European Technology Risk Assessment

By Glen Birkbeck

2026



Contents

European Technology Risk Assessment: The Framework **1**
How to use this report . . . 1
What regulation means for you . . . 2
Part 1: The Self-Assessment Checklist . . . 3
Part 2: The Risk Domains You Depend On . . . 4
Scenario Context (Q3 2026) . . . 4
2.1 Telecommunications & Connectivity . . . 5
2.2 Energy & Industrial Control Systems (ICS/OT) . . . 5
2.3 Cloud, Data Centres & Digital Infrastructure . . . 6
2.4 Semiconductors & Hardware Supply Chains . . . 7
2.5 Transport and Rail Signalling . . . 9
Part 3: The Internet Core: Routing, Names, Trust . . . 10
3.1 Border Gateway Protocol (BGP) . . . 10
3.2 Domain Name System (DNS) . . . 13
3.3 Certificate & Security Chain (HTTPS/TLS) . . . 14
Conclusion . . . 17
Part 4: AI and Your Firm . . . 17
Pathways to AI Sovereignty . . . 17
Part 5: The Mitigation Framework . . . 19
5.1 Supply Chain Diversification & Onshoring Strategies . . . 19
5.2 Cyber Hygiene & Zero Trust Architecture . . . 20
5.3 Continuity Planning for Critical Infrastructure . . . 20
5.4 Geopolitical Scenario Planning . . . 21
5.5 Vendor Risk Management . . . 22
Cross Cutting Principles . . . 22
Cross Cutting Preparedness Toolkit . . . 23
Appendix A: Cross-Cutting Preparedness Toolkit . . . 23
Browser Sovereignty: Phased Strategy . . . 23
Communications Sovereignty: Contingency for Email and Messaging . 24
Payment System Sovereignty: Contingency Plan . . . 25
AI Offline Note (Part 4) . . . 25
Appendix B: Offline Software Behaviors Guide . . . 25
Microsoft Products Offline Summary . . . 26
Non-Microsoft Desktop/SaaS Summary . . . 26
Satellite Connectivity Limitations (Part 2) . . . 27
AI Offline Note (from Part 4) . . . 27
Appendix C: Glossary of Geopolitical and Technical Terms . . . 27
Appendix D: Map of High Risk Infrastructure Corridors . . . 28
Appendix E: Key Resources . . . 30

European Technology Risk Assessment: The Framework

© 2026, Glen Birkbeck. All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means without the prior written permission of the copyright holder, except in the case of brief quotations embodied in critical reviews and certain other non commercial uses permitted by copyright law.

This work was independently authored by Glen Birkbeck. Artificial intelligence tools were used for research assistance, fact checking, and drafting support, but all analysis, structure, judgment, and final content reflect the author's own expertise and responsibility.

This is Revision 3 of the European Technology Risk Assessment. It is issued in two volumes: this volume, the framework, and the companion volume, *European Technology Risk Assessment: Context*. Revision 3 reorders this volume so the self-assessment checklist comes first, ahead of the analysis, and separates the dated context from the framework.

This publication is for informational purposes only and does not constitute legal, financial, or professional advice.

How to use this report

European Technology Risk Assessment: The Framework Revision 3 · Last updated 30 October 2026

This is the working half of the European Technology Risk Assessment: the risk domains, the framework and the checklists, written to be used rather than read. It changes slowly. When a domain, a control or a checklist item changes, we revise it and note it in the change log.

If you run a small firm, start with the free seven-check guide (fleurlamont.com/guide.html), then the £450 resilience session. This document is for an organisation with a technology risk question it needs answered and written down.

To have it applied to your organisation, with the findings ranked and walked through, that is the £1,500 risk assessment: fleurlamont.com/risk-assessment.html

What regulation means for you

The regulatory and compliance landscape is not repeated in this volume. It is dated, and it moves. It is set out in full in the companion volume, *European Technology Risk Assessment: Context*, in the chapter *Regulatory and Compliance Landscape*. What follows is drawn from that chapter.

Cyber Resilience Act (CRA). Reporting obligations apply from 11 September 2026 and the main body of the Act from 11 December 2027. The CRA imposes **lifecycle security obligations** on manufacturers of hardware and software with "digital elements." Key requirements include:

- Secure by design development practices
- Vulnerability disclosure timelines (≤15 days)
- Software bills of materials (**SBOM**s) for supply chain transparency

Implication: Companies sourcing firmware or embedded systems from non EU vendors (e.g., Chinese IoT device makers) must now verify CRA compliance or risk product recalls and liability for downstream breaches.

NIS2 Directive (Network and Information Security). Effective October 2024, NIS2 significantly expands the scope of regulated entities to include: medium sized energy, transport, health, and manufacturing firms, cloud infrastructure providers, and public administration bodies. It mandates:

- Incident reporting within **24 hours** of detection
- Board level accountability for cybersecurity governance
- Regular stress testing against hybrid threat scenarios

Gap Alert: While NIS2 requires incident reporting, it does **not** mandate physical infrastructure redundancy (e.g., backup power for data centres during grid attacks), a critical omission given Russia's kinetic targeting of energy systems.

GDPR. Data breach reporting (72 hour window) may be impossible if IT teams are displaced or systems destroyed.

Export controls (EU Dual Use Regulation 2021/821). Failure to verify final use can result in:

- Fines up to **10% of global turnover**
- Debarment from public procurement
- Reputational damage under CSDDD

CSDDD. The **Corporate Sustainability Due Diligence Directive (CSDDD)**, with national transposition due by 26 July 2028 and application from 26 July 2029, requires large EU companies to:

- Identify actual or potential adverse human rights and environmental impacts in their **value chains**
- Prevent or mitigate those impacts
- Establish grievance mechanisms

What compliance does not cover. Compliance is necessary but insufficient. True resilience requires **going beyond checklists** to embed geopolitical scenario planning into governance, procurement, and architecture decisions.

Revision 3 · Last updated 30 October 2026

Revisions

- **Revision 3, 30 October 2026.** Issued in two volumes, this one and the companion *Context* volume. The self-assessment checklist now opens this volume, ahead of the analysis. A change log is kept in the revisions list above and in the revisions note published with the report.
- **Revision 3, content update, 30 October 2026.** Part 2 now includes transport and rail signalling as a domain. Added 30 October 2026. The regulatory digest corrections to the Cyber Resilience Act and CSDDD dates are carried from the companion *Context* volume.
- **Revision 2, 26 January 2026.** Structural updates: a dedicated chapter on AI and emerging risks, and a dedicated chapter on internet core.

Part 1: The Self-Assessment Checklist

Use this quarterly checklist to evaluate organizational readiness:

Supply Chain

- Do we know the country of origin for all Tier 1 and Tier 2 hardware components?
- Have we identified at least one alternative supplier for critical semiconductors or cloud services?

Cyber & OT Security

- Are IT and OT networks segmented with unidirectional data flow where possible?
- Do we maintain SBOMs for all custom and commercial software?

Continuity Planning

- Can core business functions operate for 72 hours without internet or cloud access?
- Is emergency power available for critical systems (≥48 hours runtime)?

Geopolitical Awareness

- Has leadership reviewed a "Taiwan blockade" or "Baltic cable cut" scenario in the past 12 months?
- Do procurement contracts include clauses for data portability and service continuity during sanctions?

Internet Core Sovereignty (Part 3)

- Have we audited BGP peering dependencies and implemented RPKI validation?
- Is DNS resolution configured for EU resolvers (e.g., DNS4EU) with aggressive caching for critical domains?
- Do we have plans for TLS/PKI decoupling, including monitoring via CT logs and DANE adoption?

- For payments, have we tested EPI/wero fallbacks and Digital Euro integration?

- Browser/OS trust stores audited for EU Root CA compatibility (e.g., Firefox Sovereignty Build)?
- Comms sovereignty: Tested Matrix/EU-Connect for messaging; dual MX for email (Appendix A)?
- Satellite backups: Planned for low-bandwidth priority (e.g., IRIS²; Part 2)?

Software Licensing (Part 5)
- Audited Microsoft activation types (KMS/MAK grace periods)?
- Tested SaaS offline modes (e.g., 30-day M365 limit)?
- Inventory by license model; perpetual for critical apps?
- Procedures for offline activation (e.g., VAMT, portal jump box)?

Sample Data Residency Audit Checklist (from supplementary material):

1. Identify all sensitive data (financial, health, customer PII) stored on U.S. servers

2. Flag data subject to EU GDPR vs. U.S. CLOUD Act conflicts

3. Quantify downtime risk if U.S. authorities seize data

4. List EU based storage alternatives for high risk data

AI Sovereignty (Part 4)
- Audited AI dependencies (hardware/models/cloud)?
- Tested Mistral/open-source LLMs for sovereignty?
- Enforced EU AI Act transparency for providers?

