Resilience and Security of Digital Infrastructure
A Policy-Oriented Overview

29 November 2025

White Paper
By
Dr. Georg Serentschy

Table of Contents

1. Foreword

This article marks another step in our ongoing work on the topic of resilience and security of digital systems and is intended as an evaluation of the status quo, a contribution to the discussion, and an invitation to debate. In previous articles, we primarily dealt with various more technically oriented aspects of the topic, while this article focuses mainly on the broader context and policy aspects followed by a call for action.

2. Executive Summary

Digital infrastructure, including subsea and terrestrial cables, mobile networks, data centers, cloud platforms, satellites, and the software and governance layers that enable them to operate, has become a **fundamental utility for society, economies, security, and daily life**. Its resilience is now a central policy issue: governments and industry must be able to anticipate threats, withstand shocks and disruptions of various kinds, adapt to changing conditions, and recover swiftly. Risks are becoming increasingly multidimensional: climate change exacerbates environmental hazards, complex software stacks introduce systemic cyber vulnerabilities, supply chains remain vulnerable, and geopolitical rivalries are weaponizing connectivity and supply chains.

From a policy perspective, **resilience and security of digital infrastructure covers a broader scope than cybersecurity**. It encompasses **engineering design** (redundancy, diversity, and modularity), **organizational preparedness** (including incident response and drills), **governance clarity** (defining roles and responsibilities), and **economic stability** (avoiding single points of economic failure). Modern regulations, such as the EU's NIS2 and the Critical Entities Resilience Directive - CER, or the United States' sector-specific but increasingly strict framework, tend to be risk-based and proportional. They expand the scope of "critical" operators while requiring transparent incident reporting and mitigation plans. However, **measurement remains challenging**: comparable, outcome-focused indicators are scarce, and much of the necessary data is proprietary or classified.

Geopolitics and geo-economics are transforming the digital landscape map. Strategic competition, particularly between the US and China, has prompted the securitization of networks (vendor bans, export controls, tariffs, and investment screening, stricter FDI rules, etc.) and the use of economic statecraft (grants, subsidies, and sanctions) to steer where and how infrastructure is built. This can lead to parallel systems, with the advantage of enhanced resilience (redundancy), but also carries the risk of regulatory fragmentation. Regional dynamics vary: the EU seeks "digital sovereignty" and "strategic autonomy"; China advances the Digital Silk Road; Indo-Pacific and Global South states juggle affordability, development, and great-power pressure. Meanwhile, hyperscalers and telecom giants have become geopolitical actors in their own right; some of them are more powerful than nation states. Their capital expenditure decisions already influence global chokepoints and dependencies.

Policy toolkits are expanding. Governments are combining regulation, standards, investment screening, procurement rules, public financing, industrial policies, international agreements, information-sharing mechanisms, and operational capacities, such as cable-repair fleets and

maritime surveillance. Legal modernization, including streamlined approval procedures, the criminalization of intentional cable damage, and the harmonization of the definition of critical entities, is overdue in many areas. Cross-sector interdependencies, especially those involving energy, telecommunications and logistics, require joint planning and exercises to prevent cascading failures.

The research community is active but fragmented. Key themes include subsea cable security, cyber-physical interdependence, supply chain trust, regulatory comparisons, and resilience metrics. Gaps remain in data access, perspectives from the Global South, the rigorous economics of redundancy, organizational behavior, and the integration of climate science into digital planning. Emerging areas involve AI-enabled resilience, quantum-era security, LEO satellite constellations, and legal or normative frameworks for protecting civilian digital infrastructure during conflicts.

A **forward-looking agenda** should adopt a life-cycle digital ecosystem perspective, invest in strategic yet cost-effective redundancies, modernize legal frameworks, build resilient public–private partnerships, develop enabling capacities and human capital, coordinate internationally while respecting local contexts, incorporate climate adaptation, and test transparent metrics and stress scenarios. Importantly, policymakers must avoid counterproductive securitization by using security rhetoric to justify protectionism, which ultimately weakens resilience.

Resilience and security isn't a goal in itself, but rather an ongoing process of anticipating, adapting, and learning. Making the buzzword into a plan requires ongoing collaboration among governments, policy makers, regulators, operators of critical infrastructure, researchers, and civil society.

3. Introduction: Why Digital Infrastructure Resilience Matters

Digital infrastructures, including submarine cables, terrestrial fiber, and 5G networks, as well as data centers, cloud platforms, Internet exchange points (IXPs), satellites, industrial control systems, and the software stacks that manage them, have become the vital circulatory system of modern economies and societies. Their continuous operation supports everything from essential services like payment systems and logistics to democratic decision-making and military command. However, these infrastructures face growing exposure to complex, overlapping and accumulating risks,[1] including climate shocks, cyberattacks, sabotage, supply chain disruptions, geopolitical competition, economic coercion, criminal activity and regulatory fragmentation.

