

ARTICLE 09

# Sovereignty, Security and Global Network Fragmentation

Resilience, jurisdiction and the cost of a divided network

# Sovereignty, Security and Global Network Fragmentation

*Resilience, jurisdiction and the cost of a divided network*

**AUTHOR** Moderion Advisory

**SERIES** The Total Connectivity Economy

**EVIDENCE CURRENT TO** 6 September 2026

## EXECUTIVE PROPOSITION

Telecom sovereignty extends across equipment, software, cloud, chips, AI models, satellites, data, supply chains and operational authority. Resilience may justify redundancy and jurisdictional control, but unmanaged fragmentation can increase cost and weaken the interoperability on which security and innovation also depend.

## Executive summary

Telecom sovereignty extends across equipment, software, cloud, chips, AI models, satellites, data, supply chains and operational authority. Resilience may justify redundancy and jurisdictional control, but unmanaged fragmentation can increase cost and weaken the interoperability on which security and innovation also depend.

This evidence-led thought article develops an executive point of view using standards, official data, company disclosures and Moderion Advisory analysis. It separates established facts from emerging direction and reported implementation.

## EXECUTIVE QUESTION

How can nations secure operational control and resilience without fragmenting the standards, scale and competition that make modern networks viable?

## Key insights at a glance

- Telecom sovereignty now reaches beyond radio suppliers into software, cloud, semiconductors, AI models, cryptographic control, satellites, subsea routes and specialist operational access.
- The European Commission's January 2026 Digital Networks Act is a legislative proposal, not enacted law as of the evidence date. It links market scale, investment, security, resilience and reduced fragmentation across national markets.
- The Commission's June 2026 technology-sovereignty package defines autonomy around the ability to develop and control key technologies, data and infrastructure while reducing concentrated dependency.
- Localization is not equivalent to sovereignty. A locally hosted service may still rely on foreign updates, accelerators, keys, experts or control planes; a global service may be resilient when dependencies are visible, diversified and operationally governable.
- Common standards improve sovereignty when they enable substitution, verification and coordinated security. Fragmented proprietary or national implementations may reduce supplier choice and slow remediation.

- Resilience has a measurable premium: duplicate routes, dual operations, escrow, stock, domestic capability and tested recovery. Public policy should fund or mandate the premium explicitly when benefits exceed private commercial return.
- Sovereignty is a control property, not a vendor nationality label. It depends on operational authority, identity, data location, encryption keys, update rights, software and silicon dependencies, legal exposure and recovery capability.
- Diversification can reduce concentration risk while increasing integration, testing and incident-coordination risk. A multi-vendor count is not a resilience outcome unless interfaces and fallback paths are exercised.
- The EU's 2026 ICT Supply Chain Security Toolbox broadens the risk lens beyond radio vendors to systemic dependencies across connected products, software and services.
- This article contributes to the Total Connectivity Economy by testing its enabling mechanism against universal reach, open interoperability, governed intelligence, trusted participation and sustainable economics.
- OECD resilience research emphasizes redundancy, diversity, crisis exercises, transparency and cross-operator collaboration. Supplier nationality alone is therefore an incomplete proxy for operational resilience.

### Exhibit 1 | Sovereignty dependency map

| Domain         | Critical dependency                    | Representative control                                   |
|----------------|----------------------------------------|----------------------------------------------------------|
| Network        | Radio, core, optical and orchestration | Multi-vendor interfaces and independent operations       |
| Compute        | Accelerators, cloud and software stack | Portability, capacity reservation and alternative region |
| Trust          | Identity, keys, models and telemetry   | National authority, audit and revocation                 |
| Space / routes | Orbit, gateway and subsea systems      | Diverse paths, landing rights and restoration            |
| People         | Specialist engineering access          | Skills, runbooks and exercised recovery                  |