Part 2: The Risk Domains You Depend On

This part identifies key technology areas vulnerable to geopolitical disruptions, such as telecommunications, energy systems, cloud infrastructure, and semiconductors, with a focus on risks like undersea cable sabotage and supply chain dependencies. It provides executives with an overview of high-impact domains and initial metrics for assessment, before delving into detailed vulnerabilities and mitigation steps. Understanding these domains helps prioritise investments in resilience for European and allied businesses; AI sovereignty is covered in Part 4, and AI and emerging risks in the companion volume, *European Technology Risk Assessment: Context*.

Scenario Context (Q3 2026)

Europe's digital economy faces heightened risk due to the U.S. 6-month NATO exit timeline, tech sanctions on EU critical infrastructure, reciprocal EU restrictions, and rising sabotage risks (undersea cable tampering, DNS hijacking). This part assesses how these geopolitical shocks threaten interconnected technology domains and outlines actionable mitigation strategies.

Europe's digital economy rests on interconnected technological systems that are increasingly exposed to geopolitical shocks. This part examines core critical domains where disruption (whether through sabotage, supply chain failure, regulatory diver-

gence, or cyberattack) could cascade across sectors and borders; AI and emerging tech in Part 4 and in the companion Context volume.

2.1 Telecommunications & Connectivity

Undersea Cable Vulnerability (Baltic/North Sea Routes)

Over 95% of international data traffic between Europe and the rest of the world flows through undersea fibre-optic cables. The Baltic Sea alone hosts more than **30 active subsea cables**, linking Finland, Sweden, Estonia, Latvia, Germany, and Denmark. These routes are now high value targets:

- In 2023 and 2024, unexplained cable cuts near Gotland and the Åland Islands raised NATO concerns about covert Russian naval activity.
- Repair vessels require weeks to deploy, and redundancy is limited, especially for countries like Estonia or Latvia, which rely on just 2 to 3 major cable landings.
- A coordinated attack on multiple cables during winter could isolate the Nordic - Baltic region from global cloud services, financial networks, and emergency communications.

5G/6G Dependencies on Non EU Vendors

Despite EU efforts to diversify, European 5G rollout remains heavily dependent on **Ericsson (Sweden)** and **Nokia (Finland)**, both capable but lacking full stack semiconductor sovereignty. Meanwhile, Huawei and ZTE remain present in legacy infrastructure across Southern and Eastern Europe, creating long term maintenance and security liabilities.

As 6G standardization accelerates (targeting 2030 deployment), Europe risks falling behind in core IP development, especially in AI, native radio access networks and terahertz spectrum management, areas where China and the U.S. are investing billions.

> **Key Risk**: Single point failures in physical connectivity + strategic lag in next generation telecom innovation.

Risk Metrics:

- Non EU cable redundancy share <40% (red flag); target ≥70%
- 5G/6G vendor reliance on non EU providers >60% (red flag); target <30%

Mitigation & Preparedness:

- Activate satellite backup projects (e.g., NATO's HEIST)
- Fund EU led undersea cable projects (Atlantic Link 2)
- Accelerate EU semiconductor and telecom R&D

2.2 Energy & Industrial Control Systems (ICS/OT)

Grid Security Amid Russian Strikes on Ukrainian Infrastructure

Russia's campaign against Ukraine's power grid has demonstrated how kinetic attacks can disable SCADA and ICS systems at scale. With shared grid interconnectors (e.g., ENTSO-E synchronization with Ukraine and Moldova since 2022), European operators face spillover risks:

- Cyberattacks like **Industroyer2** have already targeted Ukrainian substations; similar malware could be repurposed against Polish, Romanian, or Slovak grids.
- Many EU distribution networks still run on outdated OT protocols (Modbus, DNP3) with minimal segmentation from corporate IT networks.

Risks to Gas Interconnectors and LNG Terminals

While EU gas storage levels are high, physical infrastructure remains vulnerable:

- Key interconnectors (e.g., Poland – Lithuania GIPL, Romania – Hungary BRUA) pass near conflict prone regions.
- LNG terminals in Germany (Wilhelmshaven), Poland (Świnoujście), and Croatia (Krk) are potential targets for drone or sabotage operations, especially if Russia seeks to amplify energy panic ahead of winter.

  Key Risk: Convergence of cyber physical threats to energy delivery, with cascading impacts on manufacturing, data centres, and public safety.

Risk Metrics:

- ICS/OT vendor reliance on non EU providers >60% (red flag); target <30%
- Grid outage duration >6 hours (red flag); target <2 hours

Mitigation & Preparedness:

- Segment OT networks from IT
- Accelerate firmware patching (<6 hours)
- Stockpile EU-made ICS hardware

2.3 Cloud, Data Centres & Digital Infrastructure

Cloud, Data Centres & Digital Infrastructure Overview

U.S. hyperscalers (AWS, Azure, Google Cloud) dominate >60% of the global market, with control planes outside EU jurisdiction, creating CLOUD Act-GDPR conflicts and concentration risks (e.g., 2023 Amsterdam Trade Bank collapse due to U.S. sanctions) [Japan Times], [Politico EU]. Physical resilience in Eastern Europe is vulnerable to hybrid threats, while 70% DNS queries route via U.S. providers (Akamai, Cloudflare), risking hijacking/blocking [Akamai]. Server (80% U.S. hardware like Intel/AMD), integration (60% U.S. tools like MuleSoft), payments (45% U.S. via Stripe/PayPal/CHIPS), cybersecurity (75% U.S. supply chains), and devices (65% U.S.-made like Apple) amplify dependencies, with cascading failures possible (e.g., cloud outage halting payments) [European Parliament], [NIST], [U.S. Department of Homeland Security].

- **Risk Metrics**: U.S. cloud share >60% (red flag, target <30%); non-EU DNS routing <50% (target ≥80%); U.S. payment share <50% (target ≥80%); U.S. device reliance >60% (target <30%).
- For detailed mitigations like BGP reconfiguration, EU DNS resolvers (DNS4EU), TLS/PKI sovereignty (EU Root CA, DANE), payment rails (EPI/wero), and browser strategies (Firefox investment), see Part 3 and Appendix A. Contract audits and EU alternatives (e.g., OVHcloud, SEPA, Adyen) remain essential starting points.

Summary Table: Critical Domains, Metrics, and Mitigation Actions

Domain	Key Risk Metric (Red Flag)	Target	Mitigation Action
Telecom	Non EU cable redundancy <40%	≥70%	Satellite backup, new cables
Energy/ICS	ICS vendor reliance >60%	<30%	Segment OT, patch firmware
Cloud/Digital Infra	U.S. cloud/DNS reliance >60%/<50%	<30%/≥80%	See Part 3 for sovereignty plans; audit vendors
Semiconductors	Asian manufacturing >60%	<40%	EU Chips Act onshoring
AI/Dual-Use	Export non-compliance risks	Full due diligence	See Part 4 and the Context volume for AI details; Regulation 2021/821 adherence
Transport/Rail	Signalling and control asset lifecycles	Renewal before end of life	Rail cyber standard CLC/TS 50701; segment signalling from corporate IT

2.4 Semiconductors & Hardware Supply Chains

Reliance on Asian Manufacturing (TSMC, Samsung)

Europe's semiconductor production stands at just 10% of global output, compared to 60% in Asia. TSMC alone produces over 90% of advanced logic chips (5nm and below), with fabs concentrated in Taiwan. A cross strait escalation could halt deliveries within days, crippling industries from automotive (infotainment systems) to healthcare (diagnostic equipment).

- TSMC's Arizona and Japan fabs won't reach full capacity before 2026–2027, and even then, will prioritize U.S. defence and consumer electronics.
- A Taiwan contingency could halt advanced chip shipments within **10–14 days**, idling European production lines.

EU Chips Act: Progress vs. Real-World Bottlenecks

The €43 billion EU Chips Act aims to double Europe's market share to 20% by 2030. Promising investments include:

- Intel's €30B "Silicon Junction" in Germany (2027 target)
- STMicroelectronics/GlobalFoundries joint venture in France
- Bosch's 300mm fab in Dresden

Yet bottlenecks persist:

- Shortage of skilled process engineers
- Limited EU based equipment makers (ASML dominates lithography but relies on U.S. and Japanese components)
- Slow permitting for cleanroom construction

  Key Risk: Strategic ambition outpaces execution timeline, leaving Europe exposed during the 2025–2028 window of maximum vulnerability.



Figure 1: High-Risk Infrastructure Corridors

- **Key Vulnerabilities**: Single source dependencies for GPUs, memory chips, and sensors; long lead times (6-12 months) for custom ASICs; exposure to export controls from China or the U.S.