“Resilience” has therefore **shifted from an engineering afterthought to a core policy goal**. Policymakers now routinely ask: How can we prevent disruptions (robustness), absorb and adapt to shocks (adaptability), and recover quickly (rapidity of restoration)? How do we

[1] See also The Critical National Infrastructure Threat Landscape (Dutch National Coordinator for Counterterrorism and Security): https://english.nctv.nl/documents/publications/2025/11/14/the-critical-national-infrastructure-threat-landscape

balance openness with security, efficiency with redundancy, cost with sovereignty, and innovation with regulation? And how are geopolitics and geo-economics reshaping the choices states and firms make about where to build, operate, and govern digital networks?

This paper provides a **general overview of the resilience and security of digital infrastructure from a policy perspective**. It highlights the role of geopolitics and geo-economics, surveys the current research landscape, and sketches an agenda for future research and action.

4. Defining Digital Infrastructure – Resilience and Security

4.1. Elements of the digital infrastructure

A policy-relevant definition of digital infrastructure includes several layers. The **physical connectivity layer** features undersea and terrestrial fiber-optic cables, microwave links, satellite constellations, mobile and fixed wireless networks, IXPs, and last-mile access networks. The **compute and storage layer** consists of data centers, cloud and edge computing nodes, content delivery networks, and high-performance computing facilities. The **control and service layer** covers the DNS and routing infrastructure, certificate authorities, software supply chains, network management systems, and essential platform services such as identity, payments, application programming interfaces, and AI inference. Lastly, the **operational and energy layer** involves power supply, cooling systems, diesel reserves, and alternative energy sources for emergencies, along with the logistics and workforce needed to maintain and repair assets.

4.2. Resilience and security as a multi-dimensional concept

Resilience goes far beyond cybersecurity. It requires a comprehensive lifecycle view that covers planning, investment, construction, operation, maintenance, protection, repair, and decommissioning. It also spans technical, organizational, legal, and economic areas, with weaknesses in any part capable of spreading throughout the ecosystem. Standard policy definitions identify four interconnected dimensions. **Anticipation and prevention** involve risk awareness, threat modeling, and design choices, such as route diversity and secure-by-design software, that reduce the likelihood or impact of disruptions. **Absorption or resilience capacity** means maintaining core functions during disruptions, such as rerouting traffic or allowing services to degrade in stages. **Adaptation and transformation** focus on learning from incidents and modifying architectures, processes, and regulations, such as adopting zero-trust models or diversifying supplier networks. **Recovery and restoration** relate to how quickly and effectively systems return to normal or acceptable service levels, as demonstrated by the mean time to repair a cable fault or execute data center disaster recovery plans.

5. Risk Landscape: Multi-Domain, Interdependent, and Escalating

Digital infrastructures face routine and non-routine risks from natural, accidental, and malicious sources. **Environmental and climate risks** include storms, floods, heatwaves, wildfires, earthquakes, volcanic eruptions, and seabed landslides, all of which are becoming

more frequent and severe as climate change advances. Higher temperatures and extreme weather also stress power grids supplying data centers and base stations. **Accidental human activities**, such as fishing trawls and purposeful cable sabotage with ship anchors, dressed up as an accident or oversight, construction mishaps damaging terrestrial fiber, or software misconfigurations causing outages through BGP leaks or route hijacks, are taking place every day. **Cyber threats** include i.a. ransomware attacks on critical service providers, exploitation of zero-day vulnerabilities in widely used software, supply-chain breaches, distributed denial-of-service attacks on DNS, IXPs, or cloud providers, as well as insider threats and credential theft. **Physical sabotage and espionage** are also present, with deliberate cable cuts, arson attacks, tampering with landing stations, intrusions into network management systems, and tapping fiber pairs. **Supply-chain and market shocks** result from shortages of semiconductors, optical amplifiers, or cable ships; from sanctions and export controls; from vendor insolvencies; and the monopolization of routing or cloud capacity by a few entities. **Regulatory and legal risks** arise from overlapping or conflicting permit regimes for cable repair, data localization laws that restrict flexible rerouting, extraterritorial sanctions, and inconsistent classifications of "critical infrastructure," which may lead to overregulation or under-regulation of assets.

Because interdependencies enable localized shocks to have global impacts, resilience must be addressed systemically rather than in isolated sectors. Think of examples like a volcanic eruption severing a nation's only subsea link, a vulnerability in a widely used software threatening thousands of services, or a cloud region failure cascading into payment and transport systems.

6. Policy Lenses on Resilience and Security

6.1. From cybersecurity to socio-technical resilience (infrastructure provider angle)

Initial policy debates focused narrowly on protection from hackers, but contemporary approaches are more holistic, **integrating engineering resilience** through redundancy, diversity, and modularity; organizational resilience through incident response, business continuity, and cross-sector exercises; **governance resilience** through clear roles, legal clarity, and international coordination; and **economic resilience** by ensuring competitive markets and avoiding single points of commercial failure.

