusted partners that grant reciprocal access to the specialties the others hold.*

Quantum sovereignty is where this argument is most pressing, while suffering from a definitional void, and is therefore stated explicitly below. Section 2.5 established that quantum resources are concentrated among a small number of suppliers and specialists to a degree that leaves domestic substitution largely unavailable, even for states that would otherwise qualify as technologically advanced.

Definition 5. *Quantum Inter-Sovereignty is a governance strategy in which states, each indispensable through a critical quantum specialty no other entity can replace, retain their Quantum Sovereignty with trusted partners that grant reciprocal access to the specialties the others hold.*

Two features distinguish it from the general case. Because domestic substitution is least available in quantum of the three domains examined here, this paper argues that Quantum Inter-Sovereignty is largely the one route by which most states can hold Quantum Sovereignty at all. The second feature follows from where the concentration sits: because it is at the input level rather than the output level, a dilution refrigerator or a doctoral-trained specialist cannot be time-shared or licensed the way compute capacity can, which pushes the binding arrangements Quantum Inter-Sovereignty requires toward long-term guarantees of physical access and personnel exchange rather than the shorter-term contractual access possible in other technologies.

Several comments on these definitions are in order.

First, Technological Inter-Sovereignty is not a fourth type of sovereignty alongside technological, AI and quantum sovereignty. It changes the strategy through which sovereign capability and its preservation is perceived. Definitions 1 to 3 specify what a state must be able to do; Definition 4 specifies one arrangement through which a state may be able to do it when the requisite components lie beyond its own reach, and Definition 5 restates that same arrangement for the domain in which it is least avoidable. The relationship between them is instrumental rather than taxonomic.

Second, it is distinguishable from three adjacent arrangements. It is not an ordinary alliance: an alliance adds an external commitment, typically defensive, without modifying the conditions of access between its members. It is not supranational integration: no participant transfers authority to a common institution, which distinguishes it from the pooled sovereignty of European law described by [Poli \(2023\)](#). And it is not the joint exercise of sovereignty over a shared object, as in the doctrine of condominium: each participant's sovereignty remains separate and entire, and what is organized jointly is access rather than authority.

Third, trust operates is integral to the structure, rather than a diplomatic facet. The European Parliament's distinction between trusted and untrusted external entities, and Ivezic's account of technology shared among an "inner circle of quantum trust", both treat the reliability of the counterparty as bearing on whether a given dependency is compatible with sovereignty. Within this prism, trust is the variable that determines which dependencies can be accepted without loss of sovereign capability. Stated this way, trust risks remaining a normative label. In the arrangements portrayed above it is conveyed through a specific, recurring set of institutional mechanisms rather than through diplomatic sentiment: differentiated access rights, which determine who may draw on a given capability and on what terms; binding agreements that convert a political commitment into an enforceable obligation; regulatory exemptions, of which the AUKUS Pillar 2 export-control carve-out discussed below is the clearest instance; information-sharing arrangements, which allow participants to verify a counterparty's reliability; supply-continuity guarantees, which commit a provider to maintain access under stated conditions rather than at its own discretion; usage rights that specify what a participant may do with a shared capability, distinct from access to it; and exit and backup provisions, which determine what happens to a participant's capability if the arrangement or a given counterparty fails. The reliance is applicable to the extent that these mechanisms are present and enforceable, not necessarily to the degree that the counterparty is politically well-disposed.

2.7.2 An Operational Test for Identifying Technological Inter-Sovereignty

The operational test proposed below is an applied contribution of this article, intended to translate Technological Inter-Sovereignty from a conceptual framework to a practical instrument to assess the existence of Technological Inter-Sovereignty. It relies on the assessments of the components comprising Definition 4, through the synthesis of recurring aspects in the literature surveyed above: (a) the preservation of Technological Sovereignty through decision-making authority and freedom of action, (b) critical technological specialization, (c) reciprocal access to special capabilities, and (d) the reduction of one-sided dependency.

To clearly identify Technological Inter-Sovereignty and distinguish it from an R&D agreement, a procurement transaction, a political alliance or ordinary technological cooperation, we propose four cumulative threshold conditions to assess the architecture of access that the arrangement creates:

1. Preservation of sovereign decision-making authority and freedom of action: The capability in question must be one whose loss, disruption, or the denial of access to it, is liable to cause material harm to security, to the economy, to the functioning of public systems, or to national freedom of action.

2. Critical technological contribution: Each party must contribute a critical specialty of technological value that no other entity can replace, including but not limited to: resource, capability, proficiency, infrastructure, an element or component, knowledge or personnel, the replacement of which would amount to, among other consequences, genuine harm or disruption to the continuity of the capability, to its quality or to its very existence, or substantial and sustained costs.