Risks from Rare Earths and Dual Use Materials

China dominates 60% of rare earth mining and processing, essential for magnets in EVs, wind turbines, and electronics. U.S. or EU sanctions could trigger retaliatory restrictions, as seen in 2023 when China limited gallium exports.

- **Mitigation Strategies**: Diversify sourcing (e.g., U.S. Mountain Pass mine, Australian Lynas Corp.); invest in recycling technologies; stockpile critical materials under EU Critical Raw Materials Act.

  Key Risk: Fragile supply chains for foundational components, where geopolitical tensions can cause immediate, cascading failures across multiple sectors.

2.5 Transport and Rail Signalling

The dependency. Rail is a control system with people on it. The safety of a modern line rests not on the train but on the signalling layer that decides where a train may be and how fast it may move: the continuous train control system, the radio and trackside equipment that carry movement authority, and the brake-control telemetry that lets a driver or a control centre stop a train. Underneath them sit the copper, the fibre and the power feeds that connect the controlling computers to the track. Rail operators are designated operators of essential services in the member states whose critical-infrastructure law names transport, and the estate is long-lived: signalling and control assets are specified, installed and kept in service over lifecycles measured in decades.

What fails. The signalling layer holds train separation, and its failure modes are physical. A continuous train control system that loses communication across its controlling computers leaves the control centre making safety decisions on degraded information, and those decisions are made by people under time pressure. A signal that a signalling system trusts can be injected from outside: unauthorised radio-stop transmissions have stopped multiple trains on a national network. Signalling-adjacent radio protocols carry documented, unauthenticated weaknesses, and an agency advisory has confirmed that a remote-linking protocol with weak authentication allows an attacker to send their own brake control commands, causing a sudden stoppage or brake failure, exploitable wirelessly. The physical route is itself a target: copper cable theft at several points on a high-speed line damages the signalling installations and strands passengers across dozens of trains. When the control layer fails, the consequence is a collision of trains, the emergency stop of rolling stock, or a whole line closed while the cause is established.

What it costs. The cost is measured first in lives, and then in the operating loss of a line and the capital of the renewal that was already in progress when the failure occurred. A signalling estate that is mid-replacement is not a protected estate: a renewal programme measured in hundreds of millions of euro does not, by itself, remove the exposure in the interim. Stranded passengers on dozens of trains and a closed trunk route are a direct operational loss, and an investigation that must reconstruct the state of the controlling computers adds weeks before the line is trusted again.

Why compliance is not enough. The European rail sector is not unregulated. ENISA's railway cyber guidance treats a signalling or train control compromise leading to an accident as a low-likelihood scenario, and its transport threat landscape records rail attacks as dominated by ransomware, data-related incidents and denial of service, while stating it holds no reliable information of a cyberattack affecting transport safety. That is a statement about likelihood, not about the absence of a mitigation: the same guidance notes that operational technology was not designed with cybersecurity in mind and carries multi-decade asset lifecycles. Safety communication on the European train control system already uses cryptographic keys to protect the integrity and authenticity of exchanged messages against insertion, corruption and masquerade, and the technical specification for interoperability was amended by Commission Implementing Regulation (EU) 2026/693. Below the regulation sits the sector standard: CLC/TS 50701:2021, which takes in the safety-related aspects of EN 50126 and draws on IEC 62443-3-3 and the Common Safety Method for Risk Evaluation and Assessment, with EN 50159-2 as the underlying threat model. The gap the domain exposes is the familiar one: the operator can hold a renewal programme, a safety body can have seen the pattern, and a protection system and a driver's refusal can both exist, and the failure can still be that a decision was made anyway.

> **Key Risk**: A long-lived signalling and control estate where the binding constraints are the decision layer and the physical route, not the network perimeter.

Mitigation & Preparedness:

- Confirm that remote-linking and radio control implementations authenticate the controller, and that the check is universal across the fleet.
- Treat the copper, fibre and power feeds along the route as a guarding and theft question, not only an engineering dependency.
- Segment signalling and control networks from corporate IT, and keep the safety decision path explicit when control systems degrade.
- Ask suppliers to build to CLC/TS 50701 and EN 50159-2, and point procurement questions at the sector standard.

Part 3: The Internet Core: Routing, Names, Trust

This part delves into the foundational internet protocols like routing, name resolution, and secure communications, explaining how geopolitical tensions could disrupt them and what European businesses can do to build sovereignty. Executives will find high-level strategies for maintaining digital operations during crises, such as reconfiguring networks and adopting EU alternatives, with technical details on BGP, DNS, and PKI for deeper implementation. It connects to broader risks in Part 2 and Part 4, emphasising resilience in connectivity and trust.

3.1 Border Gateway Protocol (BGP)

> BGP is the core routing protocol that enables global internet connectivity by exchanging reachability information between autonomous networks, directing data traffic efficiently across borders.

If U.S.-based networks could no longer be trusted (due to espionage, sabotage, or geopolitical rupture), reconfiguring BGP for Europe would involve a multi-layered,

continent-wide effort focused on **security, redundancy, and re-routed trust**. Here's what would need to be done:

1. Immediate Operational Security Measures

- **RPKI (Resource Public Key Infrastructure) Mandate:** Enforce universal RPKI adoption across European ASes (Autonomous Systems). This cryptographically validates that an AS is authorized to announce specific IP prefixes, preventing hijacks from untrusted U.S. networks.
- **BGP Filtering:** All European ISPs and IXPs would implement strict prefix and AS-path filtering:
  - Reject routes originating from or transiting exclusively through U.S. ASNs where possible.
  - Accept only known legitimate prefixes from European and other trusted regions.
- **BGP Monitoring & Anomaly Detection:** Deploy real-time monitoring (e.g., using tools like BGPStream, ARTEMIS) to detect and respond quickly to malicious announcements.

2. Architectural Reconfiguration: Creating a "Trusted Core"

- **European Internet "Moonshot":** Develop a **European Internet Exchange & Transit Backbone** with minimal dependency on U.S. transit.
  - Incentivize major European Tier 1/2 providers (e.g., Deutsche Telekom, Orange, Telecom Italia, Telia) to peer extensively within Europe.
  - Expand capacity at major IXPs (AMS-IX, DE-CIX, LINX, etc.) and create new regional IXPs in Southern and Eastern Europe to keep traffic local.
- **Trans-Atlantic Link Re-evaluation:**
  - Classify all trans-Atlantic cables as **"untrusted links."**
  - Install "policy gateways" at cable landing stations (in Europe) to scrub and filter all BGP updates from U.S. peers before they enter the European core.
  - Consider **encrypting all international transit** (via MACsec or IPsec) at the physical layer for cables still in use.

3. Geopolitical & Policy Coordination

- **EU-Wide Mandate:** The European Commission and ENISA (EU Agency for Cybersecurity) would likely issue a regulation (similar to NIS2) requiring:
  - A "Digital Schengen" for routing, ensuring intra-EU/EEA traffic stays within trusted geography.
  - Mandatory cooperation among European NRENs (National Research and Education Networks) like GÉANT to form a secure, high-capacity scientific and research network independent of U.S. paths.
- **New "Trusted Peering" Agreements:** Replace peering and transit agreements with U.S. giants (like Cogent, Lumen, AT&T) with:
  - Increased peering with alternative global hubs (e.g., in Asia, Latin America, Africa) for global connectivity.
  - Strengthened direct peering with neighboring regions (e.g., Med. cables to North Africa, terrestrial links to Turkey/Ukraine for Asia connectivity).

4. **Technical Trust Overhaul**

- **MANRS (Mutually Agreed Norms for Routing Security) Compliance:** Make MANRS requirements mandatory for all European ISPs.
- **BGPsec (if widely deployed):** Accelerate adoption of BGPsec, which provides path validation (not just origin validation like RPKI). However, BGPsec deployment is currently limited.
- **Internal Trust Anchors:** Potentially create a **European RPKI root** or a tightly controlled regional trust anchor, separate from the global RIR system (which is influenced by U.S.-based organizations like ARIN and the legacy IANA functions, though these are now under the global community).

5. **Redundancy & Capacity Building**

- **Submarine Cable Diversification:** Fast-track new submarine cables that bypass the U.S., e.g.:
  - Europe to Asia via the Middle East (or Russia, if politically possible).
  - Europe to Latin America via Africa or direct cables (e.g., EllaLink).
- **Satellite Internet as Backup:** Leverage European-backed satellite constellations (e.g., IRIS², the EU's sovereign satellite initiative) for critical government and infrastructure backup links, reducing dependency on fiber. Note limitations: Satellites offer Gbps capacity vs. Tbps cables, higher latency (vs. 60ms), and jamming risks; use for low-bandwidth priority only (see Appendix B).