6.2. Risk-based regulation and proportionality (regulatory authority angle)

Regulators are increasingly requiring risk assessments and proportional safeguards, recognizing that not all assets are equally important. European frameworks, such as NIS2, the Critical Entities Resilience Directive, and DORA for financial ICT (which sets out rules that can be applied mutatis mutandis to areas outside the financial sector), along with US sectoral directives like TSA pipeline security and FCC supply-chain rules, demonstrate this trend. The challenge is to establish obligations that are stringent enough to be meaningful yet flexible enough to adapt to evolving threats.

6.3. Whole-of-government and public–private collaboration (holistic angle)

No single vertical silo, such as a ministry or regulator can cover the full stack alone. Therefore **effective policy blends strategic direction**, through national digital strategies, industrial policies, and geo-economic instruments, with **operational coordination** via cyber emergency response teams and information sharing and analysis centers. Evidently, **economic tools** that include subsidies, tax incentives, procurement rules and export controls also have their place in the policy mix.

6.4. Measurement and accountability

To be governable, resilience must be measurable. Policymakers therefore experiment with indicators such as the mean time required to restore service, the diversity of cable routes, the proportion of traffic routed domestically versus internationally, the degree of dependency on single suppliers, or compliance scores with security frameworks. Harmonized metrics remain elusive, however, which hampers cross-border benchmarking.

7. Geopolitics, Geo-economics, and the Rewiring of Connectivity

7.1. Securitization of digital infrastructure

As strategic competition intensifies, particularly between the US and China, digital infrastructure has developed into a national security asset. Policymakers invoke existential language (“critical arteries,” “battlefields of data”) to justify extraordinary measures: investment screening, vendor bans, sanctions, state-backed cable or satellite projects, and alliances to build “trusted” networks.

7.2. Geo-economic statecraft

Governments utilize economic tools to achieve their strategic digital infrastructure objectives. **Positive tools (incentives)** include grants, concessional loans, development aid, and tax credits, which aim to influence cable routes or data center placements, as well as public procurement that impacts supply chains and promotes joint ventures or multilateral funds. **Negative tools (disincentives)** include export controls on advanced chips, so-called entity listings, tariffs, investment restrictions, like those used by CFIUS and EU-style FDI screening, and secondary sanctions that pressure groups to exclude certain vendors. These measures may lead to **fragmentation risks**: uneconomic parallel physical infrastructure that does not create useful redundancy, split 5G ecosystems, localized cloud regions driven by sovereignty concerns, and differing technical standards. While fragmentation can enhance security for some, it can also decrease global redundancy and efficiency. Therefore, a trade-off always exists between various factors such as physical versus logical redundancy and regional versus global security. Efficiency considerations also influence outcomes, depending on the observer's perspective.

7.3. Regional dynamics

Regional strategies vary widely. The **European Union** aims to balance "Strategic Autonomy" with market integration; NIS2 and the CER Directive expand obligations to a broader range of operators. The EU Chips Act, Cloud and Edge computing Rulebook, and the Cyber Resilience Act (CRA) address both hardware and software supply chains. Enforcement of the Digital Markets Act (DMA) is used as a buffer against the influence of the hyperscalers. Brussels also tests foreign subsidies regulation and anti-coercion tools to protect firms from extraterritorial pressure.

"**Digital Sovereignty**" is now high on the agenda of EU policymakers, and **EuroStack** is a vital initiative to make it a reality. The **United States** adopts a sector-specific but increasingly coordinated approach, utilizing tools such as CISA's National Infrastructure Protection Plan, executive orders on supply chains, and the Department of Justice's "*Team Telecom*"[2] reviews for cable licenses. Washington deploys export restrictions in sensitive sectors such as advanced semiconductors and AI chips, promotes "Clean Network" initiatives, and builds alliances in the Indo-Pacific.

China advances the **Digital Silk Road**, its tech arm of the Belt and Road initiative, through state-backed cable and data center projects, seeks dominance in fiber-optic and 5G markets, promotes alternative internet governance norms, and enforces data localization laws emphasizing sovereignty.

Many **Indo-Pacific and Global South nations** prioritize connectivity and affordability over great-power narratives but are increasingly compelled to select vendors and financiers amid competing offers. Organizations such as ASEAN, the Pacific Islands Forum, and the African Union strive to strike a balance between development and security without falling into dependency traps.

Russia and others, including their proxies, have increased NATO and EU focus on subsea surveillance and protection, using hybrid tactics to target European energy and telecom infrastructure., Meanwhile, Gulf states and India are pursuing strategic data center hubs to position themselves as "digital chokepoint" managers.

7.4. Corporate geopolitics

Large technology companies, including Amazon, Google, Microsoft, Meta, and NVIDIA along with major telecom operators and equipment vendors, have become important geopolitical players and investors in privately-owned digital infrastructure. The same applies to players in the satellite sector like Starlink and the new player Amazon Leo (formerly known as Kuiper). Their investments increasingly shape global connectivity, and their leverage to lobby governments for policies favoring their businesses grows proportionaly. Their proprietary risk

[2] "Team Telecom"-style approvals, stands for **any pre-licensing, interagency national-security review that vets who can land/operate a cable, imposes mitigation conditions, and retains authority to revisit or revoke the license later,** a template other jurisdiction could emulate or adapt.

models, incident data, and architectures make public oversight more complicated, nevertheless they remain vital to resilience efforts.

