Path Sovereignty: Dependence, Control, and Options in the European Digital Stack

Stéfane Fermigier · Working paper v0.14 · 14 July 2026

Abstract. The production of a digital service runs down a deep vertical chain, from application code through cloud infrastructure to silicon, fabrication, and materials, and out through concentrated distribution channels, so the dependence of any actor on the service accrues along entire paths, while the tests used in policy and procurement (ownership, data location, certification) inspect one node at a time. This paper characterizes the object those tests proxy and builds an instrument that measures it. Following the convergent definitions in the literature, digital sovereignty (strategic autonomy) is an actor's capacity to choose, operate, and re-choose its digital means over time at non-prohibitive cost: a property of option sets, priced by their breadth, their exit costs, and their half-life. European regulation already contains the criteria (the Commission's Cloud Sovereignty Framework defines its top level by "no critical non-EU dependencies"; SecNumCloud §19.6.d requires that service be maintainable from the provider's own competences or at least two third companies), and no published methodology assesses either at ecosystem scale. The instrument has two resolutions. A category-level dependency graph of the full stack (49 nodes from raw materials to app stores, with control, funding, influence, and jurisdiction overlays) yields the structure: exposure composes along paths and is invisible to node-level tests; a domestic alternative exists at a layer only where the substrate is forkable or the moat is domestically owned; the candidate policy levers are partial substitutes whose bundle outperforms even a wholesale re-homing of the US-owned categories; and every combination of the modeled instruments leaves a residual floor of dependence on Asian materials and fabrication. A measured deep dive on three layers (cloud infrastructure, productivity software, AI accelerators), with 38 sourced control-profile cells and 28 options whose key claims passed independent adversarial verification, prices the options: plural at the infrastructure layer, thin and demonstrably exercisable at the productivity layer, and asymmetric at the accelerator layer, where exit is cheap at the inference margin and expensive at the training margin. Structural results are measured; graded results are reported as signs, ordinal strengths, and rankings robust across weight realizations. Policy instruments enter the analysis as objects with three prices attached: a provision is an upper bound on the protection it names, delivery depends on the willingness of the enforcing coalition, and qualification regimes carry fixed compliance costs that fall hardest on small suppliers. The policy reading sorts instruments by layer: conduct rules to cut exit costs, procurement and openness mandates where option sets are non-empty, and state investment at the fabrication and materials floor, where option sets are empty for everyone.

JEL: F52, L86, O25, L40, D85, G34. **Keywords:** digital sovereignty, strategic autonomy, dependency networks, switching costs, option sets, cloud computing, semiconductors, extraterritoriality, public procurement.

---

1. Introduction

A modern digital service is assembled along a deep vertical chain: application code on managed platforms, platforms on cloud infrastructure, infrastructure on silicon, silicon on fabrication, packaging, and materials, with the whole reaching its users through app stores, marketplaces, and payment rails. The distribution channels are owned by a handful of vertically integrated firms (Apple's App Store, Google Play, the hyperscalers' marketplaces), so whether a given link is internal or a dependency depends on who is looking: the integrated incumbent distributes through itself, while producers without a channel of their own cross one that a rival operates and prices. Each link is a market with its own concentration, its own switching costs, and its own legal attachments. The capacity of a firm, an administration, or a bloc to choose, operate, and re-choose the digital means its functioning depends on is therefore a property of entire paths through this chain. The tests actually used to assess that capacity are properties of single nodes: the provider's place of incorporation, its ownership, the location of the data, a security certification. The subject of this paper is the gap between the proxy and the object: what the object is, how to measure it, and what the measurement says about Europe.

The dependence that matters is economic and runs through two kinds of channel along the same paths. The continuous channels operate every day and need no crisis: rents extracted on a locked-in base (Microsoft raised list prices on six suites by 8.6 to 25 percent in 2022; Broadcom's repricing of VMware pushed European private-cloud users toward exits; the US government now collects a 15 percent revenue share on certain Nvidia export licenses); defaults that steer each new firm onto the incumbent stack and foreclose tomorrow's options; an influence asymmetry over the rule-setters; and the market capture of European firms themselves. The channel is measured at market scale: 80 percent of European business spending on cloud software and services goes to US vendors, some 265 billion euros a year [Asterès 2025], and prices on that locked base rose 8.7 percent annually over the last three years, with the inflation alone estimated to drain 93 billion euros a year from the continent [Asterès 2026]. The contingent channels are the tail risks: surveillance over flows through a controlled hub and denial of access to it [Hirschman 1945; Farrell and Newman 2019], instruments that exist in law (the CLOUD Act, FISA §702, the Foreign Direct Product Rule and export controls) and have been exercised, including against allies: the AI Diffusion Framework of January 2025 placed 17 of 27 EU member states under Tier-2 compute caps before being walked back four months later, and in June 2025 Microsoft France's director of public and legal affairs, under oath before a French Senate inquiry, declined to guarantee that French citizens' data would never be transmitted to US authorities without the agreement of French authorities. Neither kind of channel is visible to a test that looks only at who owns the top of a stack, because exposure and rents both compose transitively along the production paths beneath it.

The word "sovereignty" merges two objectives that this dependence structure separates. The first is protection on the legal channel: keeping data and operations outside the practical reach of foreign compulsion. It is a security objective, and Europe has purpose-built instruments for it: ANSSI's SecNumCloud, whose §19.6 conditions qualification on EU incorporation and ownership caps, and the Commission's Cloud Sovereignty Framework (v1.2.1, October 2025), which scores procurement offers on a graded control scale. The second objective is strategic autonomy in the economic sense: the capability, the alternatives, and the value capture that determine who can choose, who collects the rents, and who could switch if choosing became urgent. This paper measures the second objective and treats the instruments of the first as objects of analysis. Three facts about them carry weight throughout. A provision is an upper bound on the protection it names: the CLOUD Act attaches to data in the possession, custody, or control of any provider subject to US jurisdiction, wherever the data sits, and where "control" ends for a venture that runs its licensor's code and depends on its update channel is a question of engineering and litigation that incorporation papers do not settle. Delivery depends on enforcement, which is endogenous: the tests bind only where the Commission, member states, procuring authorities, and private buyers choose to apply them, and the record of that willingness is mixed. And the instruments have costs of their own: qualification is a multi-year fixed cost with regressive incidence on small suppliers, and its change-control regime taxes the feature velocity on which those suppliers compete, a mechanism by which a certification can concentrate the market it was meant to open [Stigler 1971]. Section 6 returns to all three.

The same texts show that the concepts this paper computes are already named in regulation. The Cloud Sovereignty Framework scores offers on eight Sovereignty Objectives with Supply Chain carrying the highest weight (20 percent, against 10 for Legal & Jurisdictional), grades assurance on a ladder defined by *relative control* (“exclusive”, “indirect”, “marginal” control of non-EU third parties), and defines its top level, SEAL-4, as “Full Digital Sovereignty: Technology and operations under complete EU control, subject only to EU law, with no critical non-EU dependencies.” SecNumCloud §19.6.c requires that no non-EU third party on which the provider relies have the technical possibility of obtaining the data, one hop into the supply relation, and §19.6.d defines operational autonomy as the capacity to maintain service from the provider’s own competences or from “at least two third companies”: an option-plurality criterion in regulation. These are path criteria and option criteria; no published methodology assesses either at ecosystem scale, beyond one contract and one hop. Building that assessment is this paper’s job, and the stakes are rising: the Cloud and AI Development Act proposal of 3 June 2026 would move a four-level sovereignty framework into procurement law, which sharpens both the measurement gap and the enforcement and compliance-cost questions that come with writing such tests into statute.