6. **Contingency Planning for a "Splinternet" Scenario**

- **Prefix De-aggregation Strategy:** In a crisis, European networks might need to announce more specific prefixes to attract traffic away from routes transiting the U.S., preventing blackholes.
- **Pre-configured "Break-Glass" Configurations:** Network operators would have pre-tested BGP configurations to:
  - Withdraw all routes learned from U.S. peers.
  - Prefer paths via Asia, Africa, or direct peering.
- **Critical Services Localization:** Ensure core Internet services (DNS root instances, major CDNs, cloud regions) have fully operational replicas within Europe, so traffic doesn't need to leave.

7. **Long-Term Strategic Shifts**

- **European Cloud & DNS Sovereignty:** Accelerate GAIA-X (European cloud initiative) and host more DNS root mirrors and TLD authoritative servers within Europe.
- **New Protocols Research:** Fund R&D into post-BGP architectures like **SCION** (which offers path-aware, trust-based routing) for critical infrastructure.

Major Challenges:

- **Economic Cost:** Increased transit costs within Europe and to other regions; potential slowdowns if alternative paths have higher latency.
- **Global Connectivity:** Isolating from U.S. networks could degrade performance to the Americas and potentially to parts of Asia that rely on U.S. transit.

- **Coordination Overhead:** Requires unprecedented cooperation between EU member states, regulators, and competing private operators.

Conclusion:

Reconfiguring BGP for Europe in this scenario would be less about changing the BGP protocol itself and more about **enforcing strict security policies, reshaping physical and logical network topology, and shifting geopolitical alliances in the digital realm.** The goal would be to create a **resilient, trusted European routing sphere** that can operate autonomously if necessary, while maintaining selective, heavily guarded connectivity to the U.S. and the rest of the world. This would be a massive, multi-year undertaking akin to building a parallel, secured internet infrastructure.

3.2 Domain Name System (DNS)

> DNS is the internet's domain name resolution system, translating human-readable domain names (e.g., google.com) into IP addresses for routing traffic.

Bringing a new, European-controlled "root-level" DNS server online in a crisis is technically possible, but its practical effectiveness for maintaining a functional internet in Europe during a major outage is highly questionable. The core issue is that such a server would not be trusted by the global system or the devices within Europe.

The Technical vs. Political Challenge

- **Technically Straightforward**: The basic software and hardware to run a root name server are not exotic. Many organizations globally run "instances" of the existing 13 root server identifiers . The EU could download the root zone file and set up a local copy .
- **Politically & Practically Insurmountable**: A new root server would have no authority within the global DNS hierarchy, which is governed by **ICANN and the 12 independent root server operators**. For it to be effective, every network, device, and DNS resolver in Europe would need to be reconfigured to use it, replacing the built-in list of the global 13 root server addresses. This is not feasible in a short-term crisis.

How the Internet Would Actually Fail

Without US connectivity, the problem isn't that European root server instances disappear. Several (like **I-Root in Sweden**, run by Netnod, and **K-Root in the Netherlands**, run by RIPE NCC) already exist physically in Europe . The real breakdown happens downstream in the DNS resolution chain:

1. **Root Servers (Physical OK, Logical Broken)**: European root instances could still answer queries. However, if they cannot connect to the master source for the root zone file (managed by **IANA/ICANN** based in the US) to get updates, they would be serving outdated information, unable to add new `.com` or `.org` websites .

2. **Critical Failure at TLD Servers**: This is the main point of failure. The servers that manage `.com`, `.net`, `.org`, etc., are largely operated by **US-based entities like Verisign**. Even if a European computer asks a European root server for `example.com`, the root server would respond with the IP address of the `.com` servers, which are likely hosted in the US and unreachable .
3. **Authoritative Name Servers**: Finally, the servers that hold the actual IP addresses for specific websites (e.g., your company's site) might also be hosted on US-based cloud platforms like AWS, making them unreachable.

The More Realistic European Focus: DNS Resolvers

Given the above, European digital sovereignty efforts are more focused on the **recursive DNS resolver** level. These are the servers your devices actually query. Here, there are active European projects:

Project / Service	Jurisdiction & Description	Role in a Crisis
DNS4EU	An EU-funded public DNS resolver service with servers **exclusively within EU member states**.	If TLDs were still reachable, this would keep queries within European infrastructure, enhancing privacy and resilience
Quad9	A Swiss-based non-profit operating a global, secure DNS resolver	Provides a non-US jurisdiction alternative, though its global network might be affected by a US-EU split
National/Local Resolvers	Many European ISPs, organizations, and privacy groups run their own resolvers (e.g., in Germany, Austria, Luxembourg)	Local control at the resolver level is the most practical layer for sovereignty, though still dependent on the upstream TLD system

Recommendation for your planning: For true resilience in an extreme scenario, your organization should consider: 1. **Caching aggressively**: Configure internal DNS servers to hold records for critical domains for as long as possible. 2. **Maintaining a local hosts file**: For absolutely critical internal and partner services, maintain static IP-to-name mappings.

3.3 Certificate & Security Chain (HTTPS/TLS)

> HTTPS/TLS is the internet's secure communications protocol, using digital certificates to authenticate entities and encrypt data in transit, protecting against interception and tampering in contested environments.

If U.S.-based networks and services could no longer be trusted, the European digital certificate ecosystem would face immediate, systemic risks. The global HTTPS/TLS system relies overwhelmingly on U.S.-based **Certificate Authorities (CAs)** and

the infrastructure they control. A rupture would compromise trust, validation, and encryption for nearly the entire web.

The Central Risk: U.S.-Centric Trust Anchors

The security of every `https://` connection ultimately depends on a list of trusted "Root Certificate Authorities" (Root CAs) hard-coded into your browser and operating system. These Root CAs are the ultimate issuers of trust. As of today: * **A majority of these globally trusted Root CAs are operated by U.S.-based companies** (e.g., DigiCert, Sectigo, Google Trust Services, Microsoft). * The technical and policy bodies that govern the rules for CAs (the **CA/Browser Forum**) are heavily influenced by U.S. corporate and legal frameworks.

In a crisis where U.S. entities are deemed untrustworthy, their Root CAs could be weaponized to: * **Issue fraudulent certificates** for European government, banking, or critical infrastructure sites, enabling perfect man-in-the-middle attacks. * **Revoke valid European certificates**, causing widespread outages for services that depend on them.

A European Response Strategy

To build a sovereign and resilient certificate chain, Europe would need to execute a multi-phase plan:

Phase 1: Immediate Mitigation & Aggressive Monitoring

- **Mandate Certificate Transparency (CT) Logs in EU Jurisdiction:** Require all certificates valid for EU domains to be logged in CT logs operated and controlled within the EU. This creates a public, auditable record to detect fraudulent issuance instantly.
- **Deploy Advanced Certificate Monitoring:** Implement tools like **Censys** or **Crt.sh** monitoring at a continental level to alert on any suspicious certificate issuance for critical `.eu`, `.fr`, `.de`, etc., domains, especially from non-EU CAs.
- **Promote EU-Based Public CAs:** Mandate the use of EU-headquartered CAs (like **GlobalSign** (BE/NL), **Sectigo** (though US-owned, has EU operations), or **D-Trust** (DE)) for all EU governmental and critical infrastructure services.

Phase 2: Building Sovereign Trust Infrastructure

- **Create a European Root CA:** Establish a new, **EU-government-backed Root Certificate Authority**. This is a political and technical project on par with creating a central bank.
- **Force-Injection into EU Devices:** Mandate through regulation (e.g., an expanded **Radio Equipment Directive**) that all devices sold in the EU must include this **"EU Trust Root"** in their trust store, alongside existing global roots.
- **Develop an EU-Only PKI Profile:** Define stricter technical and legal requirements for certificates used in Europe (e.g., mandatory hardware security modules, specific audit standards, data residency for validation services) that go beyond the global baseline.

Phase 3: Contingency Planning for Decoupling

- **Prepare for Mass Revocation:** Have technical and legal plans to **revoke trust in U.S.-based Root CAs** from European systems in a controlled, phased manner. This would be a "break-glass" action causing massive disruption but may be necessary.
- **Cross-Certification with Allied Trust Anchors:** Establish technical cross-certification agreements with other allied, non-U.S. root programs (e.g., in **Switzerland, the UK, Japan, or South Korea**) to create a broader "Allied Trust Network" as a counterbalance.
- **Accelerate Post-Quantum Cryptography (PQC):** Invest heavily in the adoption of **PQC algorithms** within the EU PKI. This future-proofs against a scenario where a hostile actor with a quantum computer could break current encryption and retroactively decrypt traffic.