8. Digital Sovereignty and „Likeminded-Ness"

8.1. Digital Sovereignty

Triggered by geopolitical developments, such as the increasingly unpredictable positioning of the US, there are currently increased efforts in Europe and other parts of the world (e.g., Canada) to strengthen digital sovereignty. However, this vague term allows for too many interpretations and requires thorough discussion to avoid ambiguities and enable its putting into action. In our view, "Digital Sovereignty" is a multidimensional concept that goes beyond mere technological independence. Under a realistic scenario, where full self-sufficiency (autarky) is neither feasible nor desirable, **digital sovereignty could be understood as controlled digital interdependence**. This means securing critical capabilities, reducing vulnerabilities, and retaining the ability to set and enforce rules in key areas, while still benefiting from global collaboration. In other words, a concept with the following characteristics:

- **Control over critical infrastructure** (e.g., networks, data centers, technology stack, cloud).
- **Resilience in supply chains** (e.g., semiconductors, raw materials).
- **Policy and regulatory autonomy** (e.g., data protection, AI ethics, competition rules).
- **Innovation leadership in strategic domains** (e.g., AI, quantum, green tech).
- **Trusted partnerships** with like-minded countries to avoid over-reliance on adversarial powers.
- **Dynamic and adaptive**: Sovereignty must evolve with technological and geopolitical shifts (e.g., AI, quantum, semiconductors). Alliances can weaken; friends can become opponents (Example current US administration).
- **Digital sovereignty is not isolationism**: Europe (or any region in a similar situation) cannot and should not aim to replace all foreign technologies. Instead, sovereignty is about reducing critical dependencies, ensuring policy control, and fostering domestic innovation in areas that matter most.
- **It is not just about technology**: It includes legal, economic, geopolitical, and industrial dimensions.

8.2. Likeminded-Ness

The term **"like-minded" in the context of digital sovereignty, geopolitics, and technology partnerships** refers to countries or entities that share core values, strategic interests, and policy goals, particularly around democracy, human rights, rule of law, open markets, and technological resilience. However, the definition is nuanced and depends on the specific domain (e.g., security, trade, or innovation).

"Like-minded" means **a spectrum of like-mindedness, it is not a binary** concept Europe must prioritize partnerships based on shared goals (e.g., democratic tech governance) while accepting tactical divergences (e.g., data localization, Chinese vendors ban). The key is to build coalitions that are flexible, resilient, and values-driven. Core characteristics of like-mindedness can be described as follows:

8.2.1. Shared Values

- Democratic governance: Commitment to free elections, transparency, checks and balances, and accountability.
- Human rights and rule of law: Respect for privacy, freedom of expression, and ethical use of technology (e.g., no mass surveillance).
- Open and fair markets: Support for competition, anti-monopoly policies, and interoperability (e.g., opposing coercive tech standards).

8.2.2. Strategic Alignment

- Geopolitical goals: Opposition to authoritarian tech dominance (e.g., China's digital authoritarianism, espionage and cyber activities, Russia's espionage, hybrid and cyber aggression).
- Economic resilience: Shared interest in reducing over-dependence on adversarial powers (e.g., China for rare earths, US for cloud/AI).
- Security cooperation: Collaboration on cybersecurity, critical infrastructure protection, and defense tech (e.g., NATO's focus on emerging tech).

8.2.3. Technological and Industrial Synergies

- Complementary strengths: Partners bring unique capabilities (e.g., US in AI, Japan in robotics, EU in regulation, India in IT services).
- Interoperability: Commitment to open standards (e.g., Open RAN for 5G, GDPR-like data protection).
- Innovation collaboration: Joint R&D in quantum, AI, and green tech (e.g., Horizon Europe, US CHIPS Act partnerships).

8.2.4. Rule-Setting and Governance

- Multilateral standards: Working together to shape global rules (e.g., AI ethics, digital taxes, cross-border data flows).
- Regulatory convergence: Aligning on data protection, competition policy, and export controls (e.g., EU-US Data Privacy Framework).
- Countering coercive practices: Pushback against forced technology transfer, IP theft, and market distortions.

From the above it becomes clear that **not all "like-minded" partners align perfectly**. Differences exist in areas like data localization, use of Chinese equipment/vendors, AI regulation and rules, semiconductor subsidies, export controls, etc.

To sum up, **digital sovereignty is not about cutting ties; it's about having leverage**. Europe must play to its strengths (overall size of the marketplace, regulation, industrial base, talent)

while reducing asymmetrical dependencies. The **concept of "likeminded-ness"** needs dynamic interpretation and pragmatism. Further research is needed in this area to avoid unnecessary ambiguity and to specify the necessary action to be taken.

