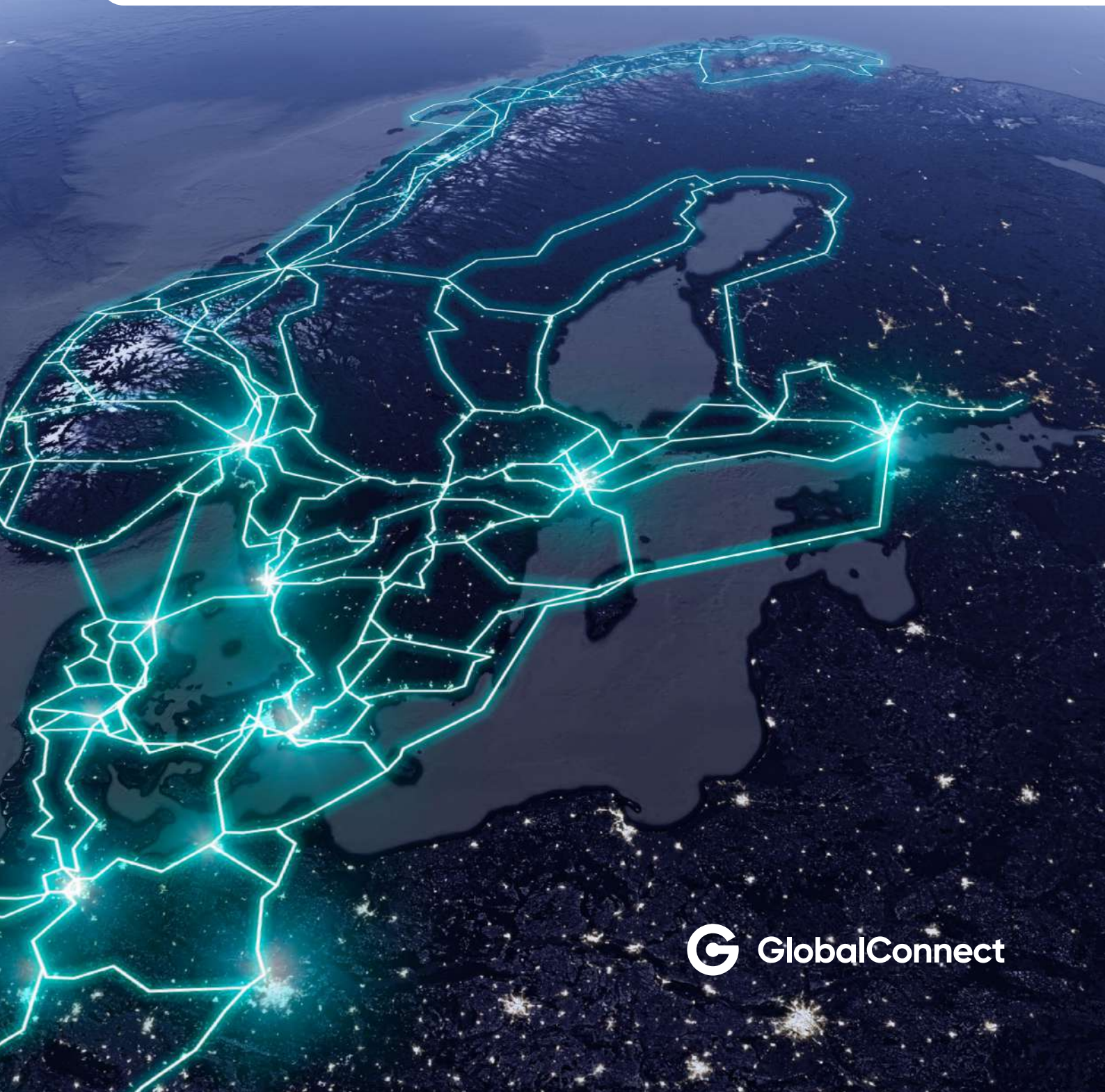
October 2025

Digital Resilience

Securing Norway's Digital Infrastructure Amid Growing Uncertainty and Geopolitical Risks



GlobalConnect

Contents

Foreword

As digital systems increasingly underpin our economy and society, their resilience has become essential. Norway is a digital frontrunner—but with that position come growing risks and responsibilities.

This whitepaper, developed by GlobalConnect, outlines how we can strengthen Norway's digital infrastructure to withstand shocks, ensure continuity, and lead in secure connectivity. Our aim is to foster shared action—across sectors and borders—before a real crisis tests us.

Best regards,

Martin Lippert
Group CEO

Per Morten Torvildsen
EVP NetCo

Sofia Lisa Dinesen
SVP Group Strategy and M&A, Sustainability, Communications and Public Affairs

Preface

In the Nordic countries, digital infrastructure has become a critical enabler of national growth, societal wellbeing, and the delivery of public services. High-speed fiber networks, data centers, mobile broadband, and international transit routes have become the digital arteries of modern society—just as essential as roads, clean water, or electricity. These networks power economic activity, enable communication, and keep public services running. As the Nordic countries continue to lead Europe in digital maturity, they must address growing expectations—and growing risks.

This whitepaper, developed by GlobalConnect, analyzes digital infrastructure in Norway and its broader role in the Nordic geography. It examines the operating capacity of the fiber networks, long-haul corridors, mobile systems, and data centers that support its digital economy. It also examines the resilience of these systems to withstand shocks, adapt to stress, and remain secure over time.

This whitepaper is divided into four chapters with these objectives:

01

To map the current state of Norway's digital infrastructure, including its fiber coverage, long-haul connectivity, mobile infrastructure and the potential for data center expansion.

02

To articulate the economic and societal value this infrastructure enables, including improved productivity, innovation, education, healthcare, and emergency response.

03

To assess the strengths and weakness of Norway's digital infrastructure through three lost-connectivity scenarios—and their likely consequences for the economy and society.

04

To identify mitigating actions already in place, remaining vulnerabilities, and forward-looking actions that can further strengthen the nation's resilience and readiness across the digital infrastructure value chain.

The analysis draws on infrastructure data, policy frameworks, real-world case studies, and insights from both operators and public-private initiatives to improve resilience. While Norway's geography, governance, and the maturity of its infrastructure are unique, it shares a common goal with its Nordics neighbors: to ensure that its digital infrastructure remains a source of national strength and an engine of growth—even under pressure.

Executive Summary

Norway stands out as one of Europe's **most digitally advanced societies**, with a digital infrastructure network that spans mountains, fjords, and Arctic communities. The country has near-universal access to high-speed internet and a resilient, green-powered network that links remote settlements and global data routes alike. **Norway's digital infrastructure has become essential to the functioning of society.** It underpins government services, energy flows, financial transactions, healthcare, and daily life. The country benefits from high digital maturity, a population that embraces digital services, and a broad commitment to cybersecurity across public and private sectors.

But **this progress masks underlying structural vulnerabilities**. Norway's geography—characterized by dispersed communities, mountainous terrain, and long fiber corridors—creates unique challenges for connectivity and redundancy. Meanwhile, **critical services increasingly rely on hyperscalers and international cloud platforms** hosted outside of Norwegian jurisdiction. Sectoral preparedness exists, but it is not enough to prevent cascading failure in the event of a systemic digital disruption.

The whitepaper's simulated outage scenarios **reveal that fallback systems degrade quickly**. Within hours, coordination across transport, healthcare, finance, and emergency services begins to fail. Within days, trust in digital services and institutional response erodes. The risks are not theoretical—they are visible today in the form of growing cyber threats, subsea cable sabotage, and cross-border dependencies.

The whitepaper outlines thee scenarios ranging from a few hours outage to a prolonged one:

Scenario 1 models a four-hour connectivity loss impacting one region and involving multiple operators simultaneously, with potential roots in control layer failures or cyberattacks
Scenario 2 reflects a prolonged 8– to 16-hour regional wide connectivity loss—consistent with a coordinated act of sabotage or systemic collapse.
Scenario 3 models a multi-day multi-regional wide connectivity loss, representing a critical infrastructure crisis triggered by compounded cyber-physical attacks or escalation during geopolitical conflict.

To meet this challenge, **Norway must move from a fragmented and distributed preparedness to integrated digital resilience**—anchored in national security strategy, operational coordination, and regional cooperation.

This whitepaper proposes a strategic shift, anchored in four structural priorities:

1. **Digital infrastructure must be treated and funded as a core national security asset**
2. **Resilience planning must go beyond physical fiber and data centers, to address software, routing systems, and digital platforms**
3. **Crisis coordination must become real-time, cross-sector, and executable under stress**
4. **Resilience must be regional by design—not national by assumption**

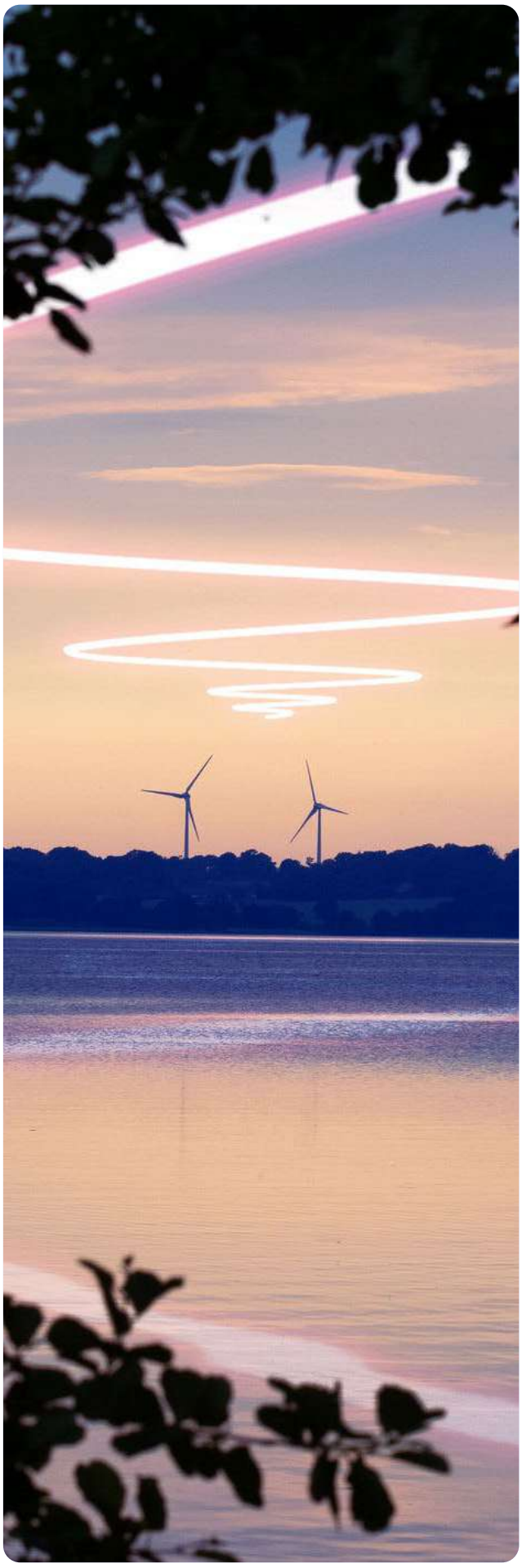
Based on these principles, the white paper proposes three strategic initiatives:

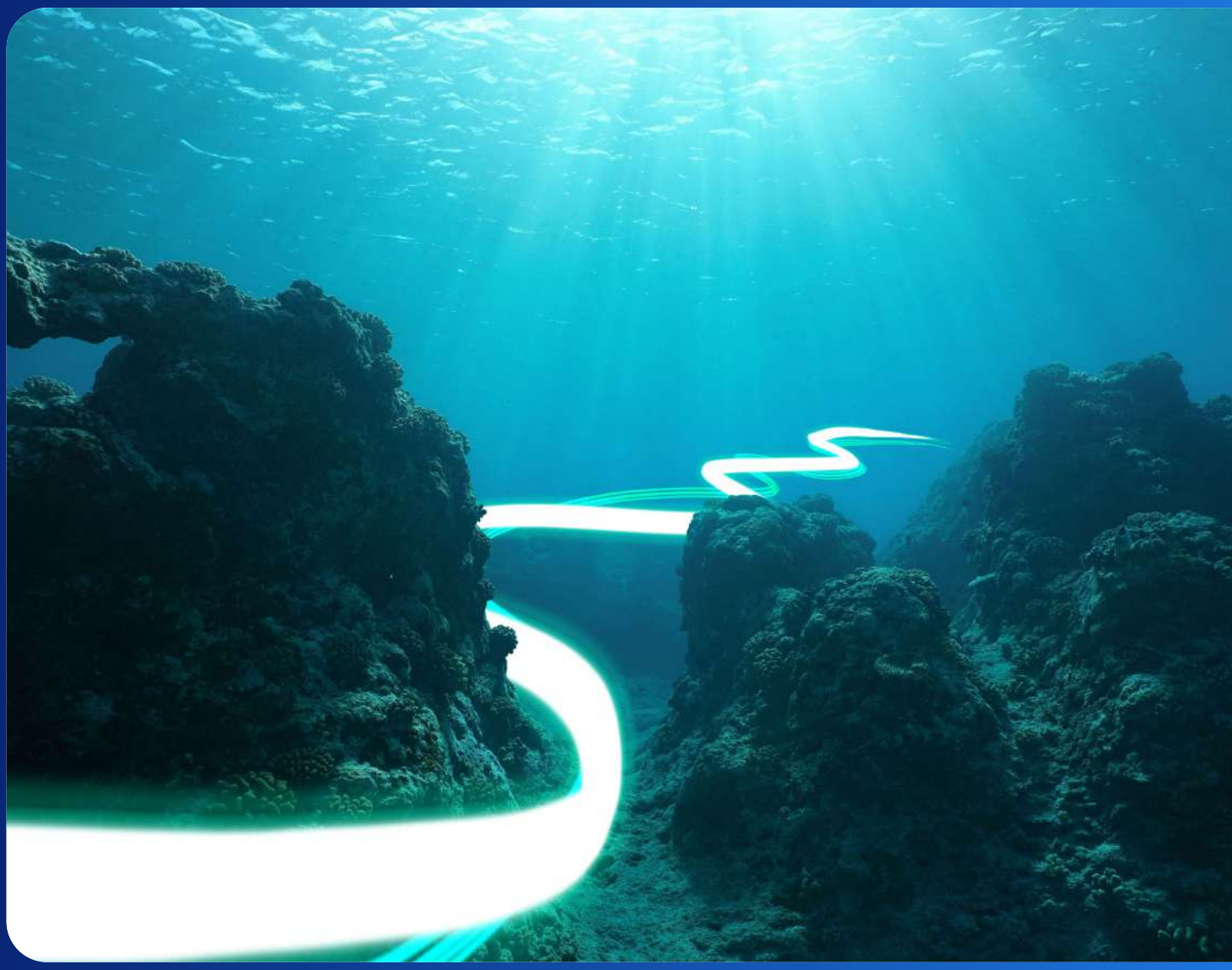
A **A national Digital Resilience certification framework,** led by NSM, to assess and validate the real-world continuity capabilities of critical entities—from telecom networks to cloud and data infrastructure.

B **A Nordic Digital Resilience Shield,** developed in partnership with trusted neighbors, to enable cross-border fallback routing, secure cloud enclaves, and joint surveillance and recovery protocols for shared infrastructure.

C **A recurring Black Sky Simulation Series,** designed to test and rehearse Norway's institutional response to multi-sector, multi-day digital failure—building not just readiness, but proven survivability.

Taken together, these measures redefine resilience not as a checklist, but as an infrastructure—governed, tested, and aligned across borders. Because in today's environment, constant availability and continuity is not something to assume. It is something to build—deliberately, together, and before it's needed.





01

Overview of the Digital Infrastructure

Norway as a green, high-performance digital backbone across mountains and fjords

Norway stands among Europe's digital elite, with high levels of fixed and mobile broadband penetration, proactive digital policy, and a well-functioning, competitive market. With real GDP per capita that is roughly 115% above the EU average[1] and consistently ranked among the least corrupt countries globally[2], Norway provides a stable and highly attractive environment for digital infrastructure investments.

The telecom market in Norway is healthy , and rational, with infrastructure build-out driven by long-term planning, utility participation (e.g. Altibox), and public-private coordination.

The country has a long-standing reputation for digital adoption: over 70%[3] of its population possesses strong digital skills, and Norwegian consumers are highly active users of online services, e-ID, and mobile payments. Norwegian consumers spend about 4% less on Telco services annually than the EU average[4], thanks to affordable broadband and bundled mobile plans.

Overview of the digital infrastructure and interdependencies

Modern life runs on digital services—from navigation apps and streaming platforms to e-health and public administration. But behind that simplicity lies a complex infrastructure most users never see.

At its core is Norway's national digital backbone: a network of long-haul terrestrial and subsea fiber cables that connect the country to global internet systems. These cables link to data centers, where cloud services and online platforms are hosted and processed.

From there, connectivity reaches homes, businesses, and institutions via fixed networks—using fiber, coax, or legacy copper. This supports critical functions like remote work, digital healthcare, and online education.

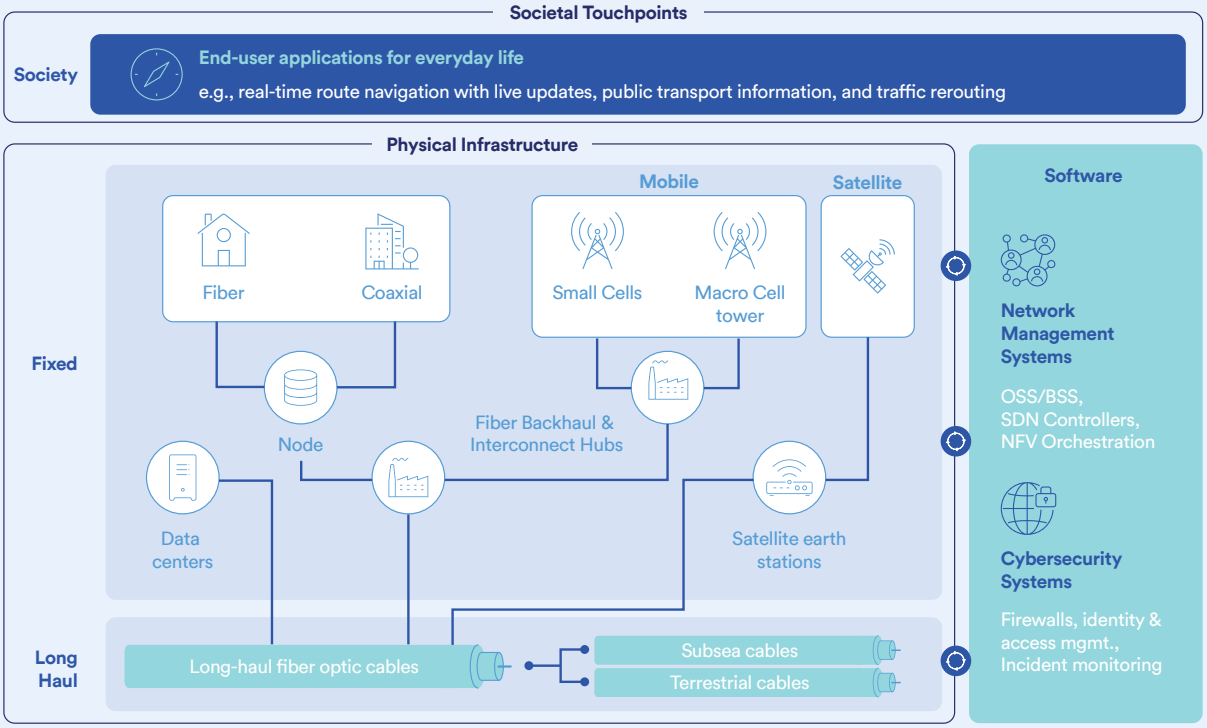
Mobile networks build on the same backbone, using antennas and small cells to deliver 4G and 5G coverage nationwide. Satellite ground stations add redundancy, especially in remote areas.

Above the physical layer, software systems manage data flows, allocate bandwidth, and ensure secure routing. Cybersecurity tools protect every digital interaction—from login credentials to online payments.

Together, these layers form the invisible engine behind Norway's seamless digital experience.

1. European Commission, EU Trade Relations with Norway: Facts, Figures and Latest Developments.
2. Transparency International, *Corruption Perceptions Index Norway*.
3. Consultancy firm analysis.
4. European Commission, *Digital Economy and Society Index (DESI) 2022: Norway.*

Comprehensive overview of network architecture and infrastructure dependencies



Mobile networks rely heavily on fixed fiber infrastructure for routing, timing, and data transport. While they appear independent, their resilience depends on the fiber backbone beneath them. Fiber networks are more robust thanks to their distributed design and rerouting capabilities. In contrast, mobile systems depend on centralized control points—like the Mobile Core—which creates single points of failure that can disrupt large parts of the network.

Some telecom operators now position themselves as fully protected against service disruptions. But in reality, all network services still rely on a shared, fragile infrastructure that no single private company can fully protect on its own.

1.1 Fixed Infrastructure: high penetration and near-universal gigabit coverage

Norway has one of the highest levels of high-speed internet coverage in Europe, thanks to strong investment in fiber infrastructure. By 2023, 93% of Norway had access to Very High Capacity Networks (VHCN), and more than 96.6%[5] of homes could get gigabit-speed services. That puts Norway among the top European countries in both categories, despite geographically challenging conditions.

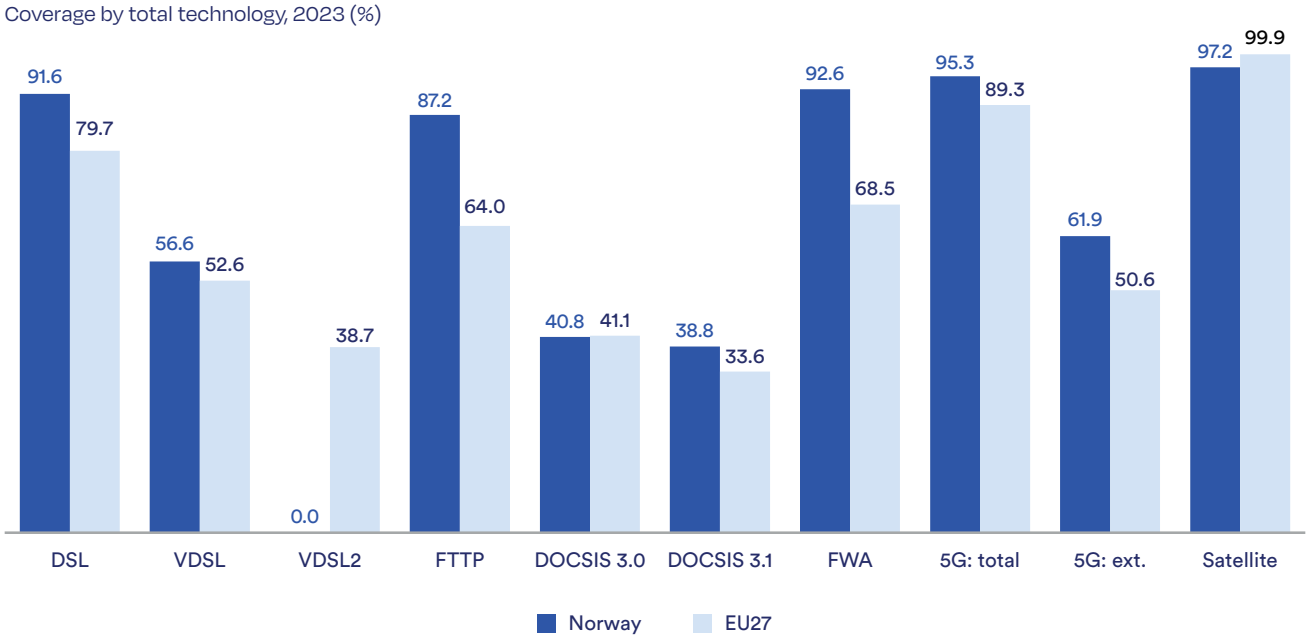
This rollout has been driven by operators like Altibox and GlobalConnect. These providers have laid tens of thousands of kilometers of fiber-optic cable across the country. Global Connect, in particular, has focused mainly on building fiber routes along key national routes.

5. European Commission. (2024, July 2). *Digital Decade 2024: Broadband coverage in Europe 2023*. Shaping Europe's Digital Future. URL: https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-broadband-coverage-europe-2023.

Coverage by technology | Norway leads in FTTP[6] rollout with 87% coverage, surpassing EU average by 23 percentage points

Coverage by Fixed technology

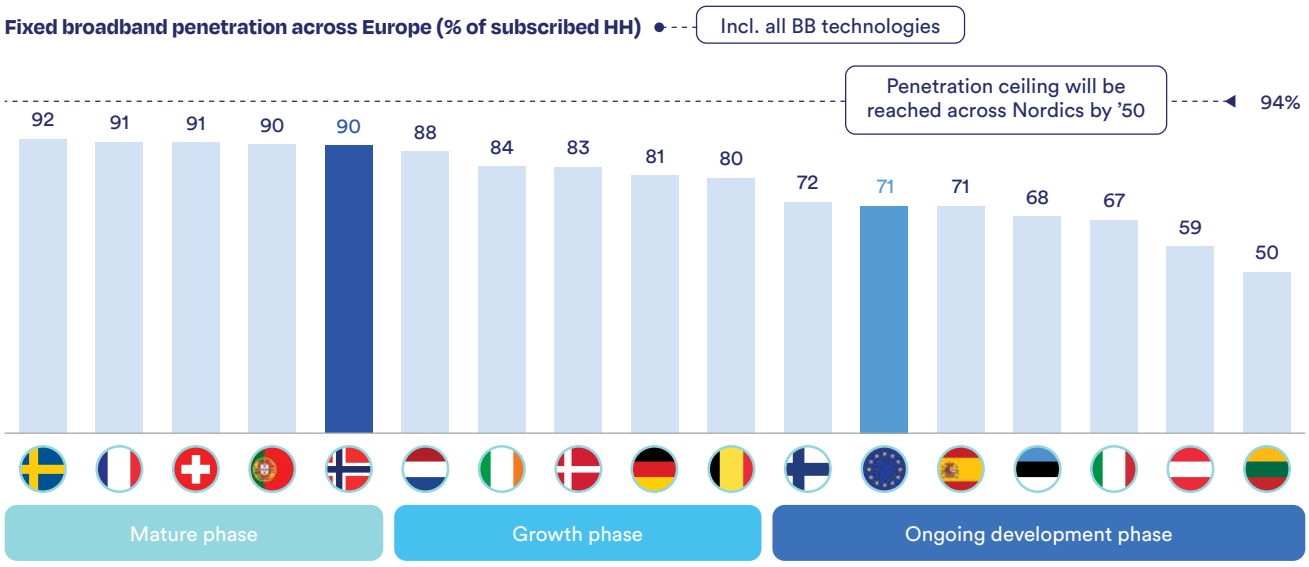
Coverage by total technology, 2023 (%)



Source: Broadband Coverage in Europe – Omdia.
Note: Category '5G: ext.' includes 3.4-3.8 GHz.