The Critical Link to BGP & DNS

A sovereign security chain cannot exist in isolation; it must integrate with the re-configured BGP and DNS layers: * **BGP + PKI:** If a European entity's IP space is hijacked via BGP, even a valid certificate is useless, as traffic can be redirected to an attacker's server. **RPKI (from the BGP section) is the essential companion to TLS certificates.** It proves ownership of the IP address, just as a certificate proves ownership of the domain name. * **DNS + PKI (DANE):** Europe could aggressively promote **DNS-Based Authentication of Named Entities (DANE)**. This technology uses DNSSEC (secured DNS) to store a website's TLS certificate or public key directly in its DNS record. This **bypasses the need for traditional CAs entirely**, anchoring trust in the DNSSEC chain, which Europe could control via its own root and TLDs (e.g., `.eu`).

Major Challenges

- **Browser & Device Hegemony:** Major browser vendors (Google Chrome, Apple Safari, Microsoft Edge) and OS makers control the default trust stores. Gaining their acceptance for a new geopolitical root is a monumental challenge.
- **Global Interoperability Fracture:** If Europe uses a different set of trusted roots, European citizens and businesses may encounter "certificate warnings" when accessing non-EU websites, creating a fractured user experience.
- **Operational Complexity:** Running a Root CA at a continental scale with the requisite ultra-high security, availability, and legal liability is a massive, costly undertaking.

Conclusion

Securing the certificate chain is about **controlling the source of digital trust**. Europe's path would involve: 1. **Monitoring** all certificate issuance for its domains. 2. **Building** its own sovereign root of trust and injecting it into the European digital ecosystem. 3. **Integrating** this trust layer with secured routing (RPKI) and DNS (DNSSEC/DANE) to create a defensible, end-to-end trusted internet infrastructure within its borders.

Without this, even with a secured BGP and DNS layer, the foundational trust behind every encrypted connection would remain vulnerable to external compromise.

Summary Table: Internet Core Protocols and Actions

Protocol	Key Risk	Mitigation	Reference
BGP (5.1)	Hijacking via U.S. routes	RPKI mandate, filtering, European backbone	MANRS compliance
DNS (5.2)	TLD unreachability	DNS4EU resolvers, aggressive caching	Quad9 alternatives
TLS/PKI (5.3)	U.S. CA weaponization	EU Root CA, CT logs, DANE	Post-quantum migration

Building on AI and cloud risks from Part 2 and Part 4, this part provides the technical foundation for sovereignty. For deeper strategies on browsers, communications, and payments, see Appendix A (Cross-Cutting Toolkit).

Conclusion

This part's integrated approach (securing **BGP** routing with **RPKI**, **DNS** resolution via EU resolvers like **DNS4EU**, **TLS** trust through an EU Root CA and **DANE**) forms a defensible digital foundation. These measures directly counter the threat vectors in the companion Context volume (e.g., **DNS** hijacking in economic coercion) and inform the mitigation frameworks in Part 5 (e.g., continuity planning with Gaia-X). By implementing phased plans, European businesses can achieve operational autonomy in contested environments. Detailed browser/comms/payment strategies in Appendix A.

Part 4: AI and Your Firm

Pathways to AI Sovereignty

Using EU-based AI providers and running open-source LLMs on local hardware are the core solutions to achieving digital sovereignty for Europe. This approach offers clear benefits but also introduces significant, often complex, new challenges in exchange for the control it provides.

These two methods work together to reduce dependency on US-controlled AI infrastructure and data flows. **Mistral AI** (a French startup) is the most prominent European alternative, positioned as a "sovereign" option with its Apache-licensed models designed to run from the cloud to the edge. Open-source LLMs (including those from Meta, Google, or Mistral) allow for **complete local control** as they can be run on in-house European hardware, ensuring that sensitive data and critical operations never leave European jurisdiction.

Switching to this model exchanges one set of risks for another, which must be carefully managed.

Aspect	Benefits & Opportunities	Risks & New Dependencies
Legal & Regulatory Compliance	Offers a **structural advantage** for complying with the **EU AI Act**, GDPR, and EU data residency laws.	**Enforcement gaps exist**. Some providers, including European ones like **Mistral**, have not fully complied with the AI Act's transparency rules on training data.
Operational & Cost Control	**Predictable infrastructure costs** (not usage-based), **low-latency performance**, and **no risk of external API changes or outages**.	**High upfront cost** of GPU hardware, expertise, and energy. Requires significant **internal IT and MLOps resources** to deploy, maintain, and secure.
Performance & Capability	**Full customisability** for specific tasks (fine-tuning) and control over updates and feature sets.	**Potential performance gap**: Top open-source models may **lag behind the frontier models** from OpenAI or Anthropic.
Supply Chain & Sovereignty	**Reduces strategic dependency** on US cloud providers for core AI logic and processing.	**Shifts dependency to hardware**: Europe is still critically dependent on **US-designed advanced chips (e.g., from NVIDIA)** for training and running these models.

Key implementation challenges and mitigations:

1. **Managing the Compliance Gap**: Even European providers may fall short of EU regulations. To manage this, you must **proactively demand transparency** (full training data disclosure, model cards) and have legal teams audit provider compliance.
2. **Building Internal Competence**: Success depends on in-house expertise. **Invest in specialised talent** for model operations, infrastructure security, and domain-specific fine-tuning.
3. **Creating a Sovereign Ecosystem**: A single company is not an ecosystem. You should support and integrate with other EU initiatives, such as:
    - **Alternative Infrastructure**: Explore the **GAIA-X** initiative for federated European cloud services.
    - **Policy & Guidance**: Utilise the **EU AI Act's regulatory sandboxes** for testing and guidance.
    - **Alternative AI**: Consider other European models like Aleph Alpha.

Strategic recommendations for European policymakers and businesses:

- **Dual Strategy is Essential**: Promote a hybrid model where **Mistral** and

similar providers serve as the base layer for sensitive applications, whilst US providers may still be used for non-critical R&D.

- **"Open Weight" is Not "Open Source"**: Clearly differentiate between truly open-source projects and "open-weight" models like Meta's Llama. The latter often come with **complex licences** that can restrict commercial use. Favour models with permissive licences like Apache 2.0.
- **Sovereignty Starts at the Edge**: Prioritise **edge deployment** (e.g., using models like Mistral's Ministral 3) for latency, cost, and data control.
- **Regulation Must Be Enforced**: The **EU AI Act** is a powerful tool for sovereignty, but its transparency requirements must be **actively and uniformly enforced** against all providers, including European ones, to be effective.

This builds on the AI dependency risks in the companion Context volume, and links to Part 2's EU Chips Act for hardware sovereignty and Part 3's GAIA-X for cloud. For UK: Align with AI Safety Institute; Canada: Leverage CSE strategies.

Part 5: The Mitigation Framework

This part offers practical strategies for mitigating technology risks through diversification, cyber defence, continuity planning, scenario exercises, and vendor management, tailored for European and allied enterprises. Executives can quickly identify key pillars to strengthen resilience, with actionable steps for implementation. It translates analysis from earlier chapters into business-focused frameworks for long-term stability.

Compliance alone cannot ensure continuity in an era of hybrid warfare, supply chain weaponisation, and transatlantic uncertainty. This part provides a proactive, multi-tiered mitigation framework that moves beyond regulatory checkboxes to operational resilience. It is structured around five pillars: **Diversification**, **Defence**, **Continuity**, **Scenario Planning**, and **Vendor Governance**.

5.1 Supply Chain Diversification & Onshoring Strategies

Strategic Goal: Reduce single points of failure in critical components and services.

Actions:

- **Map Tier 2 and Tier 3 suppliers** for semiconductors, optical transceivers, battery cells, and industrial control systems. Identify dependencies on Taiwan, China, or U.S. only vendors.
- **Qualify alternative sources** in trusted jurisdictions (e.g., Japan for memory chips, South Korea for displays, EU based PCB assemblers).
- **Accelerate participation in EU sovereign initiatives**:
  - Use **EuroHPC** for secure AI/ML workloads
  - Adopt **Gaia-X** aligned cloud providers for data residency
  - Partner with **European Processor Initiative (EPI)** for future CPU/GPU needs

- **Stockpile strategic buffers**: For mission critical hardware (e.g., **ICS** controllers, 5G radios), maintain 90–180 days of inventory, especially for components with >6 month lead times.

  Example: An automotive Tier 1 supplier shifts 30% of its MCU sourcing from TSMC to STMicroelectronics' new Crolles fab, accepting a modest performance trade off for guaranteed EU allocation.

5.2 Cyber Hygiene & Zero Trust Architecture

Strategic Goal: Assume breach; contain lateral movement.

Actions:

- **Implement Zero Trust Network Access (ZTNA)** for all remote and third-party connections, especially for OT environments.
- **Segment IT and OT networks** with unidirectional gateways (data diodes) where realtime control is required.
- **Enforce firmware integrity checks** using hardware rooted trust (e.g., TPM 2.0, Intel SGX) for servers and edge devices.
- **Adopt SBOMs (Software Bills of Materials)** and integrate them into vulnerability management platforms (e.g., automatically flag Log4j style risks).