9. Policy Toolkits: What Governments Can and Do Use

Governments now rely on a wide range of tools. Regulatory mandates and standards impose **security-by-design obligations** and **incident reporting requirements**, as seen in NIS2 or US Securities and Exchange Commission cyber disclosure rules. They also establish **certification schemes for cloud services or 5G vendors** and can require **mandatory redundancy**, such as dual homing for critical services. Investment screening and procurement rules subject foreign direct investment to review and apply "*Team Telecom*" style approvals to cable landings. Trusted vendor lists and supply-chain transparency mandates aim to manage risk. **Public financing and industrial policies** provide grants for rural fiber deployments, satellites for remote regions, and state-backed cable ships, along with tax incentives to improve data center energy efficiency or attract such facilities to specific economic areas.

International agreements and alliances, including the Quad Cable Partnership and the EU–US Trade and Technology Council (TTC), offer coordination platforms. Additional obligations and efforts to modernize subsea cable protections shape maritime conduct. Take updating or supplementing the 1982 *UN Convention on the Law of the Sea* (UNCLOS) so it fits today's reliance on submarine fiber networks and the threat landscape they face.

Mutual assistance pacts for cyber incidents, such as those under NATO or the EU Cyber Solidarity Act, further strengthen cooperation. **Information sharing and exercises** are formalized through sector-specific ISACs, joint tabletop exercises, cross-border incident drills, and both classified and unclassified threat intelligence frameworks. **Operational capabilities** include national cyber incident response teams (CSIRTs), security operation centers (SOCs), enhanced maritime domain awareness and surveillance of critical seabed corridors, and strategic stockpiles of spare cables, repeaters, or transformers supported by chartered repair vessels.

Legal modernization criminalizes deliberate cable damage (including gross negligence), streamlines repair permit processes, and harmonizes definitions of critical entities to prevent regulatory arbitrage. **Market-shaping measures** utilize competition policy to avoid concentration in routing or cloud services, while supporting open standards and interoperable architectures, such as OpenRAN or open cloud APIs, to reduce vendor lock-in.

10. Measuring and Managing Resilience: Metrics and Methods

Because resilience metrics often rely on proprietary information held by private operators, **policymakers face a persistent data dilemma**. Despite this, several measurement approaches are gaining popularity. **Structural metrics** evaluate the number of independent cable routes into a country, the proportion of critical traffic that can be rerouted domestically, and the diversity of cloud regions. **Process metrics** measure the time needed to detect and contain incidents, the frequency of red-team exercises, and compliance rates with patching and vulnerability disclosure deadlines. **Outcome metrics** focus on the annual downtime of critical

services, the economic losses caused by disruptions, and the recovery time following physical damage. **Maturity models**, such as the Department of Energy's C2M2 for the energy sector or profiles based on NIST's Cybersecurity Framework, are being adapted for telecom and data center operators. **Advanced modeling**, including agent-based simulations, stress tests, and digital twins of national networks, enables policymakers to explore scenarios such as simultaneous cable cuts combined with a cloud region outage, allowing for informed investment decisions. However, such modeling often requires secure data-sharing agreements and legal safe harbors to prevent transparency from leading to liability or reputational harm.

11. Cross-Sector Interdependencies and Cascading Failures

The functioning of modern, digitally controlled energy networks (with a growing share of renewable energies), just-in-time logistics and transport, and the financial sector depends on a resilient and secure digital infrastructure. Policies should promote joint planning, shared drills, and interoperable emergency communication protocols (e.g., satellite backups) to prevent cascading failures and crises; therefore, **power supply strategies**, including microgrids, on-site renewables, new energy resources, such as Virtual Power Plants (VPPs), and fuel supplies, are essential components of resilience planning. **Logistics and workforce** limitations are equally critical, as repairing a cable or replacing a transformer requires spare parts, specialized ships, visas for technicians, and safe access to contested waters. Pandemic-era border closures revealed these vulnerabilities and provided valuable lessons. The **financial system depends on low-latency connections** and synchronized time sources for real-time gross settlement, card networks, and high-frequency trading, and outages can have significant macroeconomic impacts. Consequently, policy must promote joint planning across sectors, combined exercises, and interoperable emergency communication protocols, including satellite backups, to prevent cascading crises.

12. Current Research Landscape: Trends, Gaps, and Debates

12.1. Focus areas in the literature

The **role of geopolitics and geo-economics** is underscored by the fact that 95% of all global data traffic traveling through submarine cables is deeply connected to geopolitics, as are vendor choices, operational factors, and security concerns. A growing body of research considers **subsea cables as critical infrastructure** by analyzing risks, legal gaps, and geoeconomic competition, while advocating for comprehensive life-cycle approaches to licensing, maintenance, and repair. Scholars examine **cyber-physical interdependence** to understand how software vulnerabilities spread through physical networks and vice versa. **Supply-chain security** research evaluates trust in vendors, the use of software bills of materials, the security of open-source components, the concentration of chip manufacturing, and the effects of export controls. Studies on **regulatory effectiveness** compare NIS2 with US sector-specific models, explore how critical infrastructure designations influence operators, and assess the effectiveness of public–private partnerships. Debates about **fragmentation versus resilience** investigate whether split networks and digital sovereignty lower risk or

instead weaken global redundancy and interoperability. Finally, methodologically focused work aims to develop **resilience indicators**, perform stress testing, and create scenario-planning tools.