*Note: Sovereignty must be tested end to end.*

### Exhibit 3 | Sovereignty and supplier-control matrix

| Control domain | Evidence                             | Failure exposure            | Possible response                       |
|----------------|--------------------------------------|-----------------------------|-----------------------------------------|
| Operations     | Privileged-access and command logs   | Remote service control      | Local authority and dual control        |
| Data and keys  | Location, key custody and legal path | Disclosure or lockout       | Customer-controlled keys / segmentation |
| Software       | SBOM, update rights and artifacts    | Unpatched or coerced update | Signed updates, escrow, validation      |
| Supply         | Component and support dependency     | Repair or expansion failure | Inventory, alternatives, redesign       |
| Exit           | Migration test and recovery time     | Permanent lock-in           | Funded, exercised exit plan             |

*Note: Assess by critical capability and service impact; company nationality alone is not a sufficient control test.*

## Core analysis

### Sovereignty is a capability question

National debates often reduce sovereignty to supplier nationality or data location. Those factors can matter, but they are incomplete. A sovereign capability is the practical ability to understand, operate, secure, restore and evolve a critical service under stress. A locally hosted system may still depend on

foreign software updates, chips, models, keys, orbital capacity or specialist support. A globally supplied system may be resilient if dependencies are transparent, diversified and contractually governable.

The correct unit of analysis is therefore the capability and its failure modes. Which components are substitutable? Who can make a high-impact change? Where are credentials and telemetry controlled? How long can the service operate if a supplier, route or jurisdiction becomes unavailable?

### **The fragmentation pressures**

Security restrictions, export controls, sanctions, industrial policy, data rules, cloud regulation and spectrum decisions are reshaping the global system. Operators may need regional architectures, approved supplier sets, sovereign cloud options and duplicated operational capabilities. Satellite services add cross-border coverage and jurisdictional complexity. AI models and accelerators create new concentration risks that traditional telecom regulation was not designed to address.

Some fragmentation is a rational response to systemic risk. The danger is cumulative. Separate standards interpretations, certification regimes, data zones and technology stacks can reduce scale, slow security updates, limit vendor competition and raise the cost of universal service. A policy that improves one dependency may create another.

### **A resilience architecture**

Resilience should be designed through proportional controls. Critical functions need verified inventories, multi-layer observability, privileged-access governance, tested recovery and clear operational authority. Concentrated dependencies may require dual sourcing, escrow, portability, strategic stock, alternative routing or domestic capability. Not every component needs local ownership; controls should reflect consequence, substitutability and recovery time.

Standards remain a strategic asset. Common interfaces and security baselines make substitution and coordinated response possible. Sovereignty and interoperability are not opposites when global standards are combined with national assurance, transparent governance and the right to operate essential functions independently during disruption.

### **The economic trade-off**

Redundancy, localization and diversification cost money. The question is not whether resilience is free, but whether the avoided systemic loss justifies the premium. Governments may need to fund or regulate capabilities whose public value exceeds commercial return. Operators should make these costs visible rather than embedding them silently in balance sheets already under pressure.

Procurement should compare lifecycle security and recovery, not only acquisition price. Policy should also assess innovation and competition effects. A highly restricted ecosystem can create domestic dependence on a smaller supplier base and reduce the scale needed to sustain research.

## **Moderion Advisory perspective**

### **Define sovereignty as an operational capability**

The practical test is whether an authorized national or enterprise team can understand, operate, secure, restore and evolve a critical service during a supplier, route or jurisdictional disruption. This definition makes dependencies testable and avoids treating origin labels as a substitute for engineering evidence.

Controls should be proportional to consequence and substitutability. Low-impact commodity components can rely on normal procurement. Critical, concentrated dependencies may require source or configuration

escrow, independent credentials, tested failover, strategic inventory, alternative routing or a domestic operating capability.

### Price the resilience-fragmentation frontier

Every sovereignty intervention should be assessed for avoided systemic loss, lifecycle cost, effect on competition, security-update speed and innovation scale. The optimal answer may be regional federation: common technical standards and shared markets combined with verified local authority over essential operations and data.