  Critical Gap: Many European firms still allow corporate laptops to connect directly to factory floor networks. This must end.

5.3 Continuity Planning for Critical Infrastructure

Strategic Goal: Maintain operations during partial or total infrastructure loss.

Connectivity Resilience:

- **Diversify undersea cable paths**: Avoid reliance on single landing zones (e.g., don't route all traffic through Cuxhaven). Use satellite backup (e.g., Starlink Business, EU IRIS² constellation) for emergency comms.
- **Deploy mesh networking** at regional HQs to enable local coordination if internet fails.

Energy Autonomy:

- **Install microgrids** with solar + battery storage at data centres and manufacturing sites.
- **Pre negotiate emergency power agreements** with national grid operators for "critical enterprise" status.

Data & Compute Continuity:

- **Maintain sovereign cloud failover**: Replicate core workloads in at least two EU based regions (e.g., Azure Germany + OVHcloud France), aligning with Part 3's Gaia-X backbone and EU DNS resolvers for resilient routing.
- **Test offline operation**: Can your ERP run for 72 hours without cloud sync? If not, redesign. Incorporate Part 3's BGP filtering and DANE for secure, autonomous connectivity. See new subsection below for software licensing details.

Reality Check: During the 2022 Ukraine blackouts, companies with local diesel generators and cached DNS survived; those dependent on cloud APIs did not.

Software Licensing Resilience

Microsoft and other software dependencies create offline risks through activation and subscription checks. Audit licensing models to identify vulnerabilities.

Activation Type	Offline Behavior	Grace Period	Mitigation
MAK (Multiple Activation Key)	Works indefinitely after initial activation.	None after setup.	Use for air-gapped systems; pre-activate all devices.
KMS (Key Management Service)	Renews every 7 days; expires after 180 days without host contact.	180 days.	Maintain internal KMS host; plan secure check-ins or MAK fallback. Note: KMS host needs Microsoft contact every 180 days.
Subscription (e.g., M365)	Check-in every 30 days; reduced functionality after.	30-99 days.	Shift critical apps to perpetual licenses; test offline modes.
Perpetual Office (e.g., 2021)	Runs offline post-activation, but new setups need portal (no phone activation since Dec 2025).	Indefinite.	Stockpile install media; use VAMT for batch activation.

For SaaS (e.g., Adobe CC, Slack), expect full failure after grace periods. Prioritise on-premises alternatives. Cross-ref Appendix A for comms (e.g., Matrix offline). For UK/Canadian firms, align with NCSC/CSE offline guidelines; inventory by model and test scenarios like "U.S. Cloud Freeze" (Part 3).

Software Category	Offline Impact	Examples
Subscription SaaS	Stops after 30 days; view-only mode.	Adobe CC, M365.
Perpetual	Full operation post-activation.	Office 2021, VLC.
Development Tools	Core offline; cloud features fail.	VS Code, Docker (local).

5.4 Geopolitical Scenario Planning

Strategic Goal: Stress test strategy against plausible, high-impact disruptions.

Conduct Tabletop Exercises for:

- **"Baltic Cable Cut"**: Simulate loss of 3+ subsea cables. Test financial transaction routing, employee comms, and customer support fallbacks.
- **"Taiwan Blockade"**: Model 60-day chip shortage. Identify which product lines can shift to older-node alternatives; which must halt.
- **"U.S. Cloud Freeze"**: Assume AWS/Azure/GCP restrict access to EU accounts due to U.S. executive order. Validate sovereign cloud migration playbooks.
- **"Hybrid Energy Attack"**: Combine cyber intrusion (grid SCADA) + drone strike (LNG terminal) + disinformation ("rolling blackouts"). Test crisis comms and board decision protocols.

Frequency: At least **biannual** for critical sectors; involve legal, procurement, and executive leadership, not just IT.

5.5 Vendor Risk Management

Strategic Goal: Ensure third parties do not become attack vectors or compliance liabilities.

Enhanced Due Diligence Measures:

- **Screen for ultimate beneficial ownership (UBO)**: Use tools like OpenSanctions or national business registers to detect hidden ties to sanctioned entities.
- **Require CRA and NIS2 compliance attestations** in all tech contracts, especially for cloud, SaaS, and embedded systems.
- **Embed continuity clauses**: Contracts should specify:
  - Minimum service levels during conflict
  - Right to audit physical security of data centres
  - Data portability guarantees within 30 days

Red Lines:

- No vendor with significant R&D or manufacturing in non EU jurisdictions should have **unrestricted remote access** to OT systems.
- Avoid sole source dependencies on vendors headquartered in countries with **extraterritorial data laws** conflicting with GDPR.

  Best Practice: A German energy firm now requires all ICS vendors to host maintenance portals within the EU and use certificate based authentication, not passwords.

Cross Cutting Principles

1. **Resilience is a board level issue**: Technology risk must be reported alongside financial and operational risk.
2. **Sovereignty ≠ isolation**: Leverage global innovation, but anchor critical functions in trusted, auditable ecosystems.
3. **Test relentlessly**: A plan untested is a plan that fails.

Cross Cutting Preparedness Toolkit

To operationalize the above mitigations across digital infrastructure:
1. Deploy a Gaia-X integrated dashboard [European Parliament] to monitor metrics in real time.
2. Conduct bi-annual supply chain audits via NIST SP 800-161r1 guidelines [NIST].
3. Mandate sector specific resilience plans (EU Digital Services Act amendment, 2026).
4. Stockpile EU made hardware for 6 month downtime scenarios.
5. Align workload placement strategies with Gartner's 2025 regional customer intimacy framework [Gartner] to reduce reliance on U.S. peering points.

This framework equips European businesses not just to survive disruption, but to **maintain competitive advantage** when others falter. The companion Context volume explores how public/private collaboration can amplify these efforts at scale.

Appendix A: Cross-Cutting Preparedness Toolkit

This appendix provides practical tools and detailed strategies for implementing sovereignty measures across the parts of this volume, including the browser, communications and payments material. Use for technical teams to operationalize high-level recommendations.

Browser Sovereignty: Phased Strategy

The case for a European sovereign browser remains strong, but it must be approached strategically.

1. **Ultimate Control Over the Trust Store:** A European browser (e.g., `EU Explorer` or `Aegis Browser`) would ship with the **EU Trust Root CA** pre-installed, allowing selective de-prioritisation of foreign roots. This decisively solves browser hegemony.
2. **Integrating Sovereign Tech Stack:** Native integration with EU projects, including default search to EU alternatives (e.g., Mojeek, Qwant), **DNS4EU**, **DANE** support, and **eIDAS 2.0** wallets. Privacy aligned with **GDPR** by default.
3. **Diplomatic and Standards Leverage:** A state-backed browser enhances negotiating power in the **CA/Browser Forum** and **W3C**, positioning Europe as a platform holder.
4. **Security from Ground Up:** Reduced attack surface with post-quantum cryptography and stripped legacy components.

Challenges

- **Cost & Complexity:** Multi-billion-euro effort for security patches, compatibility, and ecosystem building.
- **Distribution:** Regulatory mandates for pre-installation and user adoption against entrenched habits.

- **Fragmentation Risk:** Divergence could fracture the web, causing compatibility issues.

Phased Approach

Phase 1: Leverage (Next 2-3 Years)

- **Regulate Trust Stores:** Mandate inclusion of **EU Trust Root** in all EU-distributed browsers via **Radio Equipment Directive** or **Digital Markets Act**.
- **Fund Firefox:** Invest hundreds of millions in Mozilla for an **"EU Sovereignty Build"** with default EU trust/privacy settings.

Phase 2: Hedge (Parallel, Long-Term)

- **Strategic Browser Reserve:** Fund a clean fork of Chromium/Gecko as a "break-glass" codebase for crises, synced with upstream fixes.

Phase 3: Moonshot (Decadal)

- **Trusted Client Initiative:** Develop a post-quantum client for government/critical sectors, expanding to public use.

Communications Sovereignty: Contingency for Email and Messaging

European digital communication depends on US platforms, risking disruption in geopolitical ruptures.

Core Risks

- **Consumer Messaging:** Proprietary protocols (WhatsApp, iMessage) with US server control.
- **Enterprise Comms:** Cloud-tied tools (Teams, Slack) vulnerable to access revocation.
- **Email Backbone:** SMTP relies on US MTAs; DNS/PKI disruptions amplify failures.

Three-Pillar Plan

Pillar 1: Activate Alternatives

- **Matrix as Standard:** Formalise Matrix protocol as **EUS-MSG-1**; launch **EU-Connect** app for government/critical use.
- **Sovereign Email:** Mandate EU cloud migration (e.g., GAIA-X); create `mail-relay.europa.eu` network.