3. Reciprocal access to capabilities: Each state must obtain agreed-upon access to the use of the other's critical capability, for a predefined purpose in the arrangement. It ought to be clarified that the access is to the capability, not the control over it. Ownership, operation and oversight remain with the original sovereign owner, such that access must not derogate from the sovereignty of either side.

4. Preservation of external non-dependence: The arrangement must reduce one-sided dependency and diminish the ability of an external actor to unilaterally terminate a critical capability, thereby exercising a de facto veto over the national freedom of action

2.7.3 From Excluded to Indispensable: Small and Medium States

Frontier capability in these domains is ordinarily read as a question of resources. Developing and deploying frontier AI demands billions of dollars in compute, data and engineering talent alongside hyperscale data centers and advanced semiconductors, capabilities concentrated in the United States and China to the point that the two together hold more than ninety percent of global AI data-center capacity; replicating frontier-scale capability is, on this account, neither feasible nor necessary for most countries (Tony Blair Institute, 2026). Read as a resource question, the conclusion for every other state is exclusion. Technological Inter-Sovereignty reframes it. What Definition 4 requires of a participant is not scale but an indispensable specialty no other entity can replace, and indispensability is not a function of the size of an economy, a population or a research budget. A state that holds one segment of a critical stack on which others depend meets that requirement on the same terms as a state that holds several.

The consequence is a change of position rather than a change of degree. A state without such a specialty enters these arrangements as a customer, on terms set elsewhere, and its dependence is one-sided in exactly the sense Definitions 1 to 3 exclude. A state holding an indispensable specialty enters as a party whose terms must be negotiated, and it does so without producing the stack entire. This is what makes the strategy consequential for such states: it is the route by which they become central to fields that scale alone would have closed to them, and by which the capability to act in accordance with their own values and interests, which the definitions of sovereignty in this article require, is secured through the relationship rather than surrendered

to it. The specialty has to be built, through a deliberate concentration of national capability in a segment where the state can be irreplaceable rather than merely present. For small and medium-sized states the alternative of full domestic substitution is in any event unavailable, which removes the choice that superpowers still notionally possess; the strategy converts that constraint into the basis of a position.

The pattern is already observable. The Netherlands neither designs frontier chips nor trains frontier models, yet its position in extreme ultraviolet lithography through ASML gives it standing in the global AI stack that states pursuing far larger industrial strategies do not hold (World Economic Forum, 2026). Taiwan's concentration of advanced fabrication has likewise been read as a source of strategic protection rather than of vulnerability alone, an argument assessed at length in the literature under the label 'silicon shield' (Weil, Gottwald, & Taube, 2024). Neither has nearly the resources of large states, yet both are indispensable to capabilities that leading powers cannot presently reproduce.

Balston (2026) frames the position of the United Kingdom as precisely not a choice between dependence on foreign frontier providers and an unattainable wholly domestic stack. García-Herrero and Dutta (2026) reach the same conclusion by a different route, focusing on AI and showing that no country outside the two leading powers (the United States and China) holds both the governance capacity and the production capacity their definition of sovereignty requires; true sovereignty is therefore unavailable to any of them individually, which is why they propose coordinated specialization in response: participants contribute distinct comparative advantages under a shared framework rather than each attempting to replicate the full stack. Three cases illustrate how the strategy operates in practice: in defense technology, in quantum infrastructure, and in the commercial AI stack.

AUKUS Pillar 2's export-control exemption, discussed above, is the clearest instance in defense technology. The European Commission's Quantum Europe strategy, also discussed above, shows the same logic in quantum infrastructure. Brookings Institution (2025) documents a comparable arrangement in the commercial AI stack: a "third AI technology stack" outside the two leading powers, in which no single contributor holds the full stack: Canada and Australia supply raw materials, the United Kingdom chip design, the Netherlands fabrication tools through ASML, Taiwan, South Korea and Japan advanced logic fabrication and high-bandwidth memory, and France and Italy compute infrastructure. Not one of these contributors is a leading power, and each is indispensable to the stack through the specialty it holds. Managed interdependence is a structural feature of the AI stack itself, Brookings Institution (2026) argues, not a workaround limited to smaller participants: even the two leading powers depend on inputs they do not fully control. A country's capacity to set the terms of its dependencies, on this account, matters more than the scale of the dependencies themselves.

These cases should not be read as equalizing power among participants. Asymmetries in contribution persist: Kitamura (2026) cautions that selecting among foreign partners is not itself democratic accountability, and García-Herrero and Dutta (2026) identify an unresolved

incentive for a participant to withhold capacity once its own reserve is secured. Yet, the strategy opens states to a form of sovereign capability, if not without fault, that is otherwise unachievable.