The paper proceeds in two resolutions. Section 2 states the target concept: sovereignty as a property of option sets, extracted from the convergent definitions in the literature, with the measurable triple (option plurality, exit cost, half-life). Section 3 gives the model: a category-level multiplex dependency graph, control read as graded profiles over seven channels, path exposure and its graded (Leontief) extension, and the propositions the construction supports. Section 4 maps the whole ecosystem at category level (49 nodes, silicon to app stores): the structural results are measured counts on a documented sample, and the graded results are pipeline outputs under stylized intensities, reported as signs, strengths, and robust rankings. Section 5 changes resolution and prices three layers with sourced, adversarially verified evidence: cloud infrastructure, productivity software, and AI accelerators. Section 6 sorts the policy instruments by the layers where each has a case, with enforcement and compliance cost as explicit terms. Sections 7 and 8 position the work and state its limits; a companion paper develops the temporal dimension, capture, in which control changes hands through markets.

2. Sovereignty as options

The definitions of digital sovereignty in institutional and practitioner use converge. The Commission’s usage (“Europe’s ability to develop, control and scale its critical technologies”), Merz’s (“the ability to shape technology across the entire value chain in line with European interests and needs”), the JRC’s (“the EU’s capacity to exercise independence in the digital realm while remaining open and connected to global networks”) [Fratini et al. 2026], and NextHop’s, which opposes sovereignty to “situations of imposed dependency: foreign regulatory pressure, proprietary lock-in, geopolitical unavailability of a service” agree on the essentials: sovereignty is a *capacity*, never a state of possession; it is graded; it is actor-relative; it spans the value chain; it must hold over time; and it is defined against dependency imposed through several channels at once. Two guards come with it: independence is instrumental and compatible with openness (autarky is neither necessary nor sufficient), and the capacity is weighted by the criticality of what it protects.

We therefore characterize digital sovereignty (strategic autonomy) as **the capacity of an actor to choose, operate, and re-choose the digital means its functioning depends on, over time and at non-prohibitive cost, across all the layers of the value chain, under the legal, commercial, and supply pressure of other actors.** Equivalently: sovereignty is a property of the actor’s option sets, layer by layer, and it is priced by three quantities. The **breadth** of the option set: how many alternatives exist under independent control (one foreign monopolist and three rival foreign suppliers are different situations, and a domestic option is one term among others, so diversification counts). The **exit cost** E: what re-choosing would cost today, the switching-cost of the industrial-organization literature [Farrell and Klemperer 2007]. And the **half-life**: how fast the option set erodes through lock-in accretion or capture. The characterization matches the regulatory criteria of Section 1: the two-companies clause of §19.6.d is an option-breadth requirement, and the SEAL ladder grades relative control.

Three consequences follow. A wrapper that adds no option adds no autonomy, whatever it contributes on the legal channel. Diversification counts as much as domestication: an actor facing three independently controlled suppliers at reasonable exit cost is freer than one facing a single domestic incumbent, and openness stays part of the concept. And the measure is dated: an option set with a short half-life is a lesser autonomy, which is why the capture dynamic of the companion paper belongs to the definition itself.

3. The model

3.1 The graph

Let G be a directed graph whose nodes are categories of actors rather than individual firms, because the question is structural: whether a category of European buyer, or a layer of the stack, has any domestically controlled path and any options; whether one company is well run is out of scope. The graph is a **multiplex**: several relation-layers on one node set. The load-bearing relation is dependency, a directed edge $u \to v$ meaning that u's production requires v (it is hosted on, licenses its core technology from, or is structurally dependent on v); distribution edges (u reaches its users through v) carry the same semantics at the top of the stack; overlay relations carry funding, influence, and jurisdictional reach.

3.2 Control as graded profiles

Control is relative and multi-channel, and the model represents it that way. Each node carries a **control profile**: ordinal strengths (none, weak, medium, strong) per bloc and per channel, the channels being equity and governance; technology (licenses, interfaces, roadmaps); physical supply; legal reach (with data-access and supply-denial subtypes, and conduct regulation distinguished from extraterritorial jurisdiction); standards and mindshare; distribution; and capital. Single bloc labels, where this paper uses them, are derived summaries of the profiles, and Section 5 shows why the resolution matters: the same node can be EU-strong on equity and US-strong on technology, the profile of a licensed sovereign venture. In the ecosystem map of Section 4, built before the profile upgrade, each category carries one summary bloc; those results are read accordingly.

3.3 Path exposure and the sovereignty gap

Let F_J be the set of nodes controlled by a foreign jurisdiction J on a given channel. A node u is **path-exposed** when some directed dependency path from u reaches F_J: $\mathrm{desc}(u) \cap F_J \neq \emptyset$, multilayer reachability [Kivelä et al. 2014] with control membership propagated up ownership chains following Vitali, Glattfelder and Battiston [2011]. Its **ownership exposure** $e_{\mathrm{own}}(u)$ is the node-level property a registry check sees; the **sovereignty gap** is $g(u) = e_{\mathrm{path}}(u) - e_{\mathrm{own}}(u)$, and $g(u) = 1$ exactly when a domestically owned node is path-exposed. The aggregate $\sum_u g(u)$ measures how much any node-level test understates exposure; Section 4 computes it on a documented sample. Two derived quantities organize the results: the **chokepoint layer** $\lambda(u)$, the shallowest foreign node on u's paths, and the **chokepoint centrality** of a hub, the number of domestic nodes whose paths run through it.

3.4 The graded reading and its discipline

Reachability is the conservative, binary reading. The graded reading equips each dependency edge with an intensity $a_{uv} \in [0, 1]$ (the Leontief input-share) and a substitutability $s_{uv} \in [0, 1]$ (the ease of replacing v: captive at 0, forkable at 1, the cost of exit in the sense of the switching-cost literature [Farrell and Klemperer 2007]); the effective dependence is $a_{uv}(1 - s_{uv})$, and foreign-dependence solves $d = (I - A(I - \mathrm{diag}(f_0)))^{-1} A f_0$, the total direct-and-indirect share summed over all paths with the geometric decay of the Leontief inverse [Acemoglu, Carvalho, Ozdaglar and Tahbaz-Salehi 2012; Baqaee and Farhi 2024]. Cardinal intensities are unavailable for most edges, so each dependency carries an ordinal strength band derived from coded axes, a Monte-Carlo samples the numeric realizations, and we report only what survives, the sign of a quantity, its ordinal strength, and the stability of a ranking. Where this discipline holds, a number like 0.55 is a location on the sampled distribution and never a measurement.

3.5 Propositions

The construction supports five propositions; three are structural, proved as one-line reachability arguments in the companion note, one is an empirical regularity, and one is programmatic. **P1**: ownership is neither necessary nor sufficient for path sovereignty, so the gap g is the object of interest. **P2**, chokepoint relocation: an intervention that re-homes only the top of a stack sets $e_{\mathrm{path}} = 0$ only if it removes every foreign node on every path, and otherwise moves the chokepoint strictly down the stack. **P3**, the floor: if the deepest layer is entirely foreign-controlled and every stack terminates in it, path sovereignty is unattainable without a domestic path at that layer. **P4**, the forkability regularity (empirical, unlike the structural P1-P3): a path-independent domestic alternative exists at a layer only where the substrate is forkable, with its evidence, its four exceptions, and its out-of-sample checks in Section 4.3. **P5** (programmatic, with its evidence in the capture companion): under the capture dynamic, a defensible sovereignty claim must hold across control-layer transitions and not only at a snapshot.