Pillar 2: Break-Glass Comms

- **Crisis Packets:** Distribute USBs with Matrix clients and key caches.
- **Priority Layer:** Use EUROCONTROL/Galileo for low-bandwidth emergency messaging; develop Bluetooth mesh apps.

- **Email Decoupling:** Dual MX records with EU backups; trusted senders list via RPKI-like system.

Pillar 3: Long-Term Architecture

- **Project Dialogos:** Post-quantum, federated suite with **eIDAS** integration.
- **Protocol Diplomacy:** Standardise federation in IETF; fund EU contributions.
- **Sovereign Push:** Open-source alternative to Apple/Firebase.

Governance

- **ECR Regulation:** Suspend app exclusivity; prioritise sovereign traffic.
- **EDCA Authority:** Certify tools and run drills.

This integrates with Part 5.3 for offline continuity and counters the threat vectors in the companion Context volume, such as "Transatlantic Tech Rift." For UK/Canada: Align with NCSC/CSE guidelines.

Payment System Sovereignty: Contingency Plan

Current European payment infrastructure exists in a state of **strategic dependency** on US-controlled systems. In a rupture, disruptions to card networks (Visa/MasterCard), gateways (PayPal, Stripe), and settlement (SWIFT) could halt transactions.

Key Strategy: - Activate EPI/wero for instant payments; build standby engines with SEPA integration. - Develop Digital Euro rails for sovereignty; test cross-border fallbacks. - **Risk Metrics**: U.S. payment share >45% (target <20%); ensure 24-hour failover testing.

Implementation Steps: 1. Audit vendors for sanctions clauses. 2. Migrate 50% volume to EU rails (Adyen, wero) by 2027. 3. Stockpile offline POS hardware for retail.

Cross-ref Part 5 for vendor governance. Resources: EPI, Digital Euro. For the European Network for Payments, the joint interoperability entity announced by five European payment firms on 30 September 2026, see the companion *Context* volume, *Geopolitical Context and Strategic Threat Landscape*.

AI Offline Note (Part 4)

Local LLMs via Mistral for inference; test edge deployment on EU hardware to ensure sovereignty during disruptions.

Appendix B: Offline Software Behaviors Guide

This appendix compiles behaviors of key software during extended offline periods, aiding continuity planning (Part 5.3). Focus on licensing and functionality impacts.

Microsoft Products Offline Summary

Product	Offline Behavior	Grace Period	Notes
Windows (MAK)	Indefinite after activation.	None.	Pre-activate; no phone option since Dec 2025; use portal on jump box.
Windows (KMS)	Expires after 180 days without host.	180 days.	Host needs Microsoft every 180 days; notification mode post-expiry.
M365 Apps	Reduced functionality (view/print only).	30-99 days.	Shift to perpetual for critical use.
Office Perpetual	Full after activation.	Indefinite.	Download media offline via connected device.
Exchange/SharePoint (On-Prem)	Full local operation.	None.	Internal network dependent; manual updates needed.

Non-Microsoft Desktop/SaaS Summary

Category	Offline Impact	Examples	Mitigation
Creative (Subscription)	Editing disabled after grace.	Adobe CC (30 days).	Perpetual alternatives; local assets.
Productivity SaaS	Core fails without cloud.	Google Workspace, Slack.	On-premises backups; test sync.
Dev Tools	Core offline; cloud features fail.	Docker local, VS Code.	Local registries; offline builds.
Comms	Real-time stops.	Teams, Zoom.	Matrix/EU-Connect (Appendix A); mesh apps.

Satellite Connectivity Limitations (Part 2)

Issue	Impact	Mitigation
Capacity	Tbps cables vs. Gbps satellites.	Prioritise low-bandwidth (e.g., IRIS² for emergency).
Latency	60ms cables vs. higher satellite.	Non-real-time apps only.
Jamming	Easy disruption.	Layer with cables; electronic warfare drills.

Cross-ref Appendix A for comms, Part 5 for planning. For UK/Canada: NCSC/CSE equivalents.

AI Offline Note (from Part 4)

Local LLMs for offline inference; test edge deployment (e.g., Mistral models on EU hardware) to ensure sovereignty during network disruptions. Grace period: Indefinite post-setup; mitigate hardware dependencies via EU Chips Act stockpiles.

Appendix C: Glossary of Geopolitical and Technical Terms

Term	Definition
APT (Advanced Persistent Threat)	State sponsored cyber actor conducting long term, stealthy operations (e.g., APT28 = Russian military intelligence)
Dual Use Technology	Items with both civilian and military applications (e.g., AI surveillance, quantum sensors), regulated under EU Regulation 2021/821
Hybrid Warfare	Combined use of conventional, cyber, economic, and informational tactics to destabilize adversaries without formal war
NIS2 Directive	EU law requiring enhanced cybersecurity measures and incident reporting for critical sectors
SBOM (Software Bill of Materials)	Inventory of open source and third party components in software, required under CRA
Zero Trust Architecture	Security model assuming no implicit trust; verifies every access request regardless of origin
Matrix Protocol	Open, federated messaging standard for sovereign communications (Appendix A).
SaaS (Software as a Service)	Cloud-based subscription software vulnerable to connectivity loss (Part 5).
EU AI Act	EU regulation for high-risk AI transparency and compliance (Part 4).
LLM (Large Language Model)	AI systems for natural language processing, often reliant on U.S. models/hardware (Part 4).
Mistral AI	EU-based sovereign LLM provider with open-licensed models (Part 4).

Term	Definition
Model Weights	Proprietary AI parameters under U.S. export control (Part 4).
OT (Operational Technology)	Hardware/software controlling physical devices (e.g., power grids, factory robots); distinct from IT
BGP (Border Gateway Protocol)	Internet routing protocol for exchanging reachability information between networks; vulnerable to hijacks in geopolitical ruptures (see Part 3).
Certificate Authority (CA)	Entity that issues digital certificates to verify the identity of websites and entities in TLS/PKI systems (Part 3).
Certificate Transparency (CT)	Public logging system for monitoring and auditing certificate issuance to detect mis-issuance (Part 3).
DANE (DNS-Based Authentication of Named Entities)	Protocol using DNSSEC to authenticate TLS certificates, bypassing traditional CAs for sovereignty (Part 3).
DNS (Domain Name System)	Internet's domain name resolution system, translating human-readable names to IP addresses (Part 3).
DNSSEC	Extension to DNS providing authentication of DNS data to prevent spoofing (Part 3).
MANRS (Mutually Agreed Norms for Routing Security)	Guidelines for improving BGP routing security through filtering and validation (Part 3).
PKI (Public Key Infrastructure)	Framework for managing digital certificates and public-key encryption (Part 3).
RPKI (Resource Public Key Infrastructure)	Cryptographic framework validating BGP route announcements to prevent hijacking (Part 3).
SCION	Path-aware networking architecture for secure, policy-based routing as an alternative to BGP (Part 3).
Splinternet	Fragmentation of the global internet into regional silos due to geopolitical tensions (Part 3).
TLS (Transport Layer Security)	Protocol for secure internet communications, using certificates for authentication and encryption (Part 3).

Appendix D: Map of High Risk Infrastructure Corridors

Undersea Cable Hotspots:

- **Baltic Sea**: Cables between Gotland (Sweden), Bornholm (Denmark), Tallinn (Estonia), and Klaipėda (Lithuania).
- **North Sea**: Routes linking UK, Netherlands, Germany (Wilhelmshaven/Cuxhaven), and Norway.
- **Black Sea**: Limited redundancy; vulnerable near Odesa and Constan□a.