The contribution is one of analytical unit. Existing definitions of technological, AI and quantum sovereignty specify the capabilities a state should hold, and the concepts surveyed in Section 2.7.1 specify strategies for holding them under interdependence.

Naming the relationship makes it available for assessment in its own right: whether a given arrangement preserves sovereign capability can be examined by reference to the strategy of access it establishes, rather than only by reference to the capabilities each participant retains. This chapter therefore advances two claims. The first is Technological Inter-Sovereignty, together with its quantum-domain instance Quantum Inter-Sovereignty, as defined concepts. The second is the treatment of technological, AI and quantum sovereignty within a single framework rather than as separate policy fields, which allows the condition common to all three to be identified, and which indicates that the constraints most visible in quantum are an intensified form of those already present in the other two domains rather than an exception to them. The definition is stated here for the technological domain; the structure it describes is not intrinsically confined to technology, and its wider application beyond this domain is left to future work.

3. Technological Inter-Sovereignty in Action

3.1 What Distinguishes Technological Inter-Sovereignty from an R&D Agreement?

Definition 4 states that Technological Inter-Sovereignty is a governance strategy in which states, each indispensable through a critical specialty no other entity can replace, retain their Technological Sovereignty with trusted partners that grant reciprocal access to the specialties the others hold. Read against the instruments through which states already cooperate on research and development, the strategy can look like a familiar arrangement under a new name; the remainder of this section explains why it is not.

Mutual R&D between states already takes several recognized forms. At the intergovernmental level, cooperation may be organized as a legally binding treaty ("[*Pacta sunt servanda*](#)"; Vienna Convention), or through the looser, non-binding instrument of a Memorandum of Understanding (MOU), or an informal arrangement in good faith; a common variant of the binding form is the framework, which identifies the broad areas of cooperation between two parties and authorizes subordinate, agency-level arrangements for specific technical work (U.S. Department of Energy, n.d.). Beneath this intergovernmental level, exist additional contractual forms: financed R&D, in which one party finances research carried out by another; joint R&D, conducted through a cooperation agreement or a joint venture; and looser technical cooperation in working groups (European Commission, 2023). Whatever its form, the underlying activity these instruments organize is, in the [OECD's own definition \(2015\)](#): for the purpose of increase in knowledge – that of humankind, culture and society, or to devise new applications of available knowledge. According to the OECD's definition, the features must be novel, creative, uncertain, systematic and transferable or reproducible.

Mutual R&D, in each of these forms, is oriented toward the research activity itself: the joint or funded production of scientific and technical knowledge, its exchange between the parties, and the reciprocal benefit, or humanity's benefit, that the collaboration provides.

Applying Definition 4, the decisive difference between an R&D agreement and Technological Inter-Sovereignty becomes clear. It is not the legal instrument the parties employ, but the purpose of the arrangement and the architecture of access it creates. The purpose of Technological Inter-Sovereignty is for a state to become sovereign, maintaining its freedom of action and values, through a critical technological specialty. An R&D agreement, on the other hand, carries no such requirement; its purpose is instead an increase in the depth and breadth of technological knowledge and capability. An R&D agreement may therefore serve as a component within a technological inter-sovereign arrangement, but it is not sufficient in itself. As such, Two states can jointly advance a single technological prospect while both remain dispensable to it, or the technology in question may simply not be critical enough to implicate sovereignty at all – an R&D agreement on marine plastic-waste recycling techniques, for instance, does not promise either party's sovereignty in the sense the definition of

Technological Inter-Sovereignty requires. Table 1 provides a concise comparative analysis through the prism of Definition 4.

Table 1. *Operational Comparison of Technological Inter-Sovereignty and R&D agreements*

Criterion	Standard R&D Agreement	Technological Inter-Sovereignty Strategy
Main Purpose	Increase the depth and breadth of technological knowledge, scientific discovery, or new developments.	Achieve Technological Sovereignty (as described in Definition 1).
Condition 1: Sovereign Authority	Not required. Capability in itself loss does not diminish sovereignty necessarily.	Mandatory. Capability disruption causes material harm to security, economy, or freedom of action.
Condition 2: Critical Technological Contribution	Not required. Inputs, resources, and partner entities are dispensable or replaceable.	Mandatory. Each party contributes an indispensable technological specialty, critical to the overarching capability achievement
Condition 3: Reciprocal access to capabilities	Not required. Focus on shared IP or joint project deliverables.	Mandatory. Reciprocal access to capability use only. Ownership, operation, oversight, and sovereign authority remain fully with the original state.
Condition 4: Non-Dependence	Not required. Does not prevent one-sided foreign leverage or structural reliance.	Mandatory. reduces one-sided structural dependency and foreign veto over national decision-making.