4. The ecosystem at category level

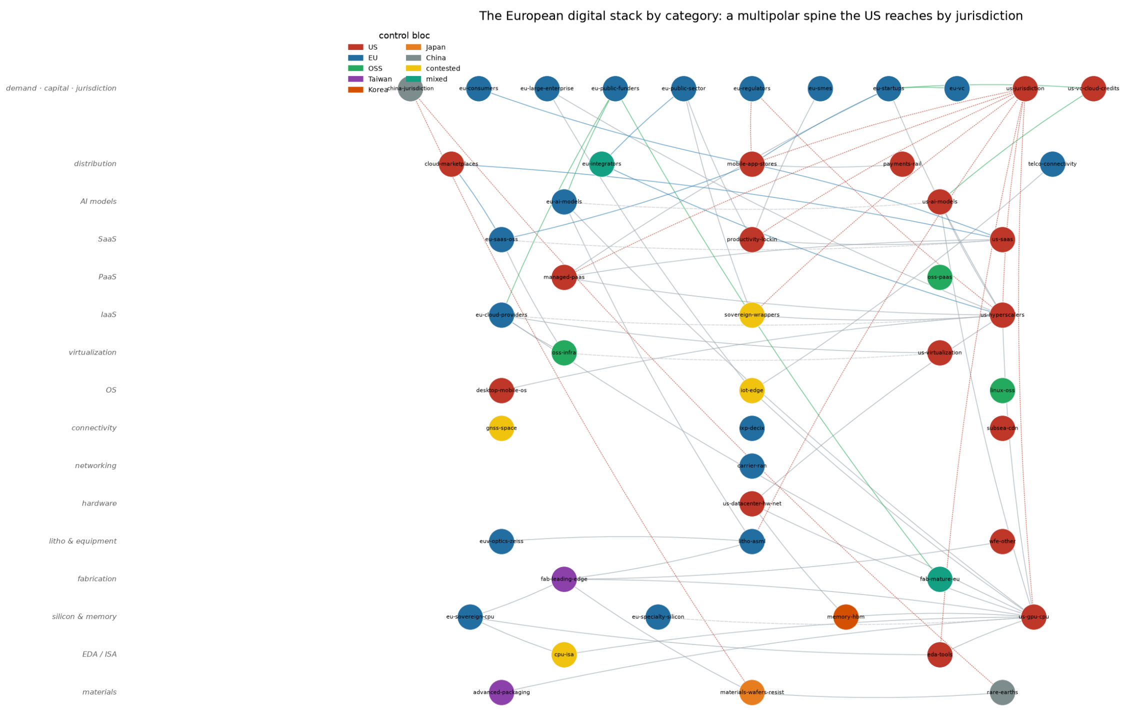
Epistemic status of this section: the node set, the edges, and the control summaries are documented and sourced (a non-exhaustive sample, so exposure counts are lower bounds); the three backbone layers of Section 4.1 are measured per-edge; the graded quantities of Sections 4.5-4.7 run on stylized intensities through the Section 3.4 discipline, so their content is signs, ordinal strengths, and robust rankings. They are the pipeline demonstrated end-to-end, and they become findings only as calibrated intensities replace stylized ones, layer by layer, in the manner of Section 5.

The graph has 50 categories and 71 documented edges across five relation types in the structural map (Figure 1), collapsed by a merge rule (same layer, bloc, substitutability band, criticality band) to a computable core of 49 nodes and 127 edges (96 dependency and distribution, 19 jurisdictional reach, 12 funding and influence); the 2026-07-13 revision split out the client operating systems, browsers, enterprise demand, and IoT/edge that the first, cloud-centered aggregation had buried, carrying seven axes each, with a traceability table so that every one of the roughly 180 finer categories in the underlying taxonomy is subsumed by exactly one compute node. Table 1 is the object itself: the production spine from raw materials to distribution, then the cross-cutting layers, demand, capital, governance and jurisdiction, and the knowledge-and-influence layer that carries the skills pipeline, the integrators and resellers, the analysts and trade press and trade shows that set enterprise defaults, civil society, and the adversary. The column d is the graded foreign-dependence of Section 3.4, the share of a node's own inputs that traces to a foreign-controlled node below it; a node at the floor of its branch reads $d \approx 0$ because little sits beneath it, and its weight instead appears as systemic influence when the whole system leans on it (Table 3). Nodes marked "·" act through the overlay relations, funding, influence, and jurisdictional reach, so the spine metric does not apply to them. The "US reach" mark flags the fourteen categories the US jurisdiction node can compel (Table 2). One row is the sovereignty gap made concrete: the sovereign wrappers are EU-incorporated, so $e_{\mathrm{own}} = 0$, yet carry $d = 0.80$ and a US-reach mark, so $e_{\mathrm{path}} = 1$ and $g = 1$.

Layer	Category	Bloc	Substit.	Crit.	US reach	d
raw materials	Rare-earth & raw-material processing	China	low	critical		0.00
materials	Materials & advanced packaging	Japan	low	critical		0.90
memory	Memory / HBM	Korea	low	critical		0.90
fabrication	Leading-edge fabrication	Taiwan	low	critical		0.82
lithography	EUV lithography & optics	EU	low	critical	●	0.90
EDA / equipment	Design tools & fab equipment	US	low	critical	●	0.90
ISA	Instruction sets	contested	med	high		0.00
silicon	AI accelerator silicon	US	low	critical	●	0.78
silicon	EU specialty silicon	EU	med	medium		0.74
firmware / OS	Firmware, OS, virtualization	US	low	high	●	0.78
commons	Open-source substrate (Linux, K8s)	OSS	high	high		0.00
hardware / net	Networking, hardware, trust anchors	US	med	critical		0.90
networking	EU connectivity (RAN, IXP, RIPE)	EU	high	high		0.65
space	GNSS / space segment (Galileo)	contested	med	high		0.00
datacenter	Datacenter physical (land, power, cooling)	mixed	med	high		0.00
IaaS / PaaS	US hyperscalers	US	low	critical	●	0.68
IaaS	EU cloud	EU	med	medium		0.52
IaaS (sovereign)	**Sovereign wrappers** ($g = 1$)	contested	low	high	●	0.80
IaaS (specialist)	Specialist & neo-clouds (AI compute, quantum)	mixed	med	medium		0.90
identity	Identity / IAM	US	low	critical	●	0.80
dev tooling	Software supply chain	US	med	high	●	0.40
security	Cybersecurity (stack, MSSP, threat intel)	mixed	med	high		0.85
SaaS	US SaaS & productivity lock-in	US	low	high	●	0.69
SaaS	EU SaaS / open-source apps	EU	med	medium		0.46
AI models	US AI models	US	med	high	●	0.70
AI models	EU AI models	EU	med	medium		0.47