Scenario tests should include not only cyberattack but loss of cloud region, satellite gateway, software update, subsea route, chip supply, trust anchor or specialist access. Dependencies that fail together must not be counted as independent resilience.

### A vendor-diversification scorecard

Each critical capability should be assessed across supply continuity, ownership and control, jurisdiction, remote access, software-update authority, vulnerability response, component provenance, interoperability, exit effort and operational substitutability. Scores should be weighted by service criticality and blast radius. The resulting decision may be exclusion, dual sourcing, escrow, isolated deployment, enhanced monitoring or accepted dependency with a funded exit plan.

Open interfaces can reduce switching cost only when implementations conform, performance is portable and the operator owns integration knowledge. Otherwise, disaggregation can replace one product dependency with multiple integration dependencies. Procurement should therefore include conformance evidence, data and model portability, configuration export, source or artifact escrow where justified, and a timed recovery exercise.

### The sovereign cloud and edge control stack

Data residency answers where data is stored; it does not answer who can administer the service, compel disclosure, change software, control encryption keys or restore operations during geopolitical disruption. A sovereign design separately locates data, metadata, identities, keys, control plane, support access, software supply chain and backup. It also defines which global APIs remain permitted and through which policy gateway.

Compatibility with hyperscale services can be maintained through open workload packaging, documented interfaces, customer-controlled keys, portable observability and tested export. Highly sensitive workloads may require nationally controlled operations; less sensitive services can use global platforms with bounded data and authority. The classification should follow mission impact, not a blanket localization slogan.

### A controlled transition from high-risk infrastructure

The transition begins with an asset and dependency inventory, service criticality map and regulatory deadline. The operator then freezes avoidable expansion, establishes compensating controls, qualifies replacement architectures, builds parallel capacity, migrates bounded domains, verifies service and security, and retains rollback until acceptance. Disposal follows evidence that legal hold, data destruction, license and environmental obligations are complete.

Sequencing should protect emergency services, lawful access, interconnection, roaming and enterprise commitments. A politically announced deadline does not remove engineering constraints; equally, technical complexity should not become an excuse for unmanaged delay. The board requires a funded plan with capacity, workforce, interoperability and incident gates.

## Trusted participation requires resilient openness

Sovereignty should provide operational authority, recovery capability and lawful protection without destroying global interoperability. The North Star is resilient openness: common standards where systems must cooperate, diversification where concentrated failure is material, and sovereign control where essential services, identities, data, keys or decision rights require it.

## Sovereignty claims require legal-status and control-status discipline

The final review distinguishes enacted obligations, legislative proposals, voluntary toolboxes and strategic policy packages. Each can shape investment expectations, but they do not carry the same legal force.

Operational sovereignty should be evidenced through decision rights, key custody, data and model control, update authority, substitution time, tested recovery and jurisdictional exposure. Local hosting or domestic branding alone does not satisfy that test.

## Exhibit 2 | Policy test for a sovereignty control

| Question                | Positive test                         | Risk warning                        |
|-------------------------|---------------------------------------|-------------------------------------|
| <b>Resilience</b>       | Reduces a defined failure mode        | Symbolic origin rule                |
| <b>Proportionality</b>  | Matches consequence and recovery need | Uniform control on all assets       |
| <b>Competition</b>      | Preserves substitutable suppliers     | Creates a new monopoly              |
| <b>Interoperability</b> | Uses common verifiable interfaces     | National technical island           |
| <b>Funding</b>          | Premium and beneficiary are explicit  | Hidden burden on operator cash flow |

*Note: Moderion Advisory policy screen.*

## Executive action agenda

- Map sovereignty dependencies across all five ecosystem layers and their critical interfaces.
- Classify controls by consequence, substitutability, recovery time and jurisdictional exposure.
- Quantify the lifecycle cost and public value of redundancy, localization and diversification.
- Preserve common standards, portability and security coordination wherever national control does not require divergence.
- Test disruption scenarios involving cloud, chips, software updates, subsea routes, satellites and specialist access.