3.2 A Contemporary Case Study: The Genesis Mission

The Genesis Mission, established by [U.S. Executive Order 14363](#), is intended to build an “integrated AI platform” for federal scientific research (The White House, 2025b). The United States extended its first international partnership to Japan on June 4, 2026, in a \$1 billion [program](#) uniting twelve DOE National Laboratories, one DOE Office of Science User Facility, and twelve Japanese research institutions across quantum, fusion energy, biotechnology, advanced materials, particle physics, and autonomous systems (DOE, 2026). The partnership is governed by a “Statement of Intent” (DOE, 2026; [RIKEN, 2026](#)), which places the collaboration among the non-binding, framework-building instruments discussed in Section 3.1.

Its purpose, however, is framed around technological sovereignty rather than the language of typical R&D exchange. RIKEN President Makoto Gonokami describes Japan’s role as putting into practice “a new form of AI sovereignty” (RIKEN, 2026), a claim closer to Definition 1’s independent ability to act in accordance with one’s own values and interests than to ordinary research cooperation. He assigns each partner a unique, irreplaceable specialty: the joint teams draw on “the DOE’s high performance systems and Japan’s Fugaku,” and METI Vice Minister Takehiko Matsuo describes Japan’s role explicitly “as a trusted partner” to the Genesis Mission (DOE, 2026). Access under this framework is strictly bounded: Gonokami frames the arrangement as a forum in which data is shared while being mutually protected (RIKEN, 2026), and the Executive Order requires that partnerships with external, non-Federal

collaborators be “structured to preserve the security of Federal research assets” and subject to “classification, privacy, and export-control requirements” (The White House, 2025b). [A Report](#) frames the broader stakes in similarly relative terms, describing the initiative as designed to help both nations maintain their technological dominance over China (Japan Times, 2026) which reflects the systemic U.S.-China technological rivalry ([Yoshimatsu, 2026](#); [Zhang et al., 2026](#)).

This element of trust is precisely what Definition 4 requires of a trusted partner. combined with each side holding an indispensable specialty the other cannot replace (Japan’s infrastructure in the 'Fugaku' supercomputer, and the United States' national laboratories, data resources, and commercial ecosystem) – the arrangement might track Definition 4, entailing Technological Inter-Sovereignty, so long as each country reciprocally grants access to what they hold. If the conditions – trust, indispensableness, reciprocity, and achieved sovereignty, hold - the Mission partnership may itself amount to an instance of Technological Inter-Sovereignty, rather than merely an example that resembles one.

3.2.1 Applying the Operational Test to the Genesis Mission

Application of the test indicates that the partnership between the United States and Japan exhibits several of the features of Technological Inter-Sovereignty: advanced and complementary capabilities, a partnership defined as trusted, the protected sharing of data, and recognition of the sovereign implications of the arrangement. The publicly available information described does not yet fully establish, however, the existence of reciprocal access rights or irreplaceability of each state's contribution. Table 2 provides an analysis of the Technological Inter-Sovereignty achieved through Genesis Mission.

The Genesis Mission is therefore properly classified at this stage as an emerging case, or a candidate, for Technological Inter-Sovereignty, rather than as a fully institutionalized and established instance of it. This classification reinforces the claim that Inter-Sovereignty is more than a political label – it is a framework that can be examined against clear conditions.

A brief comparison with adjacent arrangements is instructive. Measured against Genesis, AUKUS Pillar 2 may display a higher degree of the trust between the partners, as it is translated also into regulatory exemptions in the field of export control. The same holds for the Brookings Institution analysis described in [Section 2.7.3](#), given the increased criticality of each state to its respective aspect of the technology. Quantum Europe illustrates the pooling of resources and the coordination of investment, however it remains to be examined whether special, critical contributions, and reciprocal access rights protecting each state's freedom of action are also present in it.