Energy Interconnectors at Risk:

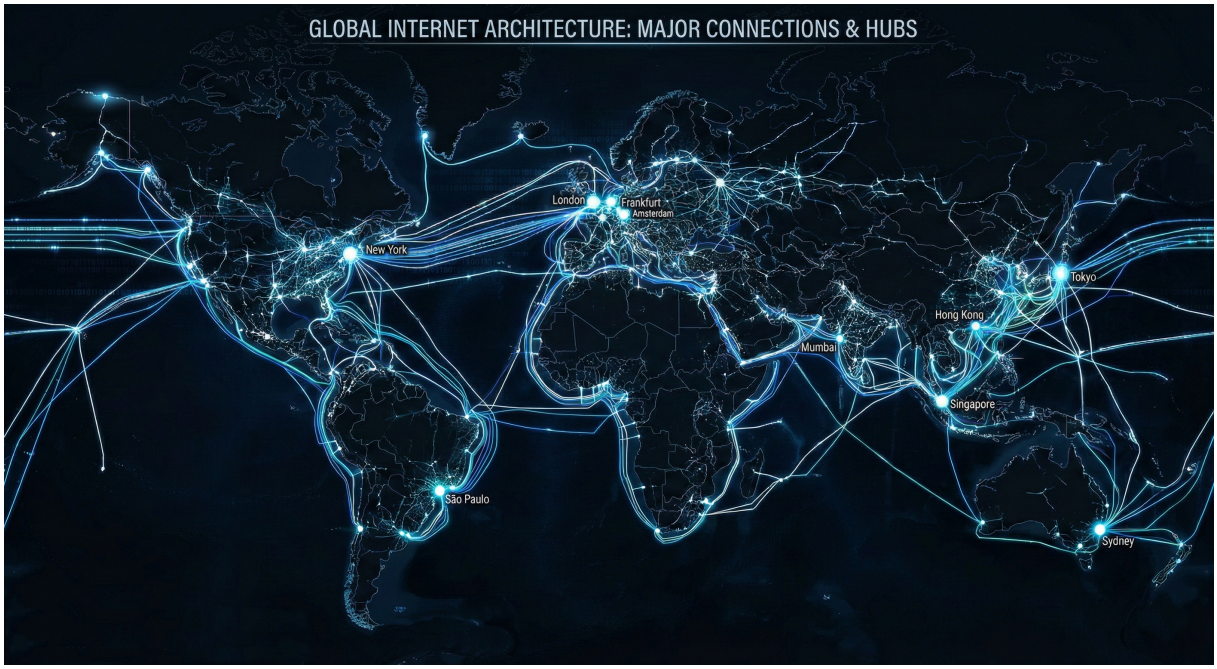


Figure 2: World Map of High-Risk Corridors

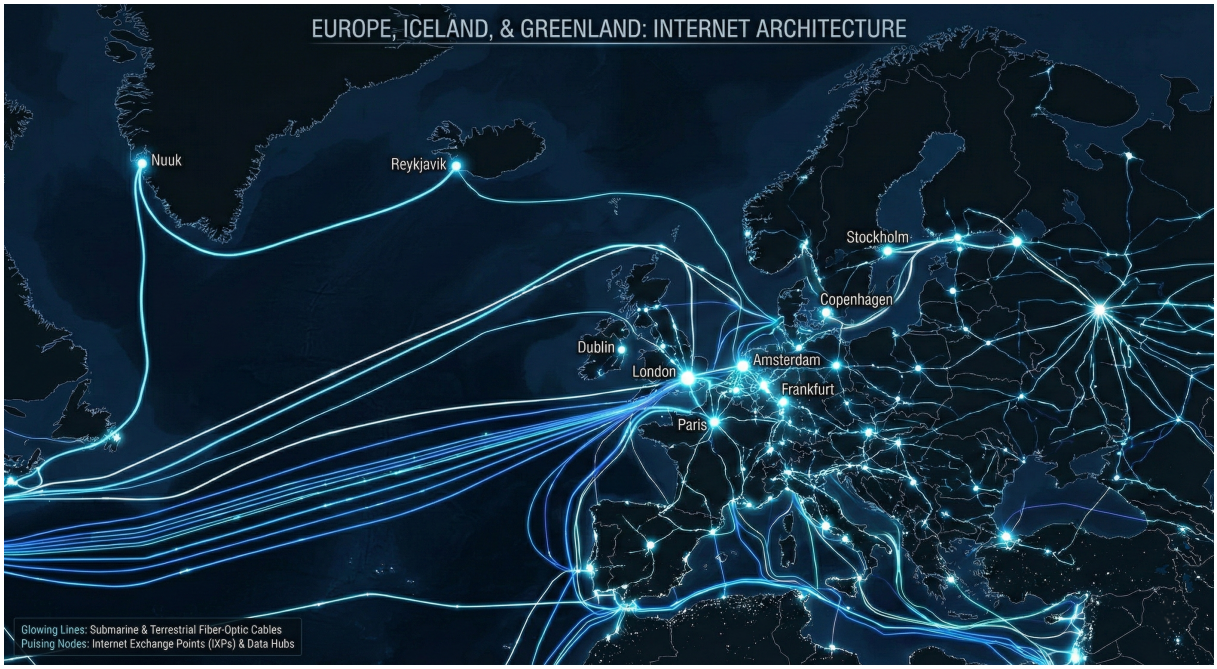


Figure 3: Detailed Europe Map of Infrastructure Risks

- **LitPol Link** (Lithuania–Poland)
- **BRUA Pipeline** (Bulgaria–Romania–Hungary–Austria)
- **GIPL** (Gas Interconnector Poland–Lithuania)
- **Isaccea–Orlivka Power Line** (Romania–Ukraine border)

Semiconductor Supply Chokepoints:

- **Taiwan Strait**: >90% of advanced logic chips transit this zone
- **Strait of Malacca**: Critical sea lane for raw materials (e.g., neon gas, rare earths)

Appendix E: Key Resources

Conflict & Threat Monitoring

- ACLED Ukraine Conflict Monitor – Real time tracking of violence against infrastructure (https://acleddata.com/monitor/ukraine-conflict-monitor)
- ENISA Threat Landscape Reports – Annual cyber threat analysis (https://www.enisa.europa.landscape)
- OpenSanctions – Database of sanctioned entities and politically exposed persons (https://www.opensanctions.org)

Regulatory Guidance

- EU Cyber Resilience Act (CRA) Text (https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act)
- NIS2 Directive Implementation Guidelines (https://ec.europa.eu/digital-single-market/en/network-and-information-security)
- EU Dual Use Regulation (2021/821) (https://trade.ec.europa.eu/doclib/docs/2021/may/trac

Sovereign Infrastructure Initiatives

- Gaia-X Association – European cloud/data infrastructure framework (https://gaia-x.eu)
- EU Chips Act Portal – Funding and project tracking (https://chips-act.ec.europa.eu)
- IRIS² Programme Overview – Secure EU satellite comms (https://digital-strategy.ec.europa.eu/en/policies/iris2)

Scenario Planning Tools

- ENISA's **CyCLONe** framework for cyber crisis coordination
- NATO CCDCOE's **CyCon** tabletop exercise templates
- World Economic Forum's **Global Cybersecurity Outlook** (includes private sector benchmarks)

Internet Core Tools (Part 3)

- RIPE NCC DNS4EU – EU sovereign DNS resolver (https://www.ripe.net/projects/dns4eu)
- ENISA PKI Guidelines – Public Key Infrastructure for sovereignty (https://www.enisa.europa.services/pki)

- BGPStream – Real-time BGP monitoring tool (https://bgpstream.com)

- Censys Certificate Transparency – Monitoring for PKI risks (https://censys.io)
- ICANN Root Zone Management – Governance of DNS root servers (Part 3)
- IETF BGP Specifications – Standards for BGP and routing security (Part 3)
- Matrix.org – Open federated messaging for sovereign comms (details in Appendix A)
- Microsoft Activation Portal – Offline licensing guidance (Part 5)
- IETF MIMI WG – Messaging interoperability standards (details in Appendix A)

AI Sovereignty Tools (Part 4)
- Mistral AI – EU-based sovereign LLM provider (Part 4)
- EU AI Act – Regulation for high-risk AI (Part 4)
- Aleph Alpha – European AI foundation models (Part 4)

AI Sovereignty Tools (Part 4)
- Mistral AI – EU-based sovereign LLM provider (Part 4)
- EU AI Act – Regulation for high-risk AI (Part 4)
- Aleph Alpha – European AI foundation models (Part 4)

Additional Resources from Supplementary Material

- NATO HEIST (https://natoheist.org/)
- Interactive Internet map
- Japan Times – Cloud market concentration analysis (https://japantimes.co.jp)
- Politico EU – Banking and tech dependency reports (https://politico.eu)
- Atlantic Council – U.S. authoritarian shift impacts (https://atlanticcouncil.org)
- European Council on Foreign Relations – Tech sovereignty plans (https://ecfr.eu
- New Scientist2464396-nato-tests-satellite-internet-as-backup-to-sabotaged-undersea-cables/) – NATO satellite backup for cables (https://www.newscientist.com/article/nato-tests-satellite-internet-as-backup-to-sabotaged-undersea-cables/
- Akamai – DNS delivery and security (https://www.akamai.com/solutions/dns-delivery-and-security)
- European Parliament – EU cloud and data studies (https://www.europarl.europa.eu/RegData
- NIST – Supply chain risk management guidelines (https://csrc.nist.gov)
- Gartner – Infrastructure and operations insights (https://gartner.com)
- U.S. Department of Homeland Security – ICT supply chain reports (https://www.dhs.gov/sites/default/files/2022-02/ICT%20Supply%20Chain%20Report_2.
- Merge.dev – API integration tools (https://merge.dev/blog/why-merge-is-more-extensible-than-you-think-a-guide-for-engineers)