## Conclusion

Sovereignty should be built as operational resilience, not performed as a slogan. The goal is neither unrestricted dependence nor isolation. It is a system that can continue essential service, make risk-visible choices and cooperate through trusted standards without surrendering the authority required to protect national and customer interests. In the wider series, this capability is treated as an enabler of the Total Connectivity Economy rather than as an end state in itself.

## Selected evidence and references

T016 | European Commission. Digital Networks Act proposal. 2026. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/digital-networks-act>

T017 | World Bank. Digital Progress and Trends Report 2025: AI Foundations. 2025. World Bank. <https://www.worldbank.org/en/publication/dptr2025-ai-foundations/report>

T018 | IFC. Telecoms, Media and Technology sector framework. 2025. IFC. <https://www.ifc.org/en/what-we-do/sector-expertise/infrastructure/telecoms-media-and-technology>

T027 | Multiple authors. Non-Terrestrial Networking for 6G: Evolution, Opportunities, and Future Directions. 2025. Engineering. <https://www.sciencedirect.com/science/article/pii/S2095809925002917>

- T028 | Multiple authors. Hands-On Solutions for Testing Integrated Terrestrial and Non-Terrestrial Networks. 2025. IEEE Open Journal of the Communications Society. <https://ieeexplore.ieee.org/document/11304714/>
- T037 | Bronwyn Howell. Beyond infrastructure: Internet ecosystem resilience and the public good. 2025. Telecommunications Policy. <https://www.sciencedirect.com/science/article/pii/S0308596125000953>
- T050 | Luo, Jiang & Ren. A comparative and integrative mapping of thematic trajectories, the digital turn, and future research frontiers in telecommunications policy. 2026. Telecommunications Policy. <https://www.sciencedirect.com/science/article/pii/S0308596126001357>
- P061 | GSMA. Distributed Inference: AI Adds a New Dimension at the Edge. 2025. GSMA Intelligence. <https://www.gsma.com/newsroom/article/distributed-inference-ai-adds-a-new-dimension-at-the-edge/>
- P062 | GSMA. Navigating AI Transformation: A Blueprint for Telcos. 2025. GSMA AI for Impact. <https://www.gsma.com/solutions-and-impact/connectivity-for-good/external-affairs/ai-for-impact/navigating-ai-transformation-a-blueprint-for-telcos/>
- European Commission. The Digital Networks Act. <https://digital-strategy.ec.europa.eu/en/policies/digital-networks-act>
- European Commission. Proposal for a Regulation for the Digital Networks Act. <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-digital-networks-act-dna>
- European Commission. Strengthening Europe's Tech Sovereignty. <https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty>
- ITU-R. IMT-2030 Framework: security, resilience, interoperability and sustainability. <https://www.itu.int/rec/R-REC-M.2160-0-202311-I>
- European Commission. EU ICT Supply Chain Security Toolbox (2026). <https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security>
- European Commission. Implementation of the 5G Cybersecurity Toolbox (2023). <https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox>
- European Commission. EU Cybersecurity Certification Framework. <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework>
- Internet Society. Policy Brief: Open Internet Standards (2025). <https://www.internetsociety.org/resources/policybriefs/2025/policy-brief-open-internet-standards/>
- Internet Society. Critical Properties of the Internet. <https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/>
- PR027 | OECD. Enhancing the resilience of communication networks. OECD Digital Economy Papers No. 374 (2025). <https://doi.org/10.1787/d6920477-en>
- PR028 | European Commission. Proposal for a Regulation for the Digital Networks Act, COM(2026) 16 (2026). <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-digital-networks-act-dna>
- PR029 | NIS Cooperation Group. EU ICT Supply Chain Security Toolbox (2026). <https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security>
- PR030 | European Commission. European Technological Sovereignty Package (2026). [https://commission.europa.eu/news-and-media/news/strengthening-europes-tech-sovereignty-2026-06-03\\_en](https://commission.europa.eu/news-and-media/news/strengthening-europes-tech-sovereignty-2026-06-03_en)