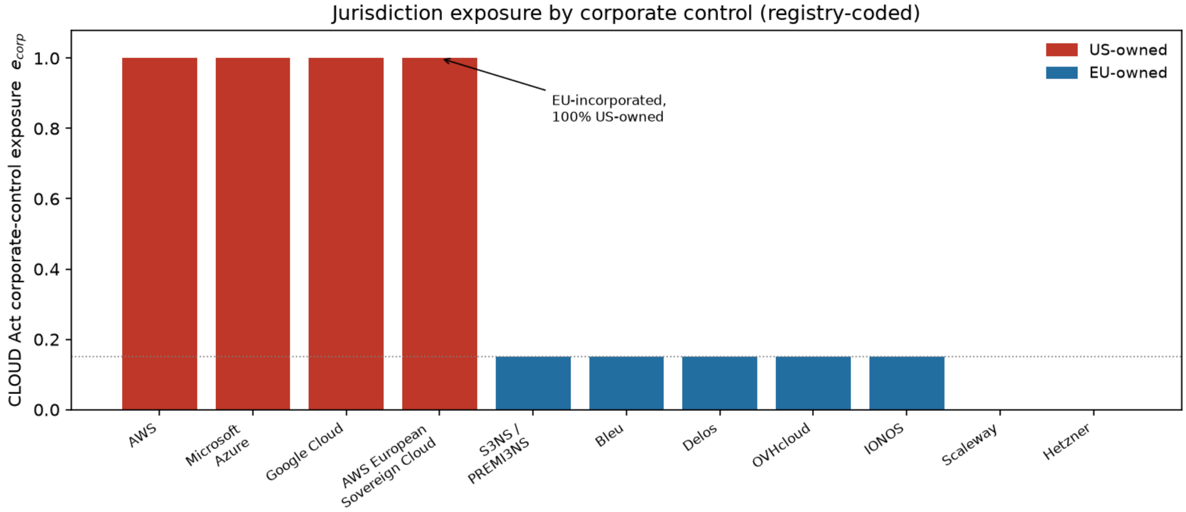
Layer	Category	Bloc	Substit.	Crit.	US reach	d
AI inputs	AI input substrate (data, RLHF, evals)	mixed	med	high		0.00
client OS	Client operating systems (desktop, mobile)	US	low	high	●	0.49
web	Browsers & web platform	contested	high	medium	●	0.35
IoT / edge	IoT, edge & embedded (industrial)	contested	med	high		0.36
distribution	US consumer distribution (app stores)	US	low	high	●	0.70
payments	Payment rails	US	low	high	●	0.00
Demand						
demand	Public sector & education	EU	low	high		0.55
demand	Sovereign-critical (defense, intelligence, justice)	EU	low	critical		0.59
demand	Critical national infrastructure (energy, health, banking)	mixed	med	high		0.56
demand	Enterprises & industry (large firms, SMEs, Mittelstand)	EU	low	high		0.45
demand	Consumers, startups, platform-dependent creators	EU	low	medium		0.57
Capital						
capital	US capital (VC, cloud credits, PE, listing venues)	US	med	high		·
capital	EU capital (VC, public funders)	EU	med	medium		·
Governance & jurisdiction						
jurisdiction	US jurisdiction (CLOUD Act, FISA, FDPR, export controls)	US	low	critical		·
jurisdiction	EU governance (regulators, DGs, CJEU, procurement)	EU	high	high		·

Layer	Category	Bloc	Substit.	Crit.	US reach	*d*
jurisdiction	China jurisdiction (export controls)	China	low	medium		·
standards	Standards bodies (IETF, W3C, ETSI, 3GPP)	global	med	high		·
shock	Transatlantic transfer regime (adequacy)	contested	low	high		·
Knowledge & influence						
talent	Skills pipeline (universities, certification funnels)	mixed	med	medium		·
channel	Integrators, resellers, consultancies	mixed	med	medium		·
influence	Market influence (analysts, trade press, trade shows, lobbies)	mixed	med	medium		·
civil society	Digital-rights and open-knowledge organizations	EU	high	medium		·
adversary	Threat actors (APTs, spyware and exploit markets)	contested	low	high		·



4.1 The measured backbone and the gap

Three of the graph's layers are measured per-edge from primary sources with an adversarial verification step. On the **jurisdiction** layer, coding the CLOUD Act corporate-control test from incorporation and ownership registries for the full 27-provider set, the eleven US incumbents and the US-owned AWS European Sovereign Cloud all reach the maximum exposure, while every EU-owned provider and sovereign wrapper sits at or below the within-caps floor. The measured picture is double-edged (Figure 2): the EU-owned, qualified structures sit at the floor because the ownership-based attachment route is absent by construction, subject to the boundary question of Section 1 over where "control" ends for a licensee, while the AWS European Sovereign Cloud, EU-incorporated and wholly owned by Amazon.com, Inc., scores maximal exposure: the proxy and the object come apart exactly where no qualification constrains the label.



The registry also yields the aggregate gap of Section 3.3, on a documented firm-level sample (twenty-one European-owned or European-controlled providers, wrappers, and public deployments with their recorded hosting, licensing, identity, virtualization, and silicon dependencies; the count moves with every edge added and claims no census). A node-level ownership check passes all twenty-one; nineteen reach a US-controlled node through a directed dependency path, so $\sum_u g(u) \geq 19$ of 21 in the sample, and sixteen of the eighteen strictly EU-owned entities carry $g = 1$. The two unexposed cases reflect dependencies the graph does not yet record, so the count is a lower bound by the monotonicity of exposure under edge addition. The number measures the wedge between what a per-entity check can certify and what the composed paths carry; it is the wedge the SEAL-4 criterion ("no critical non-EU dependencies") would have to assess and currently cannot.

On the **influence** layer, from the EU Transparency Register and the Commission's meeting disclosures, the three cloud-focused US hyperscalers record 465, 288, and 218 high-level Commission meetings (Google, Microsoft, Amazon) against 44 for OVHcloud, the largest EU pure-play, and 14 for the EU cloud-provider association. On the **funding** layer, a single US hyperscaler's announced sovereign-cloud investment (7.8 billion euros) is roughly six and a half times the flagship IPCEI-CIS public envelope (1.2 billion euros). Each edge is sourced and confidence-flagged in `data/edges/`.

4.2 Structure: multipolar control, asymmetric legal reach

Control of the stack layers, read through the summary blocs, is distributed: of the thirty-three stack and distribution categories, twelve carry a US summary bloc and six an EU one, ten are mixed or contested, and the rest are held by Taiwan (leading-edge fabrication), Korea (memory), Japan (materials and packaging), China (rare-earth processing), and an open-source commons. No bloc owns the chain: the US design layers depend on Taiwanese fabrication, which depends on European lithography, which depends on German optics and Japanese materials, which depend on Chinese refining. Control is graded and relative throughout, which is why the interesting summaries are channel summaries. On the legal channel, the asymmetry is reach: the US jurisdiction node can compel fourteen of the forty-nine categories (Table 2), eleven by data-access and three by supply-denial, against three (conduct-type) for the EU and two for China; eleven of the fourteen are US-owned, and the three that are not, European lithography under the Foreign Direct Product Rule, the sovereign wrappers through their licensed stacks, and the contested browser layer through its US vendors, show reach without ownership. Reach is the rarely exercised channel; the continuous channels run on the same paths daily, and Section 4.7 prices the exercise scenarios.