Table 2. *Assessment of the Genesis Mission through the threshold conditions*

Threshold condition	Evidence in the public record	Assessment	Outstanding gap
1. Preservation of Sovereign Decision-Making Authority and Freedom of Action	Federal AI platform spanning quantum, fusion energy, advanced materials and autonomous systems; no authority transferred to a joint institution.	Partly met	The capability material to each state's freedom of action is not individually identified.
2. Critical Technological Contribution	United States: national laboratories, high-performance systems, data resources, commercial ecosystem. Japan: Fugaku, twelve research institutions.	Partly met	Contributions are distinct and unique, yet indispensability and the extent of alternative capabilities is unevidenced.
3. Reciprocal Access to Capabilities	Clear trusted partnership. Joint teams drawing on both countries' systems; data shared while mutually protected.	Partly met	Who accesses which infrastructure, for which duration, long and on under what usage rights is unevidenced.
4. External Non-Dependence	Non-binding Statement of Intent; access subject to classification, privacy and export-control requirements.	Partly met	No clear establishment of reduction in one-sided dependency or capability to act unilaterally according to the values and interests of one side.

4. Conclusion

The capabilities underlying critical global technologies are highly concentrated. While this reality affects the technological ecosystem broadly, it is especially acute in artificial intelligence and quantum systems. When an entire value chain is controlled by a few external actors, this concentration turns technological dependence into a strategic constraint. It grants foreign suppliers a de facto veto over a state's national security, economic growth, and public systems. Producing all critical technologies domestically is an unrealistic option for almost all states, leading powers included. Examining AI, quantum, and technological sovereignty under a single conceptual prism provides a clearer view of this overarching strategic reality.

To address these challenges within the overarching prism, the article proposes a new principal strategy: Technological Inter-Sovereignty. Alongside its quantum-domain instance, Quantum Inter-Sovereignty, we further develop this framework by providing a clear, operational four-condition test to assess transnational agreements. Evaluating an arrangement against the requirements of sovereign authority, critical technological contribution, reciprocal access, and the reduction of one-sided dependency allows policymakers to distinguish true inter-sovereign partnerships from other cooperative aspects.

This framework highlights a significant shift in the global power balance. Small and medium-sized states can secure a critical role in the global supply chain, gaining substantial strategic leverage in the process, which was likely out of reach previously. By focusing efforts on mastering a specialty, indispensable niche, a smaller country avoids the impossible task of building an entire supply chain single-handedly to compete with superpowers. A state might choose to dominate a highly specialized aspect of the AI stack, similar to the position the Netherlands holds in advanced semiconductor manufacturing. Securing such a capability concentrates national resources on what truly matters for international competitiveness.

Ultimately, Technological Inter-Sovereignty offers a unique, applicable strategy for the current era. For small and medium-sized states, establishing an indispensable specialty is the most viable route to maintain their freedom of choice. Ensuring an outlook that grasps the challenges under a single prism increases its relevance and reduces structural vulnerability. While this article examines Inter-Sovereignty strictly within the scope of technology, the structural logic of reciprocal indispensability offers a framework that could be relevant to manage sovereignty in other fields as well.

References

- Amodei, D. (2025, January). *On DeepSeek and export controls*.
<https://darioamodei.com/post/on-deepseek-and-export-controls>
- Amodei, D. (2026, June). *Policy on the AI exponential*. <https://darioamodei.com/post/policy-on-the-ai-exponential>
- Balston, G. (2026). *AI sovereignty and national security: Identifying the UK's dimensions of control*. Centre for Emerging Technology and Security, Alan Turing Institute.
<https://cetas.turing.ac.uk/publications/ai-sovereignty-and-national-security-identifying-uks-dimensions-control>
- Bernama. (2024). *NVIDIA CEO Jensen Huang on sovereign AI at World Governments Summit*. <https://www.bernama.com/en/news.php?id=2269823>
- Besson, S. (2004). *Sovereignty in conflict*. Social Science Research Network.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=594942
- Bloomsbury Intelligence and Security Institute. (2025). *Sovereign artificial intelligence*.
<https://bisi.org.uk/reports/sovereign-artificial-intelligence>
- Boston Consulting Group. (2025). *Sovereign clouds are reshaping national data security*.
<https://www.bcg.com/publications/2025/sovereign-clouds-reshaping-national-data-security>
- Brookings Institution. (2025). *Making the case for a third AI technology stack*.
<https://www.brookings.edu/articles/making-the-case-for-a-third-ai-technology-stack>
- Brookings Institution. (2026). *Is AI sovereignty possible?* https://www.brookings.edu/wp-content/uploads/2026/02/20260217_AI_sovereignty_final.pdf
- Buchser, M. (2025). *The guidelines for the governance of digital platforms and generative artificial intelligence: Companion document*. UNESCO.
<https://unesdoc.unesco.org/ark:/48223/pf0000395825>
- Bundesministerium für Forschung, Technologie und Raumfahrt. (2024). *Quantum technologies conceptual framework program*.
<https://www.bmfr.bund.de/SharedDocs/Downloads/DE/2024/2024-12-11-handlungskonzept-quantentechnologie-en.pdf>