12.2. Persistent gaps in research activities

Despite this activity, significant gaps still exist. **Researchers often lack access to real incident data and infrastructure maps** due to commercial secrecy and national security classifications. **Perspectives from the Global South remain underrepresented** compared to those from the US and EU, despite small island states, African nations, and landlocked countries facing unique connectivity challenges. **Rigorous economic models of redundancy**, such as the use of additional physical cable (or logical) connections, diverse routes, or multi-cloud strategies, are still relatively uncommon. Human factors and organizational culture receive insufficient attention, despite the strong influence of decision-making incentives and institutional path dependencies on resilience investments.

Additionally, few models fully incorporate **climate risk projections** into digital infrastructure planning, beyond basic flood mapping. Finally, it should not be overlooked that **redundancy and resilience are costly**. This raises the question: **who will bear the extra costs associated with higher resilience,** taxpayers, industry, or users? Or all of them? Do we have an evidence-based key for splitting the costs?

12.3. Emerging research directions

The telecom industry is undergoing structural change as traditional connectivity-based revenues stagnate while capital needs for 5G/6G and fiber expansion rise. The entire telecom ecosystem is characterized by geopolitical challenges, disrupted supply chains, new resilience and security requirements, and evolving customer demands. Besides mitigating specific threat components, operators are pivoting toward becoming technology companies, integrating AI, quantum technologies, and cloud services to improve efficiency, cybersecurity, and infrastructure security and resilience.

Several promising directions are emerging. **AI and automation can bolster resilience** by supporting anomaly detection, predictive maintenance, and even autonomous repair through uncrewed underwater vehicles. However, heavy reliance on large AI models creates new single points of failure. **Quantum communication & cryptography, quantum sensing, and quantum computing** will revolutionize secure connections, network security and maintain long-term confidentiality. **Space-based infrastructure, especially LEO satellite constellations**, can improve resilience by offering backup links, but they also become new targets and generate debris risks. **Legal harmonization and norm-building efforts** aim to modernize UNCLOS for cables, accelerate permits for emergency repairs, and develop norms against targeting civilian digital infrastructure during conflicts.

The **intersection of quantum technologies and telecommunications is becoming increasingly strategic**, driven by both the transformative potential of quantum innovations and the evolving demands of the digital economy. Leading telecom firms globally are actively engaging with quantum technologies through acquisitions, partnerships (cooperations), internal

capacity and knowledge building, and integration with other in-house technologies by building an integrated technology stack.

12.4. Quantum application fields in a nutshell

12.4.1. Quantum-Safe Cryptography

- **Post-Quantum Threat**: Quantum computers threaten to break widely used encryption algorithms (like RSA and ECC), which secure everything from online banking, energy, logistics to military communications.
- **Proactive Security**: Telecoms are investing in quantum-resistant cryptography to future-proof their networks and protect customer data from future quantum attacks.
- **Regulatory Pressure**: Governments and industries are pushing for standards in post-quantum cryptography, making early adoption a competitive advantage.

12.4.2. Quantum Key Distribution (QKD)

- **Unbreakable Encryption**: QKD uses quantum principles to create theoretically unhackable communication channels.
- **Network Integration**: Telecoms are testing QKD in fiber-optic and satellite networks to offer ultra-secure services for governments, finance, and healthcare.
- **Market Differentiation**: Offering QKD-enabled services can attract high-value clients concerned about data integrity and security.

12.4.3. Quantum PNT (positioning, navigation and timing)

- **Quantum sensors** can provide **positioning, navigation and timing** information in environments where GPS (and similar satellite-based) signals are unavailable or unreliable, for example because of jamming and spoofing.
- Such sensors include **quantum accelerometers and gyroscopes, quantum magnetometers, and gravimeters and gravity gradiometers** as described in a topical report.
- Many **quantum sensors offer levels of precision not possible with traditional approaches** for measuring physical quantities such as time, acceleration, and magnetic fields. Furthermore, networks of quantum sensors can provide additional reliability and accuracy in the collection of PNT information.

12.4.4. Quantum Computing for Optimization

- **Network Efficiency**: Quantum algorithms can optimize routing, spectrum allocation, and traffic management in real time, reducing latency and costs.
- **AI and Big Data**: Quantum machine learning could enhance predictive maintenance, fraud detection, and customer analytics.
- **Competitive Edge**: Early adopters will gain operational efficiencies and new revenue streams from quantum-enhanced services.