Jurisdiction	Reach	Data-access (CLOUD Act, FISA)	Supply-denial (FDPR, export controls)
US	14	11: hyperscalers, SaaS, firmware/OS, client OS, browsers, identity, software supply chain, consumer distribution, payments, AI models, **sovereign wrappers**	3: AI silicon, design tools & equipment, **EU lithography**
EU	3	3: US hyperscalers, US SaaS, US consumer distribution (conduct reach)	0
China	2	0	2: rare-earth processing, materials & packaging

The EU's own supply-side holds are few and partial: lithography (ASML with Zeiss optics, a chokepoint nested in a chokepoint, and reachable through US export jurisdiction), carrier radio-access equipment, the DE-CIX exchange, the RIPE registry, Galileo; the rest are minority stakes in foreign-led layers or strength in segments that do not substitute for the chokepoints. The exposure of a European buyer composes across all of this: tracing the descendant set of the private-consumer demand node down its recorded edges, a typical European startup meets US control with no domestic escape at eight distinct layers at once, and the walk shows the model's constructs directly:

```
private-consumer-demand  [EU buyer]
├─ us-saas               [US · CLOUD Act]   <- chokepoint layer lambda
│  ├─ us-hyperscalers    [US · CLOUD Act]
│  │  └─ ai-silicon [US·FDPR] -> fab [TW] -> materials [JP] -> raw-mat [CN]
│  ├─ firmware / OS      [US · CLOUD Act]
│  ├─ identity / IAM     [US · CLOUD Act]
│  └─ software-supply    [US · CLOUD Act]
├─ consumer-distribution [US · CLOUD Act]  -> payments [US]
├─ eu-cloud              [EU]  -> ai-silicon [US] -> ... -> raw-mat [CN]
└─ eu-saas-oss           [EU]  -> eu-cloud -> ai-silicon [US] -> ...
```

Every branch reaches a foreign node ($e_{\mathrm{path}} = 1$); re-homing the shallowest layer moves λ down to the hyperscaler and then to silicon (P2, quantified in Section 4.5); and even the European branches terminate at the silicon-and-materials floor (P3).

4.3 Options track the substrate

Whether a domestically controlled alternative exists at a layer is predicted by one observable: the substrate. Across the layers with a proprietary interface, the count of no-escape to escape is eighteen to four; across the forkable layers it is zero to three, and the mixed-substrate layers sit between at one to ten. An open substrate can be forked and self-hosted while a proprietary API cannot [Lerner and Tirole 2002]; in the option language of Section 2, a forkable substrate is a standing option that exists even where no commercial alternative does.

The four exceptions, the proprietary layers that nonetheless admit a European option, refine the regularity. Two are lithography and its optics: layers where a moat exists and Europe owns it. The third is datacenter and networking hardware, where the products are proprietary but the interfaces are commoditized standards, so the moat is shallow. The fourth is virtualization, where the escape route is exactly the adjacent open-source substrate onto which Broadcom's repricing of VMware is currently driving migrations. Not one of the four is a domestic challenger that defeated somebody else's closed moat, so the refined statement is: a domestic option exists at a proprietary layer only where the domestic side owns the moat, where standardization has made the moat shallow, or where a forkable substrate next door supplies the exit.

The cross-section has an out-of-sample check in episodes where forkability was tested by acquisition or denial. When Oracle acquired Sun, and with it MySQL, in 2010, the GPL substrate let the community fork the project as MariaDB, and the fork displaced the original as the default in major Linux distributions: capturing the firm did not capture the commons. When the United States placed Huawei on the entity list in 2019, the two components of its Android dependence answered the same shock differently: the open-source core was carried forward essentially immediately, while replacing the proprietary services layer took a state-scale, multi-year effort. At the instruction-set layer, an open ISA (RISC-V) is what gives a European processor effort a path-independent substrate to build on. The episodes are documented history, and none is a controlled experiment; their evidentiary value is that the substrate coding was not derived from them. (The governance of the commons itself, who maintains and steers the open substrates, is a further channel deliberately out of this paper's scope and reserved for separate work.)

4.4 The reinforcing loop

The dependence is self-reinforcing, and the loop is where the funding and influence data of Section 4.1 do their work. US venture capital and stackable cloud credits land European startups on the US stack by default; the distribution channels then tax the resulting products; and that revenue funds the next layer of the stack, including through compute-for-equity arrangements in which the chip or cloud incumbent takes a stake in a model lab that spends the proceeds back on its patron's capacity (Nvidia's repeated investments in Mistral are the European instance). The defaults grow stickier with each turn: lock-in by increasing returns and path dependence [Arthur 1989; David 1985], operating at the scale of the stack. European capital enters the same loop instead of countering it, which is the firm-level reason that subsidy volume alone does not close the gap, and which connects to the capture dynamic of Section 4.8.

4.5 The graded reading: signs, strengths, rankings

On the stylized-intensity pipeline (Section 3.4 discipline; eight-hundred-draw Monte-Carlo over the ordinal bands), three results are robust. European demand-side foreign-dependence, weighted by buyer criticality, is positive and high, above 0.4 in every draw. The systemic hubs, the categories through which the most dependence flows in the Leontief sense, are the Asian materials layers in every draw, joined most often by the US hyperscalers (98 percent of draws, with accelerator silicon taking the slot in the rest; Table 3): the base of the stack on which even the US layers rest is not US-controlled. And among candidate interventions (Table 4), a forkable-substrate mandate is the strongest lever in every draw, with the full four-lever ordering stable across all draws; per-hub substitutions (Table 5) show chokepoint relocation in numbers, no single substitution reaching zero.

Rank	Systemic hub	Bloc	Influence	In top-3 (800 draws)
1	Materials & advanced packaging	Japan	11.01	100%
2	Rare-earth & raw-material processing	China	10.91	100%
3	AI accelerator silicon	US	6.08	2%
4	Cloud hyperscalers	US	5.93	98%
5	Memory / HBM	Korea	4.92	
6	Leading-edge fabrication	Taiwan	4.53	
7	Networking, hardware, trust	US	3.31	
8	Design tools & equipment	US	3.18	

Intervention (edge edit)	Δ exposure
Forkable-substrate mandate (raise exit on the nine captive US supply hubs)	−0.242
Procurement demand lever (re-route demand off US SaaS, hyperscalers, distribution)	−0.193
Egress ban and portability (raise exit on US cloud, SaaS, firmware)	−0.173
Distribution interoperability (app stores, payments)	−0.013

Domestic substitute for one hub	Bloc	Δ exposure
US SaaS	US	−0.179
US hyperscalers	US	−0.147
Sovereign wrappers	contested	−0.097
IoT & edge	contested	−0.037
US consumer distribution	US	−0.027
US AI silicon	US	−0.022

4.6 Portfolios and the attainable frontier

The levers interact, and the interaction is signed and robust (Table 6): every overlapping pair is a partial substitute in all eight hundred draws, the one disjoint pair is additive, and the size of the interaction tracks the overlap of the targets. The full demand-side bundle (procurement plus forkable substrate plus egress and portability) cuts the criticality-weighted exposure from 0.55 to 0.19 on the base weights, the deepest reduction of any package and a level no single lever approaches, while buying roughly forty percent less than the sum of its parts: the bundle is justified by reach, and it should be defended as a package with diminishing returns.