- Bundesministerium für Forschung, Technologie und Raumfahrt. (2026). *Technological sovereignty*.
https://www.bmfr.bund.de/EN/Research/EmergingTechnologies/TechnologicalSovereignty/technologicalsovereignty_node.html
- Bureau of Industry and Security. (2024, September 5). Department of Commerce implements controls on quantum computing and other advanced technologies alongside international partners. <https://www.bis.gov/press-release/department-commerce-implements-controls-quantum-computing-other-advanced-technologies-alongside>
- Bureau of Industry and Security. (2025, August 29). Department of Commerce closes export controls loophole for foreign-owned semiconductor fabs in China.
<https://www.bis.gov/press-release/department-commerce-closes-export-controls-loophole-foreign-owned-semiconductor-fabs-china>
- Carnegie Endowment for International Peace. (2026). *The compute coalition: How to build the future of AI in the free world*.
<https://carnegieendowment.org/research/2026/06/the-compute-coalition-how-to-build-the-future-of-ai-in-the-free-world>
- Cellucci, D., & Singh, R. (2026). *Sovereign AI: Dimensions of institutional control*. arXiv.
<https://arxiv.org/pdf/2603.14664>
- Center for a New American Security. (2025). *The rising tide of sovereign AI*.
<https://www.cnas.org/publications/commentary/the-rising-tide-of-sovereign-ai>
- Center for a New American Security. (2026). *Sovereign AI index*.
<https://interactives.cnas.org/reports/sovereign-ai-index/>
- Center for Strategic and International Studies. (2025a). *AUKUS Pillar Two: Advancing the capabilities of the United States, United Kingdom, and Australia*.
<https://www.csis.org/analysis/aukus-pillar-two-advancing-capabilities-united-states-united-kingdom-and-australia>
- Center for Strategic and International Studies. (2025b). *The sovereign cloud, sovereign AI conundrum*. <https://www.csis.org/analysis/sovereign-cloud-sovereign-ai-conundrum-policy-actions-achieve-prosperity-and-security>
- Crespi, F., Cerra, A., & Zezza, F. (2025). Coopetitive technological sovereignty. *Intereconomics*, 60(2). 73-80.
<https://www.intereconomics.eu/contents/year/2025/number/2/article/coopetitive>

[-technological-sovereignty-a-strategy-to-reconcile-international-collaboration-with-knowledge-and-economic-security.html](#)

Data & Society. (2026). *Rethinking AI sovereignty in and from the majority world*.
<https://datasociety.net/points/rethinking-ai-sovereignty-in-and-from-the-majority-world/>

Deloitte. (2026). *A new era of self-reliance: Navigating technology sovereignty*.
<https://www.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2026/tech-sovereignty.html>

Domino Theory. (2024). *Puzzling out sovereignty in AI: NVIDIA vs the hyperscalers*.
<https://dominotheory.com/puzzling-out-sovereignty-in-ai-nvidia-vs-the-hyperscalers/>

Draghi, M. (2024). *The future of European competitiveness: A competitiveness strategy for Europe*. European Commission.
https://commission.europa.eu/topics/competitiveness/draghi-report_en

Edler, J., Blind, K., Kroll, H., & Schubert, T. (2021). *Technology sovereignty* (Discussion Paper No. 70). Fraunhofer ISI.
https://www.isi.fraunhofer.de/content/dam/isi/dokumente/cc/innovation-systems-policy-analysis/2021/discussionpaper_70_2021.pdf

Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. *Research Policy*, 52(6), 104765.
<https://www.sciencedirect.com/science/article/pii/S0048733323000495>

European Centre for Development Policy Management. (2024). *Global approaches to digital sovereignty*. <https://ecdpm.org/application/files/7816/8485/0476/Global-approaches-digital-sovereignty-competing-definitions-contrasting-policy-agendas-and-international-tensions.pdf>

European Commission. (2023). *Guidelines on the application of Article 101 of the Treaty on the Functioning of the European Union to research and development agreements* (2023/C 259/01). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2023_259_R_0001

European Commission Joint Research Centre. (2025). *Open but not powerless: Towards a common understanding of EU digital sovereignty*.

https://publications.jrc.ec.europa.eu/repository/bitstream/JRC144908/JRC144908_01.pdf

European Commission. (2025). *Quantum Europe strategy* (COM(2025) 363 final).

https://www.european-quantum-act.com/European_Quantum_Strategy.html

European Commission. (2026a). *Commission proposes tech sovereignty package*.

https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1187

European Commission. (2026b). *Strengthening Europe's tech sovereignty*. Shaping Europe's

Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty>

European Parliament. (2025). *European technological sovereignty and digital infrastructure*

(A-10-2025-0107). https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html

European Quantum Act. (n.d.). *Updates*. <https://www.european-quantum-act.com/>

García-Herrero, A., & Dutta, S. (2026). *Programmable sovereignty: Coordinated specialization as a response to the N-2 problem in AI*. Portulans Institute.