12.4.5. Quantum Sensors for Infrastructure

- **Precision Monitoring**: Quantum sensors can detect minute changes in temperature, magnetic fields, or vibrations, improving the maintenance of cables, data centers, and cell towers. **Allows to detect and locate damages or acts of sabotage.**
- **Environmental IoT applications**: wildfire detection, enhanced smart agri, e-health applications.

12.4.6. Strategic Acquisitions and Talent

- **Access to IP**: Acquiring quantum startups gives telecoms access to patents, prototypes, and specialized talent.
- **Speed to Market**: Building quantum capabilities in-house is slow; acquisitions accelerate R&D and deployment.
- **Ecosystem Leadership**: Telecoms aim to shape industry standards and partnerships by controlling key quantum assets.

13. Policy Recommendations: Building Durable, Adaptive Resilience

Policy action should advance on several fronts. **First,** authorities need to adopt **a life-cycle, ecosystem view** by integrating resilience requirements from planning to decommissioning and by harmonizing maritime, telecom, cyber, energy, and competition policies to ensure consistent governance.

Second, diversification must be pursued strategically. Multi-path connectivity, such as maintaining at least two diverse routes for each critical service, and multi-cloud or hybrid strategies for public services, can reduce risk. However, redundancy costs should be weighed against exposure through clear cost–benefit analyses.

Third, legal and regulatory frameworks require updating, including streamlined permits for cable laying and repairs, criminal penalties for intentional damage, and clarified procedures in the Exclusive Economic Zone; critical infrastructure lists and obligations should be reviewed regularly to prevent static, one-size-fits-all rules, and incident reporting should be mandatory with safe harbors to foster transparency.

Fourth, public–private partnerships and information exchange must be strengthened by institutionalizing joint exercises, red teaming, and cross-sector drills; creating secure data enclaves for sharing sensitive topology and incident information for research and modeling; and aligning incentives through tools like resilience bonds and cyber insurance that reward best practices.

Fifth, governments should invest in capacity building by expanding the fleet of modern cable-laying and repair vessels, stockpiling critical spares, and funding research into predictive maintenance, self-healing networks, quantum sensing, and sustainable data center

technologies; they must also cultivate human capital in fields ranging from maritime law to cyber forensics.

Sixth, international coordination should progress without ignoring local circumstances. Regional forums can align standards and share resources, for example, through the repair coordination centers, while development finance packages should prioritize affordability and security for underserved regions. Diplomatic efforts should also promote norms against targeting civilian digital infrastructure.

Seventh, climate adaptation must be integrated into digital resilience planning by mapping future hazard zones such as sea level rise and extreme heat, areas increasingly at risk of flooding and landslides, etc., and relocating or reinforcing assets as necessary. Energy efficiency and alternative cooling methods can help reduce the strain on power grids.

Eighth, governments and operators should develop and evaluate metrics by piloting national resilience dashboards that monitor key indicators and conducting periodic stress tests like those used in banking.

Finally, policymakers should avoid counterproductive securitization by ensuring that designating assets as critical provides resources and adaptive governance rather than just restrictions, and by resisting the use of security rhetoric to justify protectionism that undermines diversity and resilience.

Finally, we emphasize that comprehensive strategies and well-thought-out policies are a necessary but not sufficient prerequisite for successful resilience and security policy. **Implementation in political and corporate action** is, so to speak, the **capstone in the architecture of such a policy**.

14. Research and Policy Agenda

Universities, think tanks, standards bodies, and operators should form consortia to develop open datasets, interoperable tools, and policy playbooks, ideally supported by multilateral funding (such as insurers like Munich Re or Swiss Re, the World Bank, or regional development banks) to include low- and middle-income countries. A collaborative agenda is essential. Stakeholders should collaborate on **shared taxonomies and data standards** for incident reporting and infrastructure mapping, and develop **open, privacy-preserving modeling platforms**, such as federated learning environments, to simulate cross-border disruptions without exposing sensitive data. **Comparative legal studies** can identify best practices in repair permitting, liability frameworks, and public financing instruments. **Economic research** should quantify the value of redundancy and determine optimal investment levels for different contexts. **Socio-political analyses** can clarify how narratives contrasting security and development influence infrastructure choices across regions. **Ethical frameworks** are needed to balance the prevention of surveillance with legitimate security monitoring at landing stations and IXPs. **Finally, research at the climate–digital nexus** must integrate IPCC scenarios, World Economic Forum risk forecasts, and similar datasets into network planning while

assessing the carbon footprint of resilience strategies. Universities, think tanks, standards bodies, and operators should form consortia to produce open datasets, interoperable tools, and policy playbooks, ideally supported by multilateral funding from organizations such as the World Bank and regional development banks to ensure low- and middle-income countries are included.