Portfolio (joint edit)	Joint	Sum of singles	Interaction
Forkable + procurement	−0.319	−0.435	−0.116
Forkable + egress/portability	−0.311	−0.414	−0.104
Egress + procurement	−0.276	−0.366	−0.090
Forkable + distribution	−0.247	−0.255	−0.008
Procurement + distribution	−0.200	−0.206	−0.007
Egress + distribution (disjoint targets)	−0.186	−0.186	0.000
Bundle: procurement + forkable + egress	**−0.352**	**−0.607**	**−0.255**

The attainable frontier closes the graded reading. Re-homing the ownership of every US-controlled category (its foreignness set to zero, the dependency structure untouched) leaves the exposure at

0.28, above the 0.19 the policy bundle reaches without transferring a single share, because the re-homed stack still terminates in Taiwanese fabrication, Korean memory, Japanese materials, and Chinese raw-material processing; the bundle and the re-homing together bottom out at 0.15, the model's immovable floor. An ownership transfer at continental scale buys less than the demand-side package, and the floor is Asian and commercial: a quantitative caution against reading the dependence as a purely American and purely legal problem.

4.7 Exercised chokepoints and the insurance value of options

The exposure measured so far is potential; simulating the exercises prices it. A hub stops supplying the mapped ecosystem, each dependent loses the un-substitutable share of its inputs, and the loss propagates statically (no rebuilding, an instantaneous upper bound). The scenarios span the blocs: Japan restricted semiconductor materials to Korea in 2019, and China has imposed rare-earth and gallium export controls. Three readings are band-robust (Table 7). The worst scenario is the hyperscaler cutoff, in every draw, because it sits shallow where the loss arrives undiscounted; the deep-floor shocks arrive attenuated in a static model that therefore understates them, their real cost being the impossibility of rebuilding fabrication at any relevant horizon. Half of the substantial scenarios are not American. And an ex-ante forkable-substrate mandate cuts the loss in every scenario, from every bloc, in 100 percent of the draws, because even an Asian shock reaches European demand largely through the captive hubs whose dependence the mandate attenuates: options pay in both states of the world, less rent and lock-in while nothing happens, a smaller loss when anything does, so their case does not rest on the probability of any particular legal scenario.

Scenario (denied hub)	Bloc	Loss	Under mandate	Insurance value
US cutoff: hyperscaler services	US	0.27	0.09	0.17
US cutoff: SaaS / productivity	US	0.18	0.07	0.11
Japan materials & packaging denial	Japan	0.14	0.03	0.11
US supply denial: AI accelerators	US	0.13	0.02	0.11
China raw-materials denial	China	0.13	0.03	0.10
Korea memory / HBM denial	Korea	0.10	0.03	0.06
Taiwan fabrication loss	Taiwan	0.07	0.02	0.05
US supply denial: EDA & fab equipment	US	0.04	0.00	0.04

4.8 Sovereignty is also a flow

The graph so far is a snapshot, and control blocs are not fixed: a European category's control can change hands through capture. On a defined universe of 125 prominent European technology firms, a governance lock (foundation, steward-ownership, founder super-voting shares, a golden share, or state control) is associated with staying under European control in 89 percent of resolved cases against 55 without, and none of the governance-locked firms was acquired against its will. Capture makes path sovereignty multi-temporal in the sense of P5, and it is the half-life term of the option triple: today's domestic option can be gone the moment its firm is bought. A companion paper develops the registry, the mechanism, and the policy consequence.

5. Three layers, measured

This section changes resolution and epistemic status: control profiles, option sets, and exit costs for three pilot layers, with 38 sourced cells, 28 options, 22 exit-cost evidence items, and 48 dated events (2022-2026), produced by a research workflow in which each researcher's key claims were independently re-verified against primary sources (29 verdicts, none refuted). Data and per-cell sources: `data/pilot/`.

5.1 Cloud infrastructure

The control profile splits where a single label cannot. On equity and governance, the US is strong: Amazon, Microsoft, and Google hold about 70 percent of the European cloud market, and European providers' combined share fell from 29 percent in 2017 to 15 percent in 2022 and has held roughly steady since (Synergy), the largest EU players (SAP, Deutsche Telekom) at about 2 percent each. On technology, the US is strong even inside the EU-owned sovereign offerings, which run licensed US stacks (S3NS runs Google Cloud code on Thales infrastructure; Bleu runs Azure and 365): roadmap and feature velocity stay with the licensors. On the legal channel, the CLOUD Act covers the US-controlled operators including the Amazon-owned German subsidiaries of the "European Sovereign" offering, and the Senate testimony of Section 1 is the channel's evidence from inside the incumbent. The EU cells are documented but different in kind: weak on equity share, conduct-type on the legal channel (Data Act, GDPR, DMA), and medium on physical supply, since the land, power, permits, and operations staff of the 140+ European hyperscale datacenters sit under host-state jurisdiction.

The option set is the most plural of the three layers, at the commodity level: OVHcloud, Scaleway, Hetzner, IONOS, StackIT, and Exoscale are independently controlled European options, comfortably clearing the two-suppliers criterion of SecNumCloud §19.6.d, and OVHcloud builds and runs its own stack (44 datacenters, more than 500,000 self-built servers). Breadth collapses as the buyer moves up-stack: OVHcloud's entire Public Cloud line is €219.2M of FY2025 revenue against hyperscaler catalogues of hundreds of managed services, so the option set that is plural for virtual machines is nearly empty for managed platforms, which is chokepoint relocation restated in option terms. Exit costs are falling by law: the Data Act (Reg. 2023/2854, applicable 12 September 2025) caps switching charges at direct cost and bans them from 12 January 2027 (Art. 29), and the three hyperscalers eliminated switching-egress fees in 2024 in its shadow, a dated, documented reduction of E for the entire layer. And the demand-side lever has now been exercised at the top: the Commission's own Sovereign Cloud tender (up to €180M over six years, minimum SEAL-2) was awarded on 17 April 2026 across four lots to European consortia (Post Telecom/OVHcloud/Clever Cloud; STACKIT; Scaleway; Proximus/S3NS et al.), most reaching SEAL-3.

5.2 Productivity software

The incumbent's position is measured: up to 77 percent of the EU productivity-software market (Compass Lexecon for the Open Cloud Coalition, 2025), and the Commission's preliminary finding of dominance in the worldwide market for SaaS productivity applications for professional use, in the Teams tying case settled by commitments binding for seven to ten years (September 2025). The lock is technological (formats plus identity coupling) and the rents are documented: the March 2022 list-price increases of 8.6 to 25 percent across six suites. The legal channel shows the two objectives of Section 1 side by side: Microsoft's EU Data Boundary (completed February 2025) localizes storage and processing, and the company's own sworn testimony declined to guarantee immunity from the CLOUD Act; the EDPS meanwhile found (8 March 2024) that the European Commission's own use of M365 infringed Regulation 2018/1725 and ordered the suspension of extra-EEA flows.

The option set is thinner, two to three independent European controllers (Nextcloud GmbH; ZenDiS, the openDesk integrator, 100 percent owned by the Federal Republic of Germany; Open-Xchange), and its exercisability is no longer hypothetical: Schleswig-Holstein reports close to 80 percent of state-administration workplaces (outside the tax administration) on LibreOffice as of December 2025 and completed the migration of almost 44,000 mailboxes from Exchange to Open-Xchange in October 2025 (over 100 million items, about six months). Exit is expensive, slow, and demonstrated finite; the Munich precedent, a migration later reversed, is the standing caution that exits need institutional durability as well as feasibility.