Fixed broadband penetration | Norway among EU leaders with 90% household broadband penetration, 18 p.p. above EU average

Fixed broadband penetration across Europe (% of subscribed HH)



Source: Omdia; Company information; Desk research.
Note: As of 01.01.24.; EU average includes 31 country, incl. UK, Ukraine, Russia.

6. Fiber To The Premises (FTTP): Full-fiber internet connection where fiber optic cables run directly to the home or business, enabling ultra-fast, low-latency broadband.

As a result, Norway's fiber-to-the-premises (FTTP) coverage stands at 87.2%—or 23 percentage points higher than the EU27 average of 64%[7]. That includes some of Europe's most challenging geographies, ensuring high-speed access across remote and mountainous Arctic communities.

Norway is at the forefront of broadband adoption, with 90% of households subscribed—18 percentage points above the EU average[8]. Norway's strong consumer demand, digital literacy, and bundling options (for both fixed-line and mobile service) have contributed to its high penetration rate and a smaller "digital divide" between higher- and lower-income households.

The country shows strong growth in fiber adoption, with fiber-to-the home (FTTH) representing 74% of total fixed-line broadband connections[9]. Copper cables are in the process of being phased out or replaced. Telenor announced the shutdown of its copper network in 2019, expecting to reach complete decommissioning in September 2025.

Norway's long-haul digital infrastructure has been shaped by its challenging geography—a country with mountains and widely spread coastal cities, with limited east–west width, particularly in the northern regions. Today, Norway's main backbones run north to south and are all in Norwegian territory, linking key population centers from Oslo to Tromsø complemented by subsea cables for both domestic and international capacity.

Oslo plays a key role in the Nordic triangle, linking Norway to Denmark and Sweden. It is also positioning itself as a low-latency bridge between the EU and North America or Asia, as seen in projects like Arctic Connect. Several commercial initiatives are afoot to assess expanded connectivity even further through new routes such as Leif Erikson (to Canada) and additional Arctic fiber routes. The Government has decided a new sea cable to Svalbard through its state owned company Space Norway. Norway's new fiber infrastructure has improved international connectivity to Europe's five major data centers hubs—Frankfurt, London, Amsterdam, Paris, and Dublin. Oslo's route via Esbjerg links directly to London, Amsterdam, and Frankfurt through Arelion's backbone.

1.2 Mobile infrastructure: High 5G performance and universal coverage

High-bandwidth mobile broadband keeps Norwegians connected and provides a vital backup in areas where fiber to the home is not yet available. The country is on track to meet its goal of 100 Mbps for all by end of 2025[10].

5G coverage now exceeds 99% of the population[11], using both low-band (700 MHz) for wide coverage and mid-band (3.6 GHz) for high performance. Operators have phased out 3G, reallocated spectrum, and expanded handset financing to help users upgrade to faster 5G plans.

The rollout accelerated through discounted licenses tied to rural coverage targets. These incentivizes pushed operators to go beyond the minimum requirements, bringing early 5G access to remote areas, including fjords and islands. Now, new regulations require at least three operators to serve every household. A new emergency network is also planned based on 5G slicing across the three mobile networks. This policy supports national resilience by ensuring multi-operator redundancy.

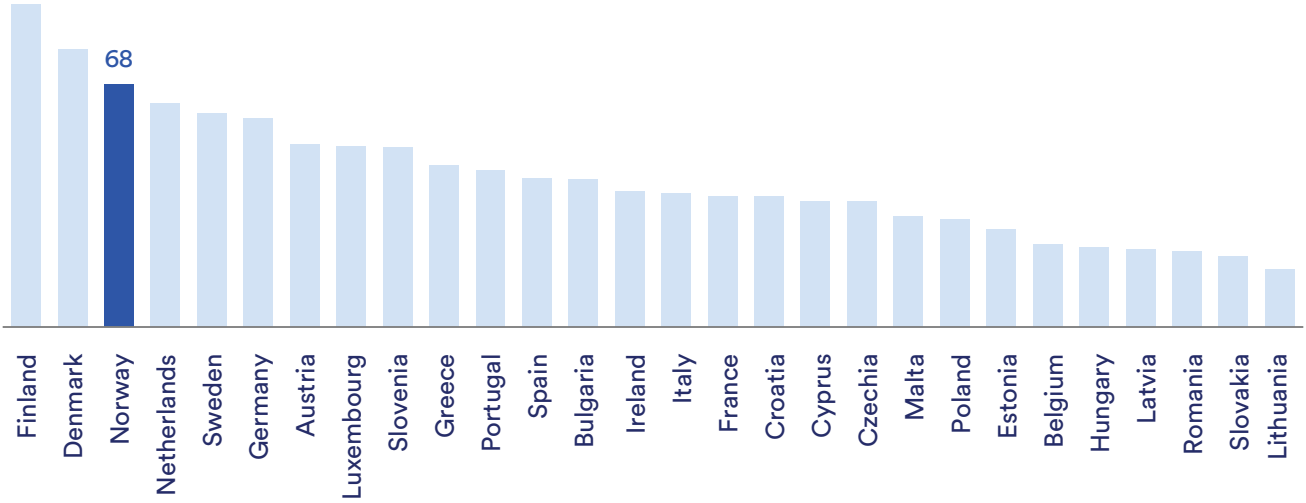
With 68% of mobile users on 5G plans[12], Norway ranks third in Europe for 5G SIM penetration, trailing only Finland and Denmark. Norwegians now enjoy some of the world's fastest mobile speeds, with average 5G download rates around 256 Mbps, according to Opensignal[13].

7. Ibid.
8. Omdia, data as of January 1, 2024; EU average includes 31 countries, including the UK, Ukraine, and Russia.
9. National statistics agencies; Omdia; company information; Statistics Norway; and Consultancy firm analysis.
10. Simon Dux, "Norway on Course for 100Mbps for All by End 2025," *Mobile Europe*, May 7, 2025..
11. European Commission, Shaping Europe's Digital Future, Digital Economy and Society Index (DESI) 2024 Indicators, 5G Coverage, Percentage of Households, accessed June 2025.
12. Source: Omdia.
13. Rupert Bapty, "Rising 5G Availability & Consistency Boosts Norwegians' Overall Experience," Opensignal, September 11, 2023.

5G adoption | Norway sees strong 5G uptake with 68% of the population using 5G subscriptions, driven by aggressive operator migration strategies

5G adoption

5G mobile subscription penetration (in % of population), 2024



Source: Omdia; Samena Telecommunications Council; Desk research.

1.3 Data center structure: renewable-powered and ready for hyperscalers

Norway's data center sector has grown rapidly, evolving from local co-location sites to large-scale cloud infrastructure. The country now hosts over 70 data centers with a combined capacity of around 500 MW[14]. Major global players have established hyperscale facilities, including Google (Skien) Microsoft (Oslo, Stavanger), TikTok (Hamar), and Green Mountain (Enebakk, Rennesøy, Rjukan). Google's Skien site alone is expected to reach up to 860 MW in its final stage and TikTok's Project Clover site up to 150 MW.

Although Norway represents less than 1% of Europe's population, it is projected to account for up to 5% of Europe's data center power capacity by 2030. This strong position is driven by Norway's access to 100% renewable hydropower, a cool climate, and well-developed infrastructure. A significant share of capacity is operated by non-European hyperscalers—primarily Microsoft, TikTok, and Google—reflecting Norway's growing international role in digital infrastructure but also the need for investments in European data center providers.

Norway offers economic and political stability, low-emission electricity, natural cooling, efficient permitting, and strong fiber connectivity. These strengths continue to attract major investments. By 2030, total capacity is expected to reach 900–1,200 MW, including expansions by Green Mountain and growing interest from hyperscalers across the country.

14. Norwegian Datacenter Industry, *The Data center Industry in Norway 2023–2024*.

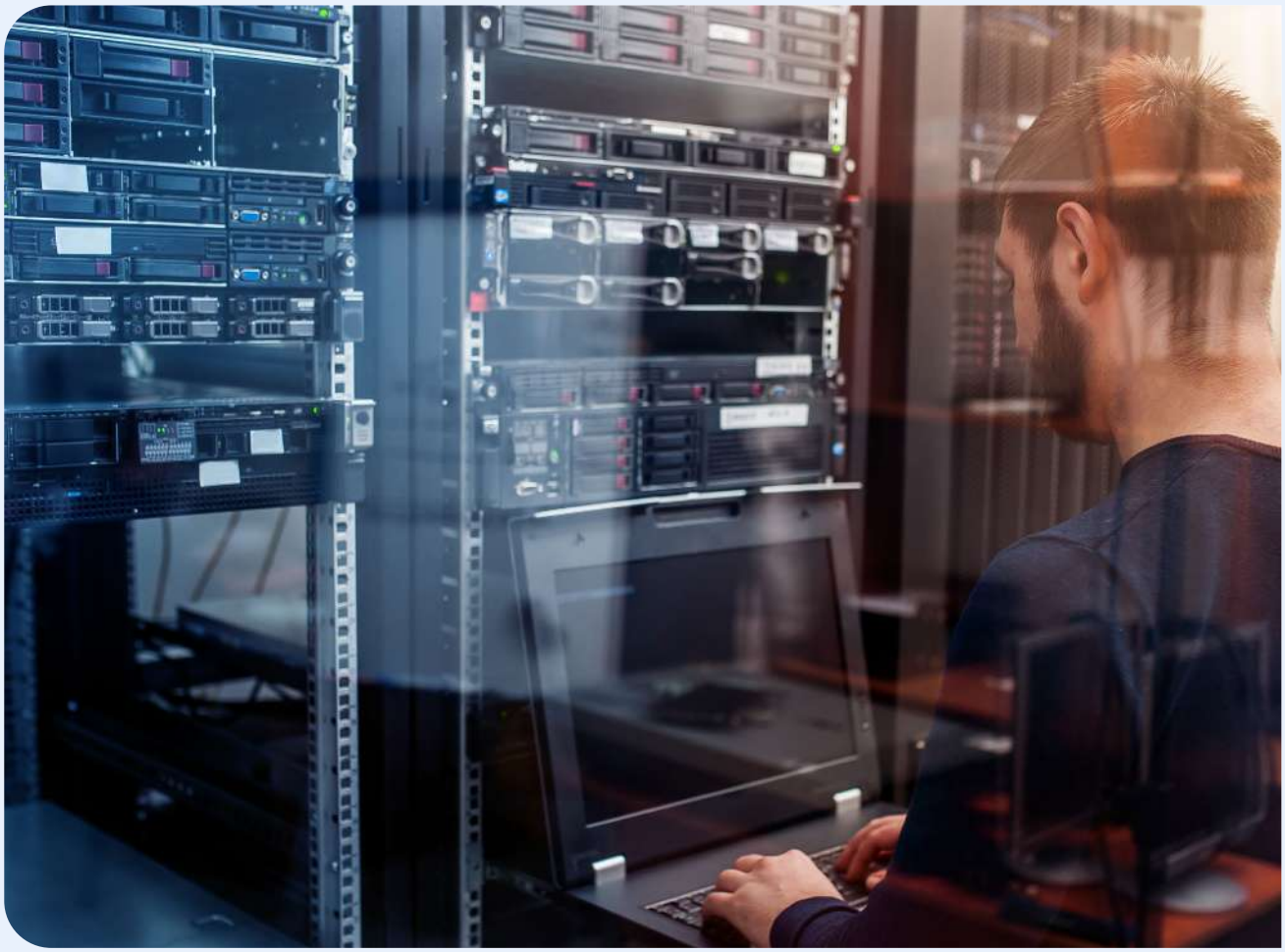
1.4 The role of GlobalConnect

GlobalConnect plays a pivotal role in Norway's digital infrastructure. The company operates a neutral open-access backbone—with a north–south fiber network that reaches Tromsø and provides multi-route coverage via valleys, coastlines, and inland corridors. GlobalConnect covers 100% of transport routes with high and very high demand, as well as 98% of data center corridors.