<https://portulansinstitute.org/programmable-sovereign-coordinated-specialization-as-a-response-to-the-n-2-problem-in-ai/>

Google Workspace. (n.d.). *Digital data sovereignty and how it works*.

<https://workspace.google.com/security/digital-sovereignty/>

House of Commons. (2026, March 10). *Technology sovereignty* [Hansard debate].

<https://hansard.parliament.uk/commons/2026-03-10/debates/A91DF2A1-6231-4A38-AF17-56B742D06E95/TechnologySovereignty>

House of Commons Library. (2026). *AUKUS pillar 2: Advanced capabilities* (CBP-9842).

<https://commonslibrary.parliament.uk/research-briefings/cbp-9842/>

Huang, C., & Soete, L. (2025). Rethinking the role of international cooperation in innovation policy. *Economics of Innovation and New Technology*.

<https://www.tandfonline.com/doi/full/10.1080/10438599.2025.2459764>

Information Security Media Group. (2026). *Post-quantum security spurs national sovereignty thinking*. BankInfoSecurity. <https://www.bankinfosecurity.com/post-quantum-security-spurs-national-sovereignty-thinking-a-32095>

- International Business Machines Corporation. (2026). *AI sovereignty*. IBM Institute for Business Value. <https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ai-sovereignty>
- Ivezic, M. (2026a). *Quantum sovereignty primer: Inside the new tech arms race*. PostQuantum.com. <https://postquantum.com/quantum-computing/quantum-sovereignty-intro/>
- Ivezic, M. (2026b). *Physics at the heart of the new cold war*. PostQuantum.com. <https://postquantum.com/post-quantum/physics-quantum-cold-war/>
- Ivezic, M. (2026c). *Quantum geopolitics: The global race for quantum computing*. PostQuantum.com. <https://postquantum.com/quantum-computing/quantum-geopolitics/>
- Ivezic, M. (2026d). *Quantum sovereignty in practice: When geopolitics becomes architecture*. PostQuantum.com. <https://postquantum.com/quantum-sovereignty/quantum-sovereignty/>
- Japan Times. (2026, June 5). *Japan and U.S. to collaborate on AI-driven scientific technologies*. <https://www.japantimes.co.jp/news/2026/06/05/japan/japan-us-ai-cooperation/>
- Kitamura, M. (2026, July 12). *The AI sovereignty problem, from Brussels to Bengaluru*. Tech Policy Press. <https://www.techpolicy.press/newsletter-july-12-2026/>
- Kurosaki, M. (2026, July 28). *The AI sovereignty paradox*. Lawfare. <https://www.lawfaremedia.org/article/the-ai-sovereignty-paradox>
- Lawfare. (2024). *Sovereign AI in a hybrid world: National strategies and policy responses*. <https://www.lawfaremedia.org/article/sovereign-ai-in-a-hybrid-world--national-strategies-and-policy-responses>
- March, C., & Schieferdecker, I. (2023). Technological sovereignty as ability, not autarky. *International Studies Review*, 25(2), viad012. <https://academic.oup.com/isr/article/25/2/viad012/7151276>
- McKinsey & Company. (2026). *Sovereign AI ecosystems for strategic resilience and impact*. <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/sovereign-ai-building-ecosystems-for-strategic-resilience-and-impact>