15. Conclusion: From Buzzword to Action

Resilience has become a common policy buzzword, but building truly resilient digital infrastructures requires more than just slogans. It involves an encompassing holistic approach, creating and implementing resilience-promoting policies, providing proper governmental support, mobilizing adequate financial means, i.a. to realize technical redundancy, enhancing institutional agility and flexibility, diversification of suppliers, introducing compatible standards, ensuring public oversight, engaging private expertise, and lastly, realizing strategic independence and global collaboration. **Geopolitics and geo-economics** will continue to influence **who builds and controls the world's central nervous system**. Policymakers must understand these factors and integrate them in their strategies without letting them undermine the resilience they seek to strengthen.

Ultimately, resilience is not a fixed end state, but an ongoing practice of anticipation, adaptation, learning and implementation. The outline presented here covers life cycle governance, redundancy measures, legal updates, strengthened partnerships, climate integration, and strict metrics, thereby providing a blueprint for implementing these policies in political and business practice.

16. Acknowledments

We thank our interviewees from the regulatory community, the security apparatus, policy experts and relevant individuals from industry and academic security experts for their inspiring and insightful insights. Special thanks goes to our **WeltWert®-Insights** partners **Derk Oldenburg** and **Paul Timmers** for assisting us with sounding-board discussions and, who played a key role with many valuable discussions, critical feedback and important contributions.

17. References

17.1. Key Policy and Legal Instruments

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).
Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive).
Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA).
Regulation (EU) 2023/1781 establishing a framework of measures for strengthening Europe's semiconductor ecosystem (EU Chips Act).
Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), COM(2022) 454 final, and subsequent trilogue agreement (2024).
United States, National Cybersecurity Strategy (2023) and Implementation Plan (2023), The White House.
Executive Order 14017, "America's Supply Chains" (24 February 2021).
U.S. Department of Homeland Security & CISA, National Infrastructure Protection Plan (2013, updated guidance 2016).
United Nations Convention on the Law of the Sea (UNCLOS), 1982 — provisions on submarine cables (Arts. 112–115) and related state obligations.
NATO, "Strengthening the Protection of Critical Undersea Infrastructure" (various communiqués and 2023/2024 reports).

17.2. Standards, Frameworks, and Guidance

National Institute of Standards and Technology (NIST), Cybersecurity Framework 2.0 (2024).
U.S. Department of Energy, Cybersecurity Capability Maturity Model (C2M2) v2.1 (2022).
European Union Agency for Cybersecurity (ENISA), "Good Practices for the Security of Submarine Cables" (2020) and subsequent resilience reports.
OECD, "The Resilience of Communication Networks" (2021).
International Telecommunication Union (ITU): Various recommendations on network resilience and submarine cable protection.
Internet Society, "Undersea Cables and the Future of the Internet" (2021) and related resilience analyses.

17.3. Academic and Think-Tank Literature

Govella, K. M. (2025). Undersea Cables, Geoeconomics, and Security in the Indo-Pacific.
Bria, F., Timmers, P., Gernone F., Renda, A., Fischer C., Grabova, O. EuroStack – A European alternative for digital sovereignty (2025)
Serentschy, G. (2024). Digital Infrastructure Resilience and Security (EU version).
Burnett, D. R., Beckman, R., & Davenport, T. M. (eds.) (2014). Submarine Cables: The Handbook of Law and Policy. Martinus Nijhoff.

Cowhey, P., Aronson, J. D., & Richards, J. E. (2021). Digital DNA: Disruption and the Challenges for Global Governance. Oxford University Press.
De Ridder, S. (2021). “The Politics of Internet Interconnection: Resilience, Power, and Control.” Telecommunications Policy, 45(6).
Maurer, T. (2018). Cyber Mercenaries: The State, Hackers, and Power. Cambridge University Press. (On state–private interplay in cyber operations.)
Livingston, S. (2020). “The Vulnerable Backbone: Policy Options for Securing Submarine Cables.” Journal of Cyber Policy.
Bendiek, A., & Schulze, M. (2021). “EU Cyber Diplomacy: Enlargement of Scope, Diminishing Returns?” SWP Research Paper.
Farrell, H., & Newman, A. (2019). “Weaponized Interdependence: How Global Economic Networks Shape State Coercion.” International Security, 44(1).
Nye, J. S. (2022). “Power and Interdependence in the Digital Age.” International Affairs, 98(6).
Robles, A. (2023). “Cable Chokepoints and the Indo-Pacific Digital Order.” Asia Policy, 18(2).
Kuerbis, B., & Mueller, M. (2020). “Internet Routing Security: Governance Challenges and Policy Options.” Journal of Cyber Policy.
IPCC, AR6 Working Group II Report: Impacts, Adaptation and Vulnerability (2022), Climate Risk context for Infrastructure Planning.

17.4. Industry and Operator Reports

Google, Meta, and Microsoft annual infrastructure investment disclosures (various years).
TeleGeography, Submarine Cable Map and annual Global Bandwidth Research Service (ongoing).
Uptime Institute, Global Data Center Survey (annual), outage statistics and resilience practices.
Cloud Security Alliance, “The State of Cloud Security Resilience” (2023).

=== End of Document ===