The company serves about 486,000 premises, including roughly 309,000 apartment buildings, duplexes, and other multi-dwelling units. With a stronghold in Oslo and Norway's southern regions, GlobalConnect supports the enterprise and public sectors with dark fiber, transport, and cloud connectivity.

In addition, GlobalConnect is a registered data center operator and provides colocation services to public and enterprise clients—offering secure, scalable environments for private cloud and server infrastructure. Its facilities include several sites now operated under the **Valhalla** platform, a carrier-neutral, pan-Nordic data center network strategically located across key metros such as Oslo, Stockholm, and Copenhagen. These sites feature direct backbone access and high-availability infrastructure, tailored to support critical workloads with a strong focus on connectivity, ESG standards, and future-ready capacity expansion.

With its experience in cross-border capacity planning and long-distance network routing, GlobalConnect strengthens Norway’s position as a resilient digital link between the Nordic region and the world.



02

Digital Economy and Society Benefits

Norway shows how advanced digital infrastructure can support not just economic competitiveness, but societal resilience and cohesion. With a robust broadband backbone, extensive fiber deployment, and secure national platforms, Norway's digital systems are woven into the fabric of everyday life. They power vital services, improve communication, and drive future innovation. This section outlines how digital infrastructure creates national value, backed by measurable results and cross-sector impact.

2.1 Economic value

Digital infrastructure is not just a supporting function—it has become a **fundamental driver of economic activity in Norway**. It underpins how businesses operate, how people work, and how value is created across industries. As digital systems have become embedded in everyday transactions and operations, they have helped unlock new efficiencies leading to sustained growth.

Manufacturing offers a compelling case of how digital infrastructure directly drives productivity and competitiveness. 24% of manufacturers in Norway rely on IoT monitoring systems—highlighting the shift toward connected, automated operations. These technologies enable real-time tracking, predictive maintenance, and smarter logistics—leading to reduced downtime, lower costs, and faster decision-making. In Norway's advanced industrial base, digital tools are helping manufacturers stay globally competitive in high-value production.

This industrial digital evolution is mirrored in other parts of the economy. Cloud services now form the backbone of enterprise operations, enabling smaller firms to access scalable tools that were once limited to large corporates. The near-universal use of digital payments and online banking has made financial transactions faster, more secure, and more cost-effective. In the energy sector, digital infrastructure enables smart grid operations and real-time monitoring—critical for managing Norway's 100% renewable hydropower system. And investments in telecom infrastructure—spanning 5G, fiber, and resilient platforms—are not only powering digital services but also **contributing directly to GDP and job creation**.

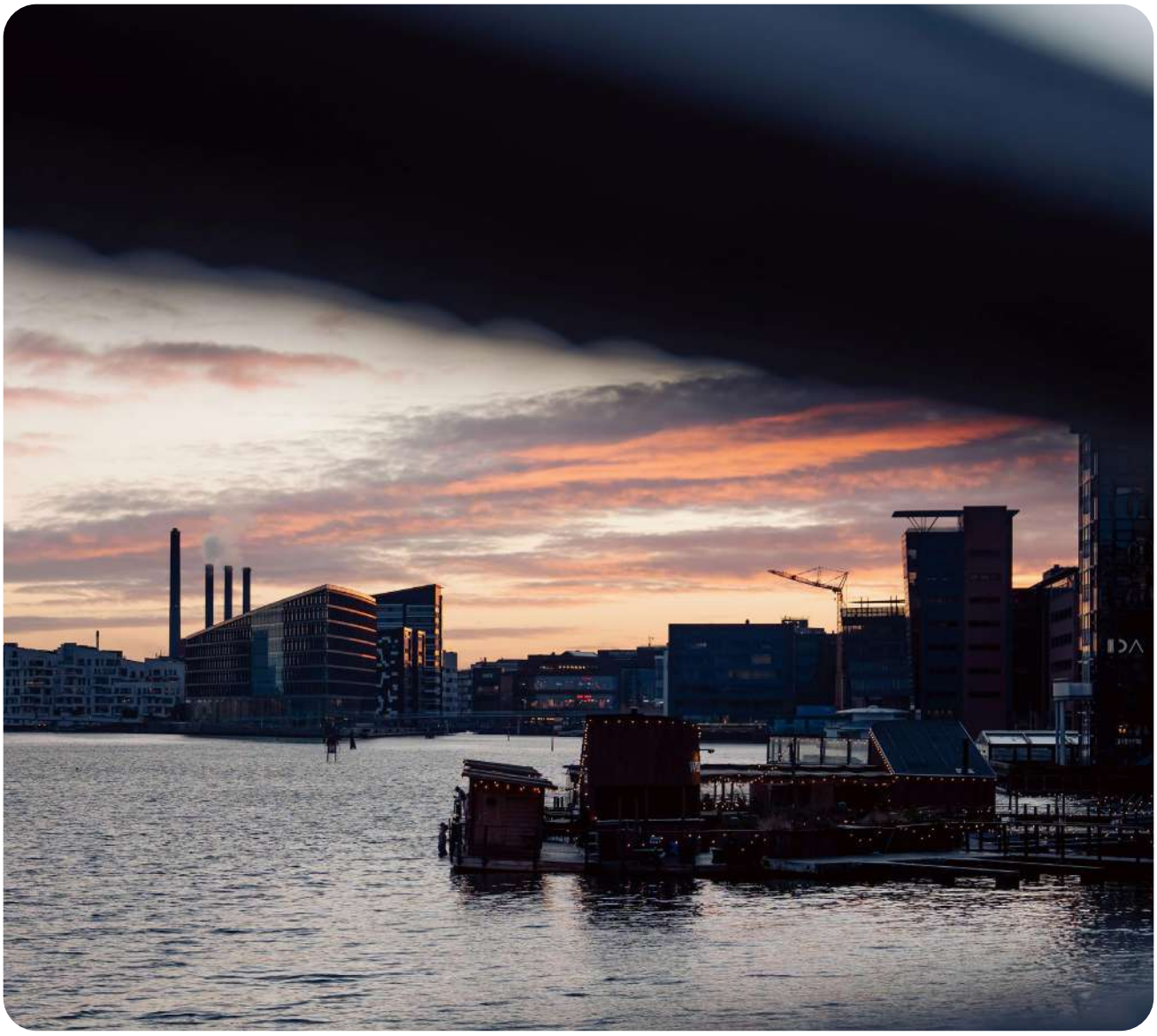
The table below provides an overview of how digital infrastructure contributes to key areas of Norway's economic landscape:

What emerges is not just a story of digitalization—it is a structural shift in how the Norwegian economy functions and grows. As digital adoption continues, so too will the scale of its contribution across all sectors.

Economic digital impact

Sector	Digital impact & adoption rate by sector
General economic impact	35% of Norway's workforce operate fully remote or in hybrid formats 71% of enterprises rely on cloud services for e.g. communication and data storage
Digital transactions	98% of all transactions at points of sales are cashless payments, with either mobile or card 97% of Norwegian adults use online banking
Telecom & Cloud Economy	ICT contribution to national GDP: 2.7% (sector GDP: 12.4B€) Telco directly employs more than 11,700 people Wage level in ICT sector is 30% higher than the average across industries in Norway
Digital infrastructure & Industry 4.0	23.5% of companies across industries use IoT monitoring systems, with a 24% share in manufacturing sector 94.8% of active businesses have access to broadband speeds of at least 1 Gbps

Sources: Norges Bank, Eurostat, OECD, Nkom Statistics, Statistics Norway, EURES, Eurostat-Cloud: Statistcs on the use by enterprise, Statista Digital payment Norway.



2.2

Societal value

Digital infrastructure has become central to how modern societies operate. In Norway, digitalization touches nearly every aspect of society, often in ways that are seamlessly embedded into daily routines yet profoundly impactful. From the way people access healthcare to how they move through cities, interact with the government, or engage in civic life, the benefits of digital integration are both broad and deeply personal.

Everyday tasks, once tedious and time-consuming, have become effortless and instant. Services that once required appointments, paperwork, or long travel times can now be accessed from a smartphone or laptop. At the core of this system is ID-porten, the national gateway for secure digital identification and login to public services. It supports several eID providers, including BankID, MinID, and Buypass, and is used by over 90% of the adult population. Through ID-porten, Norwegians can access a wide range of services—such as tax filings, health records, student portals, and municipal platforms—via a single secure authentication layer.

This infrastructure ensures that digital interactions with both government and private providers are **efficient, secure, and widely accessible**, reinforcing the resilience and reach of Norway's digital society. This convenience is more than just timesaving; it levels the playing field. No matter where someone lives—city center or rural village—digital systems bring public services closer to everyone. They help reduce inequality, increase efficiency, and enhance quality of life for all.

Digitization has also changed how people engage with government: public communication increasingly depends on digital platforms—such as SMS alerts and emergency apps while most TV and radio/music content is now either consumed via streaming services or delivered via digital platforms.

Healthcare offers one of the clearest illustrations of this transformation. Electronic health records are used nationwide, and more than 20% of consultations happen online. This shift has reduced strain on hospitals and allowed patients—especially in underserved regions—to access care more easily. Digital platforms such as Helsenorge.no give citizens access to services like prescriptions, appointment scheduling, and patient records—all widely used in 2024. Since its launch, the app has reached 56.5% of the population and is available in 30.3% of municipalities. These digital tools make healthcare more accessible, transparent, and efficient across the country.

Public transport is another example of how digitalization improves everyday experiences. In the Oslo region, 95% of tickets are sold digitally, and 82% are purchased via the Ruter app—now used by over 500,000 people. Digital tools not only streamline commuting; they also support more dynamic mobility options such as e-scooters, ride-sharing, and real-time traffic routing. For citizens, this means more flexibility, less time spent waiting, and better access to education, work, and culture.

To put the full scale of impact into perspective, the following overview summarizes key ways in which digital infrastructure delivers value across sectors:

Societal digital impact

Sector	Digital impact & adoption rate by sector
Healthcare	20% of healthcare consultations conducted online E-health platform Helsenorge.no is used by 57% of total population
Emergency response	Digital infrastructure enables 730,000 emergency calls a year
Mobility & Transport	95% of public transport tickets are sold digitally, with 82% purchased via Ruter app
Public Services	Digital ID (ID-porten) used by over 80% of adults 99% of Norwegians engage with government digitally
Education	Nearly 100% of schools connected to high-speed internet 98% of secondary students have their own digital device to enable study processes
Media & Civic Life	83% of adults access news online, highest share of all media channel usages 66% of citizens get government alerts via digital channels

Sources: Akershus Fylkeskommune, Helsedirektoratet, Norge.no, OECD, Eurostat, Reuters, Helsedirektoratet, Rail transport SSB, SSB Norwegian media barometer.

Digital infrastructure shapes how society moves through nearly every aspect of daily life. In education, digital infrastructure enables more connected classrooms and helps students build key skills from an early age. That foundation carries into adulthood, where public services—once time-consuming—are now accessed in seconds. This shift has also changed how people engage with government: platforms like ID-porten and Digipost make it easy to stay informed and connected, reinforcing a more transparent and responsive democracy.

In conclusion, Norway's status as one of the world's most digitalized societies has led to substantial progress—economically, socially, and administratively. Digital systems underpin the everyday functioning of the country. But as this integration deepens, so too does Norway's structural dependency on its digital infrastructure. When digital systems fail or come under attack, the effects can spread quickly and cause major disruptions and societal worries. The risk is even greater in today's **shifting geopolitical landscape**, where state and non-state actors increasingly view digital infrastructure as a strategic lever and target.

Disrupting connectivity, platforms, or cloud services—many of which are hosted in other countries—can quickly paralyze the core functions of a society and its economy. This raises a critical question: how can Norway protect its digital infrastructure in a crisis and prevent full-scale breakdowns? Ensuring the resilience and security of these systems is essential for the country to function in the face of growing threats.

03

The Importance of a Resilient and Secure Digital Infrastructure

3.1 When the network fails: real-world consequences

What happens when digital infrastructure suddenly fails—not for minutes, but for hours—across critical parts of society? Too often, **authorities and assessments underestimate the extent of our dependency on connectivity and the complex interdependencies between sectors**. To move beyond assumptions, we examined the effects of a prolonged connectivity loss across five key domains beyond general business continuity: financial systems, energy, transportation, healthcare and education.

While these sectors offer a clear view of how essential operations can be disrupted, the true impact extends far beyond them. A systemic outage reverberates across the entire economy and society—triggering second-order effects in areas not immediately visible, from governance and public safety to supply chains, labor markets, and social cohesion.

Living a loss of connectivity event: the story of Kari

08:00

After dropping Elias at kindergarten, the signal dropped. No news, no information. Lars, my partner, shrugged: “Probably just a local fiber issue.” We smiled—maybe this would be fun. I headed home to log in.