- Microsoft. (2026). *Digital sovereignty*. Microsoft Learn. <https://learn.microsoft.com/en-us/azure/azure-sovereign-clouds/digital-sovereignty>
- NVIDIA. (2025). *Italy drives industrial renaissance with NVIDIA AI*. <https://blogs.nvidia.com/blog/italy-sovereign-ai/>
- NVIDIA. (2026). *What is sovereign AI?* <https://blogs.nvidia.com/blog/what-is-sovereign-ai/>
- OECD. (2015). *Frascati Manual 2015: Guidelines for collecting and reporting data on research and experimental development*. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2015/10/frascati-manual-2015_g1g57dcb/9789264239012-en.pdf
- OECD. (2025a). An overview of national strategies and policies for quantum technologies. OECD Digital Economy Papers, No. 379. OECD Publishing. <https://doi.org/10.1787/5e55e7ab-en>
- OECD. (2025b). Competition in artificial intelligence infrastructure. OECD Roundtables on Competition Policy Papers, No. 330. OECD Publishing. <https://doi.org/10.1787/623d1874-en>
- OECD. (2025c). OECD Science, Technology and Innovation Outlook 2025: Driving Change in a Shifting Landscape. OECD Publishing. <https://doi.org/10.1787/5fe57b90-en>
- Poli, S. (2023). Reinforcing Europe's technological sovereignty through the CSDP. *European Papers*, 8(1). https://www.europeanpapers.eu/system/files/pdf_version/EP_EF_2023_I_013_Sara_Poli_00665.pdf
- Quantum Industry Consortium. (2025). *Europe's quantum edge hinges on urgency, collaboration and coordination*. The Quantum Insider. <https://thequantuminsider.com/2025/04/02/quic-report-europes-quantum-edge-hinges-on-urgency-collaboration-and-coordination/>
- RIKEN. (2026, June 5). *Message from President Gonokami regarding the new Japan-US strategic partnership on “AI for Science”*. https://www.riken.jp/en/news_pubs/news/2026/20260605_1/index.html
- Robles-Carrillo, M. (2023). Sovereignty vs. digital sovereignty. *Journal of Digital Technologies and Law*, 1(3), 673–690. <https://www.lawjournal.digital/jour/article/view/236>

- Simon, T., & Haklai, B. (2025). Data Disaster – A new threat for sovereignty. *International Journal of Disaster Risk Reduction*, 125, 105538.
<https://doi.org/10.1016/j.ijdr.2025.105538>
- Stanford Institute for Human-Centered Artificial Intelligence. (2026). *Artificial intelligence index report 2026*. <https://hai.stanford.edu/ai-index/2026-ai-index-report>
- State Council of the People's Republic of China. (2020, October 22). China to include quantum technology in its 14th Five-Year Plan.
https://english.www.gov.cn/news/videos/202010/22/content_WS5f90e700c6d0f7257693e3fe.html
- TechPolicy.Press. (2025). *Rethinking sovereign AI as strategy*.
<https://www.techpolicy.press/rethinking-sovereign-ai-as-strategy/>
- The White House. (2025a, July 23). *White House unveils America's AI Action Plan*.
<https://www.whitehouse.gov/releases/2025/07/white-house-unveils-americas-ai-action-plan/>
- The White House. (2025b, November 24). *Executive Order 14363: Launching the Genesis Mission*. <https://www.whitehouse.gov/presidential-actions/2025/11/launching-the-genesis-mission/>
- Tony Blair Institute for Global Change. (2026). *Sovereignty in the age of AI: Strategic choices, structural dependencies*. <https://institute.global/insights/tech-and-digitalisation/sovereignty-in-the-age-of-ai-strategic-choices-structural-dependencies>
- United Nations High-Level Panel on Digital Cooperation. (2019). *The age of digital interdependence*. <https://digitallibrary.un.org/record/3865925?ln=en>
- U.S. Department of Energy. (n.d.). *International commitments primer*.
<https://www.energy.gov/ia/international-commitments-primer>
- U.S. Department of Energy. (2026, June 4). *United States and Japan announce historic \$1 billion partnership under President Trump's Genesis Mission*.
<https://www.energy.gov/articles/united-states-and-japan-announce-historic-1-billion-partnership-under-president-trumps>
- Vienna Convention on the Law of Treaties*, May 23, 1969, 1155 U.N.T.S. 331.
https://legal.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf

Weil, S., Gottwald, J.-C., & Taube, M. (2024). The European Union, Taiwan, and the Silicon Shield argument: A conceptual assessment through the lens of grand theories. *European Politics and Society*, 26(3), 537–563.

<https://doi.org/10.1080/23745118.2024.2417028>

Wilson Sonsini. (2026, July 29). *Back-to-back executive orders shape the U.S. quantum agenda*. <https://www.wsgr.com/en/insights/back-to-back-executive-orders-shape-the-us-quantum-agenda-what-founders-and-investors-need-to-know.html>

World Economic Forum. (2025). *What is digital sovereignty and how are countries approaching it?* <https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/>

World Economic Forum. (2026). The myth of AI sovereignty. <https://www.weforum.org/stories/2026/04/the-myth-of-ai-sovereignty/>

Yoshimatsu, H. (2026). Policy emulation and vested interests: Japan's strategic response to economic security amid US–China technology competition. *Japanese Journal of Political Science*, 27(2), 147–162. <https://doi.org/10.1017/S1468109926100243>

Zhang, M.Y., Wang, S., Wei, Y., & Chen, Z. (2026). When science meets geopolitics: global AI research network transformation (2000–2025). *Science and Public Policy*. <https://doi.org/10.1093/scipol/scag017>