5.3 AI accelerators

The accelerator profile is the most concentrated of the three. On technology, Nvidia's CUDA ecosystem (more than 7.5 million developers per the FY2026 10-K, with an EULA that fences translation layers) sits on top of a shipment position measured at about 98 percent of 2023 data-center GPU units (TechInsights), with 2024-25 revenue-share estimates spanning 80 to 95 percent. On supply, the floor is Taiwanese and Korean: TSMC fabrication, advanced packaging capacity of which Nvidia pre-books on the order of 60 percent, and HBM from three suppliers. On the legal channel the reach has been exercised against allies and then destabilized: the AI Diffusion Framework (90 FR 4544, January 2025) exempted ten EU member states and placed the other seventeen under Tier-2 compute caps; BIS announced rescission on 13 May 2025, two days before the compliance date, and no formal rescission or replacement rule had been published as of January 2026. Two rule reversals in five months, with no European input, is direct evidence on the option-set half-life; the H20 license episode (halted April 2025, resumed August 2025 against a 15 percent revenue share to the US government) adds the rent. On capital, Nvidia's repeated investments in Mistral put the incumbent inside Europe's flagship lab's cap table.

The option set nonetheless contains a second exercisable supplier, inside the same bloc, and its exit price is asymmetric. AMD is exercisable at training scale in Europe: EuroHPC's LUMI runs 2,978 nodes of four MI250X each, and a CSC study benchmarked 140-billion-parameter LLM pretraining on the ROCm stack; on inference, MLPerf v4.1 put eight MI300X within 3.3 percent of eight H100 on Llama2-70B offline. Exit at the inference margin is cheap and getting cheaper; exit at the training margin still pays the full CUDA-ecosystem toll. European design capacity is not an option on this horizon (SiPearl's Rhea1 is an HPC CPU, taped out mid-2025; Graphcore, the leading UK designer, was sold to SoftBank in 2024). The count therefore depends on the margin: the pilot's option table holds seven exercisable suppliers, and every one of them, AMD included, is a US firm under US export law, so breadth in the Section 2 sense (alternatives under independent control) is one. The second supplier disciplines prices; it adds no independent controller.

5.4 What the pilot changes

Three lessons carry back into the model. Control profiles proved necessary: "EU-strong on equity, US-strong on technology" describes a qualified sovereign venture. Option breadth and exit cost are measurable today from public material (price lists, regulations, migration reports, benchmark suites), so the graded layer of Section 4 can be calibrated rather than stylized, layer by layer. And exit costs are use-case-resolved: the training/inference asymmetry shows that E belongs on the edge and the use case; a node-level E is underspecified.

6. Policy: instruments sorted by layer

The results assign each instrument, across the demand-side agenda (procurement preference, open standards, portability: the line associated with the EuroStack Initiative [Caffarra et al. 2025]) and the state-investment agenda [Bria, Timmers and Gernone 2025], the layers where the model gives it a case. The assignments inherit the epistemic status of their sources: where they lean on the graded rankings of Sections 4.5-4.7 they are ordinal, pipeline-status results under the Section 3.4 discipline, and where they lean on Section 5 they are measured; the calibration step that would upgrade the former is the programme's next milestone (Section 8). Two variables run through every assignment: enforcement, which the enforcing coalition chooses and no text can supply, and compliance cost, whose incidence across suppliers the instrument's design fixes.

Conduct rules that cut exit costs act on the whole layer at once, and they economize on enforcement. The three hyperscalers eliminated switching-egress fees in 2024, after the Data Act's switching articles were adopted and before its charge ban binds (January 2027); the Teams commitments and the DMA operate on the same channel. These instruments need no subsidy, and compliance is observable in a public price list, so they consume little of the enforcement willingness that audit-based regimes require. Their natural next targets are the managed-service and identity layers where Section 5.1 shows the option set collapsing.

Demand-side procurement and openness mandates act wherever options exist or can be created, and the machinery now exists. The CSF gives procurement a graded control scale and a pass/fail gate, and the April 2026 award shows European consortia clearing SEAL-3 at Commission scale; whether the gate binds outside Commission procurement remains an enforcement choice, since the framework obliges nobody else. The graded reading (Sections 4.5-4.6) says the strongest single lever is the forkable-substrate mandate, that the demand-side levers are partial substitutes justified as a bundle by the exposure level only the bundle reaches, and the pilot adds the caution that procurement preference works only where Section 5′s option sets are non-empty: at the commodity-infrastructure layer now, at the productivity layer with migration costs that Schleswig-Holstein has now priced, and at the managed-platform layer only after interoperability rules or open substrates create something to buy.

State investment has its case exactly where no actor has options. The frontier result (Section 4.6) shows the demand-side bundle exhausting itself at 0.19 with a floor of 0.15 that only fabrication, packaging, memory, and materials capacity could move, and the systemic-hub ranking (Table 3) puts the deepest leverage in that same base. At the floor, where every buyer faces the same one or two suppliers, procurement cannot re-route and conduct rules cannot cheapen exit; adding an option is the only instrument class left, and it is capital-intensive by nature. That is the layer-sorted case for investment programmes, and it is also their boundary: at layers where options exist or a moat is somebody else's, the same euros buy a capture target (Section 4.8) or feed the loop (Section 4.4).

The legal shield is worth holding at its weight, and it is an upper bound with costs attached. A provision protects at most what its scope covers: a qualified structure closes the corporate-control channel while the custody-and-control boundary of Section 1 stays litigable, and the technology and supply channels are untouched either way. Within scope, delivery depends on enforcement, and the record is mixed: the French government committed in November 2020 to move the Health Data Hub off Microsoft Azure within two years, and the platform was still on Azure when the 2025 Senate inquiry revisited it. And the protection has a price: qualification is a multi-year fixed cost (four years separate the announcement of the S3NS venture, October 2021, from its qualification, December 2025), its change-control regime slows feature release on the qualified perimeter, and both burdens weigh most on the smallest suppliers, the classic mechanism by which regulation ends up serving incumbents [Stigler 1971]. Adequacy diplomacy, custody arrangements, and the bargaining value of Europe's own holds still address the contingent channel, and their value scales with the probability of exercise; the CSF's own weighting, supply chain at twenty percent against ten for legal-and-jurisdictional, is a reasonable prior for how much of the problem this channel is.

7. Related work

The machinery is standard: multilayer reachability [Kivelä et al. 2014], production-network propagation [Acemoglu, Carvalho, Ozdaglar and Tahbaz-Salehi 2012; Baqaee and Farhi 2024], corporate-control propagation [Vitali, Glattfelder and Battiston 2011], the coercion semantics of weaponized interdependence [Farrell and Newman 2019]. The ancestry is older still: dependence as power begins with Hirschman [1945], and the economics beneath the option results is the lock-in and switching-cost literature [Arthur 1989; David 1985; Farrell and Klemperer 2007] with the economics of open source [Lerner and Tirole 2002]. Four neighbors bound the novelty. Beaumier and Cartwright [2024] stack interrelated semiconductor networks under extraterritorial law, the closest prior assembly; we extend to the full stack, add the control and option layers, and compute reachability and cascade. Lehdonvirta, Wú and Hawkins [2025] read power off cloud hub positions at country level on a single relational layer. Baldwin, Freeman and Theodorakopoulos [2023] measure transitive exposure to a marked supplier on input-output data, the closest version of the core reachability move; our marked node carries typed legal reach and a control layer. Clayton, Maggiori and Schreger [2026] give the general-equilibrium theory of coercion over networks; we are its empirical, structural counterpart for one ecosystem. Against all four, the specific contributions are the option-set characterization made computable (Section 2), control as graded multi-channel profiles anchored in the instruments' own language (Sections 3.2, 5), the two-resolution measurement (ecosystem breadth plus priced depth), and the sovereignty gap computed on registry data.