Business continuity: disconnected supply chains and halted operations

In the early hours of a regional network outage, most companies maintain operations. Warehouses, production sites, and logistics centers continue processing tasks already scheduled or pre-loaded into local systems. Freight movements planned up to 48 hours in advance continue, but coordination begins to degrade. Many industrial actors have local fallback capabilities, but few have tested them at scale or across distributed supply chains[15].

By midday, disruptions intensify. Orders cannot be confirmed, transport windows shift, and delays ripple through production lines. According to national risk analyses, Norwegian logistics chains are heavily dependent on network-based coordination and digital documentation[16]. Companies face growing friction from missing inputs, late deliveries, and stalled customer interactions. The situation is especially severe for just in time operations, which depend on up-to-date inventory data and real-time routing.

By the end of the first day, the entire system slows. National authorities describe business activity under these conditions as operating in "slow motion."[17] As more systems go dark—scheduling platforms, inventory tracking, supplier communications—production nodes are forced to work in isolation. Inter-firm coordination becomes manual and patchy. Over the next 24–48 hours, shortages begin to appear in some sectors, especially for medicines and perishable foods partially offset by local reserves.

Unlike countries with more centralized commercial infrastructure, Norway's geography and reliance on distributed logistics amplify these effects. **The country's long distances between production, storage, and consumption hubs make real-time coordination critical—when that fails, delays multiply rapidly.** Remote regions are particularly vulnerable to disruption, as are cross-border flows for essential imports. Unless connectivity is restored rapidly, core sectors enter a state of functional deceleration, with reduced throughput and growing delays across the economy.

While the outage scenarios are described from a cross-sectoral and regional perspective, certain verticals—such as pharmaceutical supply, cold-chain food logistics, and fuel distribution—face disproportionate risks due to their dependency on just-in-time coordination, strict environmental controls, or regulatory documentation. For these, even brief disruptions can cascade into shortages, safety issues, or compliance failures.

15. Direktoratet for samfunnssikkerhet og beredskap (DSB). (2015). *Cyberangrep mot ekom-infrastruktur: nasjonal risikobildevurdering*.
16. Norges offentlige utredninger (NOU). (2015). *Digital sårbarhet – sikkert samfunn (NOU 2015:13)*.
17. Direktoratet for samfunnssikkerhet og beredskap (DSB). (2015). *Scenarioanalyse: cyberangrep på ekom*.

Living a loss of connectivity event: the story of Kari

09:00

Working from home was impossible. No internet, no Teams. I restarted the router, then my laptop—twice. The presentation was ready, but stuck. Outside, a neighbor knocked—her phone wasn't calling out either.

Transportation: the fragile choreography behind everyday mobility

In the first hours of a regional network outage, transport infrastructure keeps moving, but digital dependencies begin to fail. Aviation reacts early. Norway is expanding remote tower operations: over 20 regional airports are controlled centrally via high-bandwidth connections. A major telecom outage could disable these systems, suspending normal flight operations[18].

Ground transport follows. Ticketing platforms, passenger info systems, and dispatch tools go offline. Bus and metro lines keep running temporarily, but staff lose live coordination. Train traffic slows as signaling systems fail to exchange data. Over 60% of railway control systems depend on leased public telecom lines; if these are lost, trains must stop for safety reasons.

By midday, disruptions mount. Urban areas see growing congestion as adaptive traffic control and tunnel management systems go offline. In many cases, tunnels are closed entirely due to disabled ventilation or emergency monitoring[19]. Revenue collection halts as ticketing fails.

By day one, freight logistics become disjointed. Without planning systems and geolocation tools, operators rely on manual fallback. Delays increase. Emergency services face rising travel times due to broken GPS and routing.

By the second day, fragmentation sets in. Regional routes weaken. Long-distance and intermodal transport cannot maintain schedules. The infrastructure exists, but mobility becomes erratic. Even without physical damage, the system slows into disorder.

18. Indra Sistemas. (2025). *23 Norwegian airports to be remotely operated with Indra's cutting-edge air traffic control system*.
19. NOU. (2015). Digital sårbarhet – sikkert samfunn (NOU 2015:13) [Digital Vulnerability – Secure Society].

Living a loss of connectivity event: the story of Kari

10:00

Still no notifications. I grabbed my keys and drove to the supermarket. Traffic lights seemed still functioning. Tunnel 80 was closed. The newsstand was shuttered. Inside Coop, the self-checkout froze. The cashier let me use my debit card—just barely.

Financial systems: a pause in the flow of money

In the first hours of a regional outage or an outage impacting the core financial system, Norway's payment system begins to fail. Most transactions rely on real-time authorization. Only a small number of terminals support offline processing, and contactless payments—which make up 90% of in-store card use[20]—stop immediately.

Fallback capacity is limited. Some BankAxept terminals can buffer up to 1,000 transactions, but with no connection to verify balances, usage halts quickly. Mobile wallets and banking apps are also unavailable. Cash becomes the only fallback, but it's rarely used: only 2% of consumers used cash for their last in-store payment[21].

By midday, payment failures spread. ATMs, now used infrequently, become inaccessible. Most shut down once they can't verify balances or request refills.

Behind the scenes, interbank payment systems also stop. Norges Bank's clearing infrastructure handles large-scale transfers and settlements, including state disbursements. Without connectivity, benefits, payrolls, and supplier payments freeze. Civil protection reports have long warned that such services would cease entirely in a full-scale network outage.

By day one, business payments stall, government transfers don't arrive, and individuals cannot pay bills. Authorities have advised households to keep cash and alternative accounts. In 2024, the government reaffirmed the legal right to pay with cash, calling it essential for emergency resilience[22]. But most residents are not prepared. Even a short outage disrupts commerce; a longer one halts it.

An example of how a failure in the payments sector—without being directly caused by a telecom outage—can still create cross-border disruption is the July 2025 Nets incident. A rare component failure in the Danish payment processor's central systems disabled its backup infrastructure, blocking card transactions for roughly 2.5–3 hours across Denmark[23]. Since Nets also handles acquiring and processing for merchants in other Nordic countries, the outage caused minor but noticeable disruptions in Norway, including temporary card declines and halted contactless payments in certain retail and service locations[24]. While the impact was far less severe than in Denmark, it highlights how tightly interconnected Nordic payment infrastructures are, and how a system failure, whether caused by a telecommunications outage or not, can quickly affect commerce and daily activities in neighboring markets[25].

20. Norges Bank. (2024). *Retail Payment Services 2023*, Memo 1/2024.
21. Norges Bank. (2024). *Retail Payment Services 2023*.
22. Justis- og beredskapsdepartementet. (2024). *Regjeringen styrker kontantberedskapen*.
23. The Local DK – "Failure of Denmark's Nets payment system was caused by 'technical fault'" (24 Jul 2025).
24. Conflingo – "Bank Terminals Down – Card Payment Issues Reported Nationwide" (19 Jul 2025).
25. Reuters – "Nordics and Estonia plan offline card payment back-up if internet cut" (7 May 2025).

Living a loss of connectivity event: the story of Kari

11:00

People whispered in line: no e-prescriptions, no inventory updates. "I'm waiting for the truck; it must be blocked in the traffic" said one of the staff. On the way back, the pharmacy was turning people away. "Systemet er nede," I heard. Police stood at the roundabout, directing cars by hand. My old car's radio was transmitting government news "We are working on it".

Energy: balancing the grid without sight

In the first hours of a national connectivity outage, Norway's power grid continues operating normally. Around 98% of the country's electricity comes from renewable sources—mainly hydropower (88%) and wind (9%)[26]. This mix offers flexibility: hydropower can respond quickly to shifts in demand, supporting short-term stability even if data flows stop[27]. Critical grid operations remain functional, as most utilities rely on internal communication systems or Statnett's secure SNIP network[28].

But as public networks remain offline, coordination weakens. Field reporting slows. Contractors and smaller operators face growing difficulties dispatching repair crews[29]. Customers lose access to digital tools like outage maps or usage apps. Non-critical issues go unreported.

By the end of the first day, the system becomes harder to manage. While power continues to flow, distribution operators work without real-time visibility. Norway does not use a structured prioritization tool like Sweden's Styrel, but emergency load-shedding plans exist. These rely on functioning coordination channels, which may not be available[30]. If physical damage overlaps with digital loss, local overloads could occur.

In non-priority zones—especially rural areas—low-level brownouts may begin. These are not caused by production limits, but by the inability to manage load with precision. Rotational blackouts are applied manually to avoid grid collapse. By day two, fragmentation increases. Local outages may last longer as incident tracking degrades. Energy still flows, but response becomes slow, patchy, and reactive.

If the outage continues, confidence in grid control erodes—not because electricity cannot be generated, but because no one can see where it's needed, failing, or overloading.

26. Norwegian Energy Facts. (2023). *Electricity production*.
27. Invest in Norway. (2025). *Power system in Norway*.
28. Statnett. (2022). *Sikkerhetsstrategi for kraftsystemet* [Security Strategy for the Power System].
29. NVE. (2023). *Kraftberedskapsplan og sårbarhetsanalyse* [Power Preparedness Plan and Vulnerability Analysis].
30. DSB. (2015). *Cyberangrep mot ekom-infrastruktur: nasjonal risikobildevurdering* [Cyberattack on Electronic Communications Infrastructure].

Living a loss of connectivity event: the story of Kari

12:00

Lars came home with Elias. "VPN's dead. I couldn't do anything at work." Elias was upset—his card payment for a small toy had failed. "Could be the terminal, could be the network," the cashier mumbled. Word spread: cyberattack.

Healthcare: the hidden dependencies behind patients' care

In the first hours of a network failure, Norway's healthcare facilities continue functioning, but digital services begin to degrade. Norway has adopted telemedicine at scale: by 2023, 69% of health kiosk interactions involved teleconsultations[31]. National platforms enable online sick leave certification and outpatient follow-ups[32]. These services rely entirely on network access.

Remote patient monitoring (RPM) is also expanding, supporting patients with chronic illnesses like COPD, heart failure and diabetes. Once disconnected, patients lose access to mobile health tools, wearables, and clinical supervision. Healthcare providers receive no data or alerts, suspending monitoring workflows[33].

By day one, communications between GPs, hospitals and emergency dispatch centers become manual. E-prescription platforms and electronic health records stall. Discharge planning is delayed, as follow-up instructions cannot be shared digitally. Chronic patients—who represent around 10% of the population but account for two-thirds of healthcare costs—face higher risk[34].

By day two, fragmentation worsens. Teleconsultations stop entirely. Remote residents lose access to care. Mental health services, which rely heavily on digital therapy platforms, are disrupted. With no real-time data, clinicians must make decisions with incomplete information. Infrastructure remains intact but coordinated care delivery breaks down.

Education: when the classroom goes dark

In the first hours of a network outage, Norwegian schools stay open, but digital systems fail. Tools for lesson plans, attendance, grading, and communication go offline[35]. Teachers use printed materials; staff lose access to schedules and parent updates.

By midday, platforms like Skooler and Visma Flyt are unavailable. Students with special needs lose digital support. Parents receive no alerts, and uncertainty grows.

By day one, remote learning becomes impossible. Norway's system—heavily digitized since COVID—relies on platforms now unreachable. Students in isolation or remote areas are cut off.

By day two, internal functions slow. Alerts, coordination, and assessment systems degrade. Schools in colder regions may close if outages include heating.

Teaching continues where possible, but structure weakens. Without digital tools, education becomes fragmented, less equitable, and harder to manage.

31. Grand View Research. (2024). *Norway Telehealth Kiosk Market Size & Outlook, 2023–2030*.
32. Science Norway. (2024). *People are receiving more digital healthcare in Europe*.
33. Business Norway. (2025). *The rise of remote patient monitoring*.
34. Norwegian Centre for E-health Research. (2023). *Telehealth experiences from Norway – where do we go from here?*
35. Norwegian Directorate for Education and Training. (2023). *Digitalisation in the Norwegian Education Sector*.

The examples described so far reflect only the first-order impacts across selected sectors—but they are just the beginning. A connectivity loss doesn't affect systems in isolation and its impact is often underestimated. **Many other sectors—both public and private—may experience direct or indirect consequences that are harder to foresee in real time, yet equally disruptive.** From missed regulatory filings to breakdowns in public coordination, the ripple effects extend well beyond the initially visible failures.

These examples are not isolated. They expose a system-level vulnerability—one that grows as societies and economies become more and more digital. What starts as a local disruption can snowball into a national crisis. Copenhagen Economics estimates that in Denmark, a severe national connectivity outage could cost **up to €500 million to €1 billion per hour**, depending on the scale and sectoral exposure. While Norway's GDP is comparable to Denmark's in absolute value, its exposure profile is unique shaped by low population density, challenging terrain, and reliance on subsea and long-haul infrastructure. As a result, disruption costs may follow similar orders of magnitude, but with potentially greater variability across regions and sectors.

Immediate effects include failed transactions, halted workflows, and service interruptions. But second-order consequences—lost business opportunities, contractual breaches, and reputational damage—run even deeper. In digital-intensive sectors like finance, logistics, advanced manufacturing, and healthcare, even a brief outage can lead to days of disruption and recovery.

The damage also reaches telecom and cloud providers themselves. For these industries, uptime is critical. While localized failures may overwhelm support services, a systemic, multi-operator outage can undermine market trust—prompting clients to reassess the resilience of their infrastructure, backup plans, and vendor relationships. Similarly, prolonged connectivity losses lead to doubts about the government's ability to manage crises effectively. Domestic and international investors may scale back their commitments if Norway is perceived as a digitally fragile or operationally uncertain environment.

With these structural vulnerabilities in mind, the next section explores how different connectivity loss scenarios might unfold—and why Scenario 3 deserves particular attention.

Living a loss of connectivity event: the story of Kari

18:00

We tried to keep things normal—pasta, no cartoons. Elias fell asleep early. Lars leaned over: "This isn't random. It's too synchronized." I checked the weather. It was already cold, and our heat pump relies on remote controls.

3.2 Scenario methodology and definition

To evaluate the resilience of Norway's national digital infrastructure under high-impact stress conditions, this white paper defines a series of connectivity loss scenarios. These scenarios serve as the analytical foundation for understanding how various types of disruptions could affect the country.

Scenarios were defined using a structured assessment framework based on three key dimensions:

Length of the disruption during business hours:

a. A disruption lasting less than 8 hours

b. A full-day disruption of 8 to 16 hours

c. A multi-day disruption that lasts between 24 hours and a full week)

Loss of connectivity intensity, measured by severity of malfunction and operators reach:

a. Service degradation

b. Full loss of connectivity, for one operator only

c. Full loss of connectivity, for all operators within a region

Extension of the disruption across the population

a. Localized disruption affecting fewer than 5% of the population or network. That's the equivalent of a small town or city district in Norway.

b. Multiple-city disruption affecting between 5% and 30% of all users. That is comparable in size to the greater Oslo area.

c. Large-scale disruption impacting more than 30% of the population. That is comparable to entire southern half of Norway.

While sectoral scope can meaningfully shape the nature and consequences of a disruption, it has not been used as a scenario selection variable in this analysis. For the purpose of this report, **the focus remains on cross-sectorial, regionally scaled disruptions**; however, sector-specific considerations are embedded within each scenario to reflect how different domains would be affected in practice. The table below offers a conceptual overview of how impact scale and sectoral targeting may interact across potential real-world events.

	Regional	National
Sectorial	Likelihood: **Moderate** Disruption to a local system or process within a single sector	Likelihood: **Moderate - Low** Requires failure of a centrally managed service
Cross sectorial	Likelihood: **Moderate - Low** Concurrent disruptions across sectors within a region due to shared dependencies	Likelihood: **Low** Coordinated multi-sector disruption affecting national continuity

To show how the length of a disruption affects the outcome, we kept two factors constant in every scenario: the severity of the connectivity loss and the share of the population affected. Each case assumes a full, nationwide loss of connectivity that affects **30-40% of the population (hence at regional level)** and includes all major operators. This baseline lets us isolate how duration affects services failures, the economic damage, and the difficulty of recovery.

These scenarios combine events that are both likely and moderately disruptive, as well as rare but highly damaging. This mix also gives us a broad range for stress-testing. The goal is not just to simulate challenges, but to understand how systems respond when pushed to the brink. We excluded unlikely or extreme cases—such as geomagnetic anomalies (space weather) or worldwide disasters. But we included severe threats like multi-day, multi-operator connectivity losses caused by cyberattacks, infrastructure sabotage, or geopolitical conflict. These risks are no longer hypothetical—they are central to national resilience planning.

The **three scenario** are as follows:

1 **Connectivity is lost across all fixed and mobile operators, lasting up to four hours.** The disruption is regional/sectorial, but relatively brief. The impact on service is immediate, however, operators can typically restore functionality within a few hours, significantly limiting the overall disruption to customers and ensuring rapid recovery of critical services.

Low impact – Moderate likelihood: Short disruptions caused by localized hardware failure, shared infrastructure issues, or software bugs are common yet not frequent.

2 **Connectivity is lost for eight to 16 hours across all fixed and mobile operators.** This full-day disruption impacts core operations and coordination across sectors. Manual backups begin to fail, too.

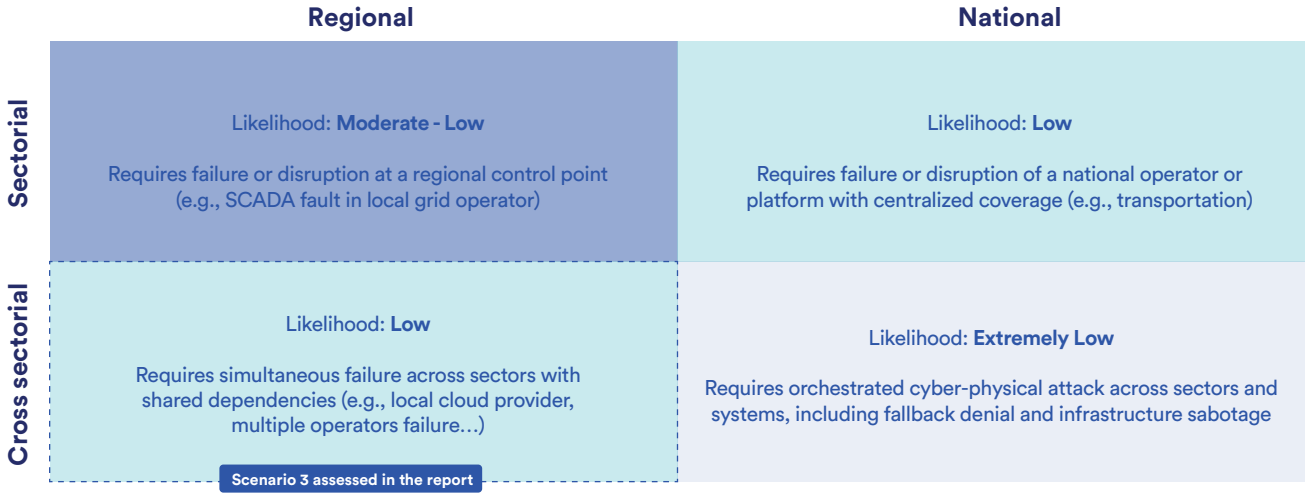
Moderate impact – Moderate-Low likelihood: Requires convergence of factors such as cyberattacks, partial grid instability, or orchestration failure. While less frequent, these events are credible under pressure (e.g. hostile state activity, insufficient fallback capacity).

3 **Connectivity is lost across all fixed and mobile operators, lasting for at least 24 hours and as long as one week**. This extended disruption causes systemic breakdowns across infrastructure, services, and public trust. The stability of Norway is challenged.

High impact - Low likelihood: Requires coordinated cyber and physical interference—such as sabotage, infrastructure denial, or prolonged grid failure. While unlikely in peacetime, such a scenario becomes plausible in the context of hybrid warfare or cross-border escalation, where the explicit objective is to sever communications and trigger cascading disruptions across multiple sectors. This risk is exacerbated in geographies with natural chokepoints—such as Norway's narrow land corridor at the **corridor of Svinesund**—where vital infrastructure (fiber cables, transport, and power lines) is concentrated in a constrained area, making disruption both more feasible and more damaging. A comparable scenario can be represented by a targeted attack on specific sectors, such as energy or transportation. In the energy sector for example, Norway operates under a concession-based system where each geographic area is served by a single licensed distribution operator. This setup, while efficient, also introduces single points of failure: compromising a key regional operator or control system could disrupt power delivery within the respective region. Conversely, the transportation sector, while more fragmented, features regional operators whose interconnectivity means that disruptions can propagate beyond their immediate areas. Entities like Ruter in Oslo and Kolumbus in Rogaland manage extensive networks that, if compromised, could affect multiple regions.

The following matrix illustrates the likelihood and the potential causes of different **scenario 3** configurations.

For the purpose of this report, we assessed scenario impacts from a regional perspective; however, events with severity and likelihood comparable to Scenario 3 could also arise from targeted attacks on specific critical sectors such as financial institutions and transportation.



3.3 Loss of connectivity scenarios root causes, real-life examples and impact estimation

The table below show how a loss of connectivity can spread quickly—with a software bug leading to platform failures and, eventually, a nationwide disruption. Each scenario is linked to specific hardware and software vulnerabilities, with real-world examples as reference points.

As the disruptions grow in severity, several patterns emerge from the cases above. These patterns offer insights into how disruptions unfold and where systems are most vulnerable:

- **Mobile and wireless services are the first to fail—their fragility making them a digital domino in a cascading crisis.** Because these systems share infrastructure, use common radio spectrum, and lack physical separation, a problem in one area can spread to multiple providers. This makes mobile services vulnerable to wide-scale loss of connectivity. Scenarios 2 and 3 show how quickly mobile disruptions can impact large populations and critical services.

Living a loss of connectivity event: the story of Kari

22:00

Lying in bed, I thought about what might come next. If the grid goes out, we're too far north for this to be safe. We were told to be prepared—but what does that really mean? I remembered the krisepakke kit the authorities recommend—flashlight, cash, radio, canned food. We never made one. Tomorrow: food, cash, batteries.

Escalation of root causes (incl. real-life examples) across scenarios

		Scenario 1	Scenario 2	Scenario 3
Hardware/ Physical	Fixed cable & equipment	Terrestrial cable cut on operator's primary route and rerouting is manual and not pre-configured; damages to network equipment (e.g. fire/flood) Example > France 2022: fiber cuts caused regional disruption for 3h	Shared backbone cut (terrestrial/subsea) and hardware failure at shared core disrupts inter-operator traffic; manual rerouting needed; damages to shared network equipment (e.g. fire/flood) Example > Norway 2024: connectivity loss across Telenor, Telia, and Ice due to shared core failure	Coordinated cuts (terrestrial/subsea) disable all redundant routes; physical isolation blocks routing until on-site repair; severe and persistent damages to shared network equipment, with difficulties in repairment (e.g. fire/flood)
	Mobile/wireless equipment	Local core outage or isolated jamming; cells go offline until rerouted/restarted	Shared core failure or jamming on common grid; recovery needs cross-operator coordination	Attack on multiple cores - control rebuilt from backup systems. Jamming of fallback options can prolong recovery time
	Power/electricity	Power loss at one core site; batteries deplete before generator can take over	Grid failure at shared site; backup activates but isn't scaled for all operators	Large-scale outage affects multiple sites; fuel shortages delay generator refueling Example > Portugal & Spain 2025: grid failure cut internet traffic by 90%; many services offline into next day
Software	Software/ control plane	Misconfigured update breaks routing or auth on one operator's system Example > Denmark 2024: TDC software issue caused hours-long outage; 112 calls affected	Faulty software pushed to shared systems causes crash across ISPs Example > Sweden 2024: CrowdStrike bug triggered widespread digital service failures	Core systems crash; orchestration and provisioning must be restored from backup
	Cyberattack	Local compromise of edge routers or control plane by malware; containment and reset handled by operator	Shared platform (e.g. DNS, auth) compromised; recovery needs joint reset	Ransomware or supply-chain attack disables control and backup; full recovery requires system rebuild

Living a loss of connectivity event: the story of Kari

Day 2 - 08:00

I left early. Tunnel 80 was still closed. I took the bus. The ATM outside Rema 1000 worked—barely. People queued silently. No mobile payments, no balance checks. At the clinic, my mom's prescription couldn't be renewed. "No access to the system," the nurse said. She looked pale.

- **Software missteps and coordination failures can ripple through systems in seconds—exposing the fragility of our interconnected digital world.** Misconfigurations, faulty updates, or bugs in the systems that manage and coordinate digital services—known as orchestration platforms—can trigger fast-moving failures before being contained. In Scenarios 1 and 2, these types of errors spread across providers within seconds before operators can react. The speed and scale of these failures expose just how fragile today's interconnected digital environments are.

- **Cyber threats have moved from theory to reality—growing in sophistication and scale with each passing year.** Norway has already been the target of several cyberattacks: In July 2023, twelve Norwegian government ministries were hit, with reports suggesting possible ties to Russian state-sponsored hackers. Earlier, in September 2020, Norway's parliament faced a major cyberattack that compromised the email accounts of several parliament members and employees. These real-world incidents underscore the risks modeled in Scenario 3, where multiple core systems are attacked at once, causing severe disruption. What was once a remote possibility is now a vividly real threat.

- **The most pressing risk today is no longer a single attack but a perfect storm—simultaneous, multi-layered assaults on interconnected systems.** Scenario 3 provides the most realistic threat: disruption is triggered by a mix of physical sabotage, cyberattacks, and power grid instability. These aren't isolated risks anymore—they are converging. Preparing for this multi-layered threat means developing integrated resilience plans, improving coordination between government and industry, and ensuring that backup systems are in place across the entire network.