8. Limitations and the measurement programme

The ecosystem map is a documented, non-exhaustive sample: exposure and reach counts are lower bounds, and the firm-level gap count claims no census. Control labels in Section 4 are summary blocs, with a few internally split categories labelled by majority; Section 5 shows the profile treatment those summaries compress. The extraterritorial-reach edges encode doctrine, with enforcement anchoring begun (the Senate testimony, the export-control record) and a specialist legal review still needed. The graded quantities of Sections 4.5-4.7 run on stylized intensities and are reported under the ordinal discipline; the denial exercise is static and understates deep-floor shocks, whose true cost is that fabrication cannot be rebuilt on any relevant horizon. The substrate and alternative codings behind the forkability counts were made by one process, a same-coder risk mitigated by the open analysis of the off-diagonal cells and awaiting an independent blind re-code. The headline qualitative results survive a coarser aggregation of the core (49 to 31 nodes), while the exact hub ordering does not, being a claim about the disaggregated core. The capture universe is a prominence sample, its governance-lock association a correlate with a mechanism, developed in the companion.

The programme continues in the direction Section 5 opened: extend the profile-and-options treatment to the remaining layers (fabrication and distribution next); calibrate the graded layer's measurable edges from the pilot's source classes; register predictions for the Data Act switching-charge ban (January 2027) before the event; and submit the reach edges to legal review. Each step moves results from pipeline status to findings under stated gates.

9. Conclusion

Digital sovereignty, taken at its definitions, is a capacity over options: to choose, operate, and re-choose at bearable cost, across every layer one's functioning depends on, durably. Measured that way, Europe's position is graded and layer-specific. On the legal channel Europe has written instruments whose texts already think in paths and options; what they deliver is bounded by scope, enforcement willingness, and compliance cost, three margins that remain open choices. The economic channels are where the dependence lives: exposure composes along paths that no per-entity test can certify; options exist and are plural exactly where substrates are open or moats are domestically owned; exits are priced, falling by regulation at the infrastructure layer, demonstrated finite at the productivity layer, and asymmetric at the accelerator layer; and beneath everything sits a floor in Asian materials and fabrication, commercial in nature, that no ownership transfer and no procurement mandate can move. The instruments sort accordingly: cut exit costs everywhere, buy options where they exist, build them where nobody has them, and keep the legal shield in proportion. What Europe's frameworks name, from SEAL-4′s "no critical non-EU dependencies" to §19.6.d's two suppliers, this paper makes measurable; the measurement says the objective is reachable layer by layer, and that incorporation labels alone settle none of it.

References

Acemoglu, D., Carvalho, V. M., Ozdaglar, A., & Tahbaz-Salehi, A. (2012). The network origins of aggregate fluctuations. *Econometrica* 80(5), 1977–2016.

ANSSI (2022). *Prestataires de services d'informatique en nuage (SecNumCloud): référentiel d'exigences*, version 3.2, 8 March 2022.

Asterès (2025). *Technological dependence on American software and cloud services: an assessment of the economic consequences in Europe.* Study commissioned by Cigref, May 2025.

Asterès (2026). *From technological dependency to economic capture: the cost of cloud and software services inflation to Europe.* Study commissioned by Cigref, May 2026.

Arthur, W. B. (1989). Competing technologies, increasing returns, and lock-in by historical events. *The Economic Journal* 99(394), 116–131.

Baldwin, R., Freeman, R., & Theodorakopoulos, A. (2023). Hidden exposure: measuring US supply-chain reliance. NBER Working Paper 31820.

Baqaee, D., & Farhi, E. (2024). Networks, barriers, and trade. *Econometrica* 92(2), 505–541.

Beaumier, G., & Cartwright, M. (2024). Cross-network weaponization in the semiconductor supply chain. *International Studies Quarterly* 68(1), sqae003.

Bria, F., Timmers, P., & Gernone, F. (2025). EuroStack: a European alternative for digital sovereignty. SSRN 5298046.

Caffarra, C., et al. (2025). The EuroStack Initiative: Buy European, Sell European, Fund European. eurostack.eu.

Clayton, C., Maggiori, M., & Schreger, J. (2026). A framework for geoeconomics. *Econometrica* 94(1), 105–136.

David, P. A. (1985). Clio and the economics of QWERTY. *American Economic Review* 75(2), 332–337.

European Commission (2025). *Cloud Sovereignty Framework*, version 1.2.1, DG Digital Services, October 2025.

European Union (2023). Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act). *Official Journal*, 22 December 2023.

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: how global economic networks shape state coercion. *International Security* 44(1), 42–79.

Farrell, J., & Klemperer, P. (2007). Coordination and lock-in: competition with switching costs and network effects. In M. Armstrong & R. Porter (eds.), *Handbook of Industrial Organization*, vol. 3, 1967–2072. Elsevier.

Fratini, S., Pohle, J., Di Marco, D., Thabit Gonzalez, S., & Sgueo, G. (2026). *Digital Sovereignty as a Geopolitical Strategy.* JRC policy brief JRC146878.

Hirschman, A. O. (1945). *National Power and the Structure of Foreign Trade.* University of California Press.

Kivelä, M., Arenas, A., Barthelemy, M., Gleeson, J. P., Moreno, Y., & Porter, M. A. (2014). Multilayer networks. *Journal of Complex Networks* 2(3), 203–271.

Lehdonvirta, V., Wú, B., & Hawkins, Z. (2025). Weaponised interdependence in a bipolar world: how economic forces and security interests shape the global reach of US and Chinese cloud data centres. *Review of International Political Economy* 32(5), 1442–1467.

Lerner, J., & Tirole, J. (2002). Some simple economics of open source. *Journal of Industrial Economics* 50(2), 197–234.

Stigler, G. J. (1971). The theory of economic regulation. *Bell Journal of Economics and Management Science* 2(1), 3–21.

Vitali, S., Glattfelder, J. B., & Battiston, S. (2011). The network of global corporate control. *PLoS ONE* 6(10), e25995.

Data and reproducibility. The category graph and the three measured backbone layers, with per-edge sources and confidence flags, are in `data/edges/`; the three-layer deep dive (control-profile cells, option sets, exit-cost evidence, dated events, adversarial verdicts) is in `data/pilot/`; the case-dossier layer is in `data/cases/`; the structural, graded, ordinal-robust, intervention, portfolio, frontier, and denial-shock computations are in `verify/` (`build_category_graph.py`, `compute_core.py`, `robust_ordinal.py`, `operators.py`, `denial_shock.py`, `aggregation_robustness.py`), and the firm-level sovereignty-gap computation is `verify/build_graph.py`; the capture universe is in the companion. Primary-instrument quotations (SecNumCloud 3.2 §19.6; CSF v1.2.1) are documented with page references in `notes/common/receipts-instruments.md`.