> We are incredibly dependent on digital infrastructure, yet it remains extremely fragile. Building in resilience through international cooperation is essential to ensure that seemingly minor (and sometimes preventable) accidents do not cause disruptions to a significant portion of intercontinental internet traffic.
>
> **– Tomas Lamanauskas**
> **Deputy Secretary-General of ITU**

A quantitative analysis shows the severe economic and societal costs of connectivity loss, as shown in the table below. These estimates account for the different levels of uncertainty across sectors—and differences in each region's ability to rely on backup systems. These numbers capture not just the immediate revenue losses, but the cascading failures that paralyze the digitally dependent industries that buttress Norway's economy.

Living a loss of connectivity event: the story of Kari

12:00

The buses were packed; once at home I left Lars a note—on paper. I was heading to my mom's. At the next junction, a small crowd had gathered around a police patrol. They finally said it: 40% of the country had lost connectivity. "We're working on it," they said. But no timeline.

Impact estimation across disruption scenarios

		Measured KPIs	Scenario 1	Scenario 2	Scenario 3
Economical	Digital transactions	Offline digital payments (€M)	5–8 €M	16–24 €M	160–244 €M
		Interbank settlement, large scale transfers (€M)	–	12,000 €M	61,800 €M
	Data center industry	Impacted revenues (€M)	1–2 €M	4–6 €M	43–65 €M
Societal	Emergency responses	Missed emergency calls:	110–160	330–490	3,200–4,900
	Mobility & Transport	Flights delayed/ cancelled (pp):	13–20 k	40–61 k	400–600 k
		Urban public transports delayed/cancelled (trips)	112–170 k	340–500 k	1,700–2,500 k
	Healthcare	Missed scheduled tele-consultations:	1–2 k	3.6–5.5 k	35–55 k
	Public Services	Unavailable government transactions:	46–69 k	140–210 k	1,400–2,100 k
	Education	E-learners impacted:	175–265 k	530–800 k	1,700–2,600 k
	Media & Civic Life	People temporarily unavail. to online news:	270–400 k	820–1,200 k	2,700–4,100 k

Sources: Statista-Digital Payments Norway, Nextmsc-Norway Data center market, Helsedirektorate, SSB-Transportation, Norwegian media barometer.
Note: Impact assessment based on estimates of population impacted and severity of the outage.

Several key insights emerge from the data:

- **The true economic cost of connectivity loss lies far beyond telecoms—it's the ripple effect through supply chains that delivers the harshest blow.** Direct losses in the telecom and digital service sectors make up only a small part of the overall damage. Most of the economic impact comes from the ripple effects through the supply chain—like missed deliveries, delayed production, and cascading slowdowns in sectors that rely on real-time digital operations.

Living a loss of connectivity event: the story of Kari

22:00

At my mom's, she had her old battery radio playing. Nødvarsel had issued a vague update. "The government will speak once the networks are stabilized." We didn't talk much. She lit a candle. I reached for my phone—then remembered.

- **Data center risk is rising.** As Norway expands its cloud infrastructure, any future connectivity loss is likely to have broader, more systemic consequences. Business continuity risks will grow in both size and depth. The consequences of such an event include financial losses up to €1 million for a single data center even for brief outages, with nearly 20% of that related to detection, diagnosis, and system restoration[36]. Data loss, SLA violations, and customer churn can escalate quickly, while broader financial and reputational damage often exceeds immediate recovery costs and becomes difficult to fully quantify. Moreover, such vulnerabilities pose a risk to the country's credibility as a reliable digital hub and may undermine its ability to attract future investments

- **As disruptions deepen, critical sectors like healthcare and emergency services don't just falter—they face systemic breakdowns.** As the connectivity losses grow in length and complexity, key sectors—especially emergency response, healthcare, and transport—move from temporary disruption to full-scale breakdowns. These sectors don't just suffer financial losses; they experience functional degradation, coordination failures, and a growing public backlash.

Here is how the impact builds in each of the three scenarios:

- **Scenario 1 (4-hour connectivity loss):** For the first hour, cached data and automatic failover systems keep basic functions running. But as the blackout stretches beyond 2–3 hours, cracks start emerging.

  - **Business continuity:** Local operations hold internal order systems, warehouse tasks, and production lines continue using cached data and on-premise infrastructure. Air and sea cargo move as planned as long as fallback systems hold, and remote employees—around 500,000—work on offline tasks. External system syncs begin to fail, setting the stage for deeper breakdowns. Manufacturing switches to local, pre-programmed controls that can run independently from the cloud. Robots and automated systems run in isolation, partially reducing efficiency gains from digitization (-15/20%)[37] but maintaining minimal output.

  - **Economic transactions:** Retail purchases continue in offline mode, allowing most basic transactions to be processed. Up to €8 million of offline transactions are blocked as majority of POS freeze after reaching the limits of offline transactions. As anxiety arise, consumers flock to ATM terminals initially operating in offline mode, but many are soon disconnected as a security measure.

  - **Energy:** The grid holds. Smart meters store data locally. Remote control rooms retain partial visibility via cached telemetry and backup links. Approximately 40% of renewable capacity (relative to the connectivity loss area) is strictly monitored and configured to disconnect promptly in case of unpredicted production peaks. At this stage, grid design mitigates blackout risks preventing them from amplifying network stress.

  - **Transportation** c.a. 32k rail trips experience delays and potential cancellations as trains reduce speed and increase spacing. Urban transport slows down due to lack of coordination and difficulties in validating the tickets affecting other 100k passengers. Up to 20k air travelers are affected as main airports freeze and staff struggle to manage check-ins and baggage manually. Critical road tunnels may be closed as a precautionary measure, as real-time monitoring and emergency

36. Ponemon Institute – Cost of data center outages.
37. Based on Strategic consultancy firms, assuming partial maintenance of productivity gains in a first phase.

Living a loss of connectivity event: the story of Kari

Day 3 – 08:00

The fridge was humming weakly. We had oatmeal. Lars and Elias joined us mid-morning. "All tunnels into Tromsø are closed," Lars said. Main roads were for emergency use only. The store shelves were half empty. Two-item limit per person. My card worked—just. A woman behind me sobbed.

communication systems become unreliable, making continued operation unsafe. Traffic lights remain functional but lose optimization, causing initial congestion. Car-sharing services and part of the electric vehicles are no longer available due to failed authentication and charging access.

- **Healthcare**, hospitals work from cached electronic records, postponing up to 2k online consultations and approximately 20k medical prescriptions cannot be used. Difficulties arise in hospitals ERs due to the unavailability of systems, potentially posing urgent ER patients' lives at risk. In addition, remote health control systems are not able to transmit real time data to hospitals and practitioners.

- **Other** (emergency, public communication, education): Emergency services switch to voice and radio, but 110–160 calls face delays without GPS-assisted dispatch. Around 50k e-government transactions are queued, and 200k students lose access to digital learning. News sites go offline, pushing the public back to radio and TV for information.

- **Scenario 2 (8- to 16-hour loss):** As the disruption extends into a full working day, the **impact shifts** from temporary inconvenience **to systemic degradation**. What could be absorbed through cached data, manual overrides, and short-term fallbacks in the first few hours begins to unravel. This is no longer just a longer outage—it's a qualitatively different **phase of crisis, where coordination weakens, resilience buffers deplete, and multiple systems start to fail in parallel**. By this stage, the response is fragmented, and the shock is no longer linear—it's **exponential**. As the outage passes the 8-hour mark, it becomes not just longer, but deeper—an erosion of cohesion, control, and capacity.

- **Business continuity:** External integrations collapse: supplier portals, inventory syncs, and ERP platforms go dark. Last-minute supply chain adjustments freeze. Structured businesses with scheduled replenishments and stocks are able to manage demand surges while replenishment halts for unprepared retailers. Remote teams disconnect, and logistics flows lose visibility. Physical cargo moves, but rerouting becomes guesswork; some shipments are blocked due to tunnels closure. Automotive and electronics production lines slow down, and output drops further. Operations begin to fragment.

- **Economic transactions:** Online payment systems continue to support transactions, as long as card limits are not exceeded, and operators permit offline mode. However, rising public anxiety drives consumers to crowd supermarkets. As predefined thresholds are surpassed, cards begin to be rejected at checkout. Meanwhile, as the cut-off time for interbank transactions is reached, approximately €12B[38] in payments are blocked—affecting interbank settlements, supplier payments, and margin transfers, and triggering liquidity mismatches across institutions.

- **Energy:** Without access to live SCADA data, the grid suffers for prolonged absence of frequency or load monitoring. Balancing becomes unstable and operators begin manually ramping up conventional production assets, while disconnecting wind plants to reduce the risk of cascading blackouts.

- **Transportation:** Around 65k rail trips face compounded delays as coordination between lines breaks down and some services are suspended. Up to 40k air travelers are affected by mounting delays or cancellations as fallback

38. Norges bank - Annual Report 2023.

Living a loss of connectivity event: the story of Kari

18:00

The power flickered, then went out for over an hour. We lit a fire. My mom asked if we were at war. "Not yet," Lars said. But we weren't sure. Still no signal. No updates. No trust.

procedures fail and flight operations are limited for security reasons. Urban transport becomes increasingly unreliable, with buses operating off-schedule and real-time updates unavailable. Traffic congestion intensifies interfering with emergency service vehicles and logistics

- **Healthcare:** Non-urgent procedures are cancelled and telemedicine collapses entirely. As time passes, hospitals struggle to maintain coordination, remote monitoring systems remain offline, and critical data becomes inaccessible placing an increasing number of citizens' lives at risk, particularly among chronically ill patients

- **Other** (emergency, public communication, education): Emergency dispatch is overwhelmed, with 330-490 calls critically delayed. e-Government services stall, virtual exams are cancelled, and parents keep being cautious. Lack of official updates fuels panic and erodes public trust.

- **Scenario 3 (multi-day loss; up to a week):** When connectivity is lost for days, the disruption becomes systemic. Redundancies collapse, coordination breaks down, and institutional capacity is overwhelmed. Trust erodes—not just because systems fail, but because the response appears slow and fragmented. What begins as technical fragility turns into perceived strategic vulnerability. Damages start to propagate beyond the initially affected areas, spilling over into adjacent sectors, regions, and even neighboring countries. At this point, Norway risks entering a true **doomsday scenario** for a digital state—where service failure cascades into institutional and geopolitical instability.

- **Business continuity:** Systems unravel. Manual workarounds falter, inventory data is outdated, and dispatches stall. Manufacturing can't retrieve orders, predictive tools are blind, and fast-moving stock starts disappearing from supermarkets' shelves as a result of both panic buying and difficult inventory management. Over 40% of workers sit waiting. Continuity doesn't degrade—it collapses.

- **Economic transactions:** People rush in supermarkets and the few remaining cards still being accepted fail. Over € 60 billion in retail, corporate, and cross-border transactions accumulate, halting everyday transactions, payrolls, treasury operations, and supplier payments. Even if financial markets remain technically open, trading would decouple from real-time liquidity and settlement visibility. To preserve confidence and prevent disorderly pricing, authorities would likely preemptively suspend exchange operations—not because systems are unavailable, but to protect the integrity of the market.

- **Energy:** Control deteriorates. Smart grids revert to passive infrastructure and distribution faults go undetected. A growing share of renewable inputs disconnects, while conventional generation struggles to sustain demand due to limited capacity and insufficient fuel reserves. Brownouts spread across non-priority areas, and planned interruptions are rotated region by region. Without centralized coordination or real-time data, power flow becomes guesswork, and grid-wide instability accelerates.

Living a loss of connectivity event: the story of Kari

Day 4

People said Narvik's hospital had stopped new intake. Someone smashed a payment terminal—not to steal, but out of desperation. The ATM screen read "Service Unavailable." In the town square, printed flyers replaced digital boards. Rumors of diesel rationing spread fast.

- **Transportation:** Flights remain grounded. Rail disruption affects over 500k trips as coordination collapses. In a country without connectivity, the question is no longer how to move—but why
- **Healthcare:** hospitals revert to paper charts; consultations and lab tests accumulate. ICU triage relies on manual vitals; drug inventory management degrades. Even urgent care begins being at risk.
- **Other** (schools, emergency services, public communication): Emergency dispatch is overwhelmed, response times worsen, and critical interventions are delayed. Schools operate without digital tools, but growing anxiety and lack of updates lead many parents to keep children at home. The collapse of news and public information channels fuels misinformation and erodes public trust.

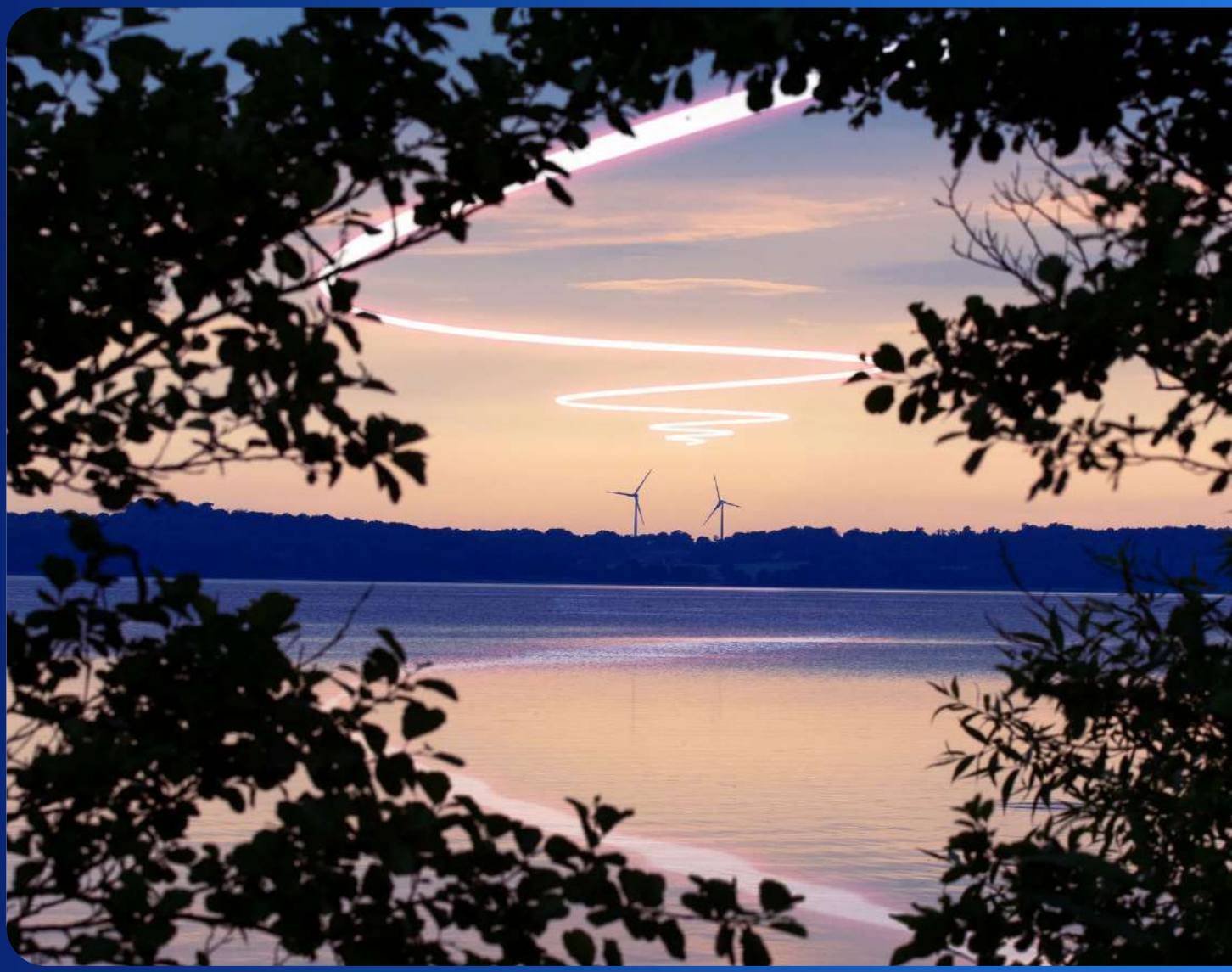
And yet, these scenarios don't fully capture the reputational and strategic implications for Norway.

In a country like Norway—where digital infrastructure is embedded in everything from Arctic surveillance to offshore energy coordination—a prolonged outage would send shockwaves beyond the balance sheet. Public confidence in the state's ability to protect and deliver essential services could erode rapidly, especially in rural and remote areas that already operate at the edge of coverage. For international stakeholders, it raises questions about Norway's resilience not just as a digitally advanced nation, but as a strategic node in transatlantic and pan-Arctic data flows. The country's ambition to be a trusted hub for green data centers and subsea connectivity relies on an image of fault-tolerant reliability. If that image falters, so too does Norway's credibility as a destination for high-value, long-term digital infrastructure investment.

Living a loss of connectivity event: the story of Kari

Day 5

No school. No alerts. Just silence. Elias asked, "Will we still have Christmas?" I didn't answer. I'd stopped hoping for the signal. That night, we all sat quietly together. "This should never happen," Lars said.
I nodded.
Not here. Not ever.



04

From Shock to Strategy

What scenario 3 tells us about what Norway still lacks

Norway stands at a crossroads in digital resilience—its future shaped by growing geopolitical tensions, rising cyber threats, and increasingly tangled cross-border dependencies. For years, the country prioritized efficiency and scale by relying on global vendors—Cisco for core systems, and the U.S.-based "hyperscalers" for cloud computing services. This strategy helped the country modernize quickly, but it also created structural dependencies and vulnerabilities that now require urgent attention.

At the same time, many infrastructure operators remain overly confident in their current capabilities—trusting that distributed assets or local redundancy alone will carry them through. But in a landscape shaped by interdependent systems, software consolidation, and targeted attacks, this confidence can mask deeper exposure. **Resilience can no longer be assumed. It must be designed, coordinated and verified.**

Norway's digital infrastructure is already governed by one of Europe's most comprehensive legal frameworks: the **Norwegian Security Act (Sikkerhetsloven) and the Ecom Act (Ekom loven)**. These Acts mandates that critical infrastructure operators—including telecom networks, cloud providers, and data centers—implement strict physical and logical security measures, maintain off-grid operational continuity, **map systemic interdependencies**, and report significant incidents. These obligations are overseen by **NKOM – the National Communication Agency** which are the regulator and control instance for the Ecom Act and **NSM – the Norwegian National Security Authority**, which acts as the country's lead agency for safeguarding national security interests. NSM is responsible for issuing threat advisories, auditing critical entities, and coordinating response efforts in the event of cyber or hybrid attacks. However, while the legal foundation is strong, practical implementation remains uneven[39]—particularly among smaller, regional, or non-European providers.

Today, digital infrastructure is no longer just a technical asset. It has become a **strategic pillar of national security**—on par with energy security. Protecting it demands more than isolated upgrades or sector-specific planning. Norway must treat digital resilience as a system-wide objective—one that encompasses national risk governance, infrastructure design, and coordinated emergency response.

This shift is already underway: Nkom started conducing regional risk and vulnerability analyses targeting exactly these issues—single points of failure, route diversity, and critical dependencies in fiber routes, centralized data hubs, and traffic-routing systems. The priority now is to operationalize these findings at scale—embedding them in investment planning, enforcing corrective actions with clear timelines, and linking them to crisis playbooks—while moving toward dynamic redundancy, so vital services can be re-routed, prioritized, and restored under cascading failures. This will require **new regulatory tools and crisis protocols**, such as intelligent traffic steering and relaxing "net neutrality" laws during emergencies

At the same time, disruptions must be managed more effectively by creating **shared platforms that give every sector real-time visibility**. Crisis escalation procedures must be formalized and stress-tested across healthcare, energy, telecoms, and digital services. These steps can help Norway detect and respond to events faster but they are not enough on their own. In today's interconnected world, resilience cannot stop at the border.

Norway's position as a digital bridge between international data flows and continental Europe gives it a **strategic role in supporting the development of a resilient regional digital backbone**. This includes storing data in neighboring countries like Sweden or Denmark, investing in cross-border routing systems, and building sovereign cloud infrastructure. With the right investments and partnerships, Norway can move from national preparedness to **leading a coordinated regional strategy**.

Unlike its Nordic neighbors, Norway's digital terrain is shaped by **distinct structural realities**: a vast and mountainous geography, low-density settlements, and extensive reliance on subsea infrastructure—even for domestic traffic. These factors make its resilience needs more complex—and often more costly—than those of Denmark and Sweden. While not all solutions are directly replicable, the Norwegian experience offers valuable insights for designing resilience under high-risk and low-density conditions.

This chapter examines Norway's path toward that goal—reviewing its current progress, identifying the remaining vulnerabilities, and outlining the systemic changes needed to build a more **resilient and interdependent digital future**.

39. Norwegian Ministry of Justice and Public Security (2022). *Meld. St. 9 (2022–2023) Samfunnssikkerhet – en felles ansvar* [White Paper on Societal Security – A Shared Responsibility]. Oslo: Regjeringen.no. Available at: https://www.regjeringen.no/en/dokumenter/meld.-st.-9-20222023/id2950130/.

> We are much more aware than two years ago—but I'd still be surprised if everyone could actually cope with a multi-day outage.
>
> **– Tobias Liebetrau**
> **Research at the Centre for Military Studies, Department of Political Science, UNICPH**

4.1 Mitigation actions and remaining vulnerabilities

Norway has taken important steps to improve the security and resilience of its digital infrastructure. However, some vulnerabilities remain. Norway must recognize that digital resilience is not just a national task. It's a shared regional responsibility and a strategic priority that extends beyond the economic contributions.

Sector-specific resilience across essential services

Many essential service sectors are working to strengthen continuity during connectivity loss, but resilience remains uneven. In healthcare, cybersecurity rules and infrastructure upgrades are improving protection, yet capabilities vary widely and many providers lack tested fallback procedures. The financial sector is expanding backup plans and exploring offline payment options—but support for true offline card transactions remains limited, and high reliance on non-EU cloud services poses strategic risks.

Emergency services use secure, satellite-backed networks but still depend on public telecoms for 112 call routing, creating single points of failure. Logistics, energy, and transport sectors are investing in multi-operator connectivity and running continuity tests. Meanwhile, the education sector depends heavily on international cloud platforms with little ability to function offline. Small businesses and municipalities often lack continuity plans or technical resources.

These structural gaps call for stronger coordination, common standards, and built-in redundancies across all layers—hardware, software, and data. Resilience must also extend across borders, with regional cooperation and diversified infrastructure critical to long-term digital autonomy and national security.

> We don't build roads for the sake of roads—we build them to open up economic opportunity and inclusion. Digital infrastructure should be seen in the same way. Resilience is not just a cost—it's a competitive advantage and a key to ensuring prosperity for all.
>
> **– Tomas Lamanauskas**
> **Deputy Secretary-General of the International Telecommunication Union (ITU)**

B Cybersecurity and threat detection

Norway's cybersecurity model is anchored in strong public-private collaboration and a proactive risk posture. Major telecom operators such as Telenor and Telia operate dedicated security teams and share threat intelligence with both peers and government[40]. National authorities provide clear guidelines, conduct audits, and issue sector-wide advisories to mitigate evolving threats. In 2025, the government escalated its warnings about foreign cyber activity and introduced new early-alert systems and coordination mechanisms[41].

However, critical gaps remain. Smaller, regional operators—such as fiber providers, private data centers, and local internet exchanges—often lack the resources, staff, and training needed for continuous monitoring and defense[42]. Many depend on external, non-European vendors for cybersecurity tools, raising concerns over supply chain exposure and lack of national control[43].

This fragmentation creates dangerous single points of failure between providers. A breach at a poorly defended node can ripple through the broader network. Moreover, like much of the Nordic region, Norway faces a persistent shortage of skilled cybersecurity professionals[44]. The National Security Authority (NSM) is expanding training and information-sharing programs, but broader investment is needed to strengthen talent pipelines and ensure consistent protection across all layers of the ecosystem.

> There's a dangerous false sense of security. Many organizations believe they're protected, but most don't even know about the international standards—let alone implement them. Especially for small and medium sized businesses pragmatic certification frameworks could be helpful to move them from zero to "secure enough".
>
> **– Thomas Flarup**
>
> **Executive VP at Terma, former Head of the Danish Centre for Cyber Security (CFCS), and former Management Board Member at ENISA**

40. Telenor (2024) *Telenor targets growing threats with cybersecurity company*, Mobile World Live.
41. NSM (2025) *National Cyber Threat Assessment – Telecom Sector.* National Security Authority.
42. NSM (2025) *NCC-NO: Building capacity for critical infrastructure.* National Coordination Centre Norway.
43. Telenor (2024) *The NIS2 clock is ticking in the EU – Where will compliance take us in the Nordics?* Telenor Digital Security.
44. NSM (2024) *Cybersecurity Skills Gap in Norway: National Assessment and Strategy Update.*

C Physical protection

Norway's critical telecom and data infrastructure is governed by the Ecom Act and Security Act, which mandates strict access controls and protection against sabotage. Key assets—including telecom exchanges, undersea cable landings, and major data centers—are subject to reinforced standards and sector-specific guidelines, such as secure power enclosures and structural resilience.

However, Norway's vast and rugged geography presents persistent challenges. Fiber routes crossing mountains and remote cable landings remain vulnerable to both sabotage and extreme weather. The 2024 storm Ingunn underscored these risks, prompting new initiatives—like the KystTele partnership with Nkom—to storm-proof and diversify exposed segments.

While urban data centers generally meet high protection thresholds, regional nodes and last-mile infrastructure often lack equivalent safeguards. Unlike more centralized countries, Norway's digital backbone is geographically dispersed, making physical access harder and emergency response more complex.

D Network redundancy and route diversity

Norway learned in 2016–2017 that relying too much on one internet route—through Sweden—created a major risk. In response, the government announced up to **NOK 100 million (~€8.8 million)** in public support to help stimulate the development of alternative international fiber routes, with **NOK 40 million formally allocated in 2018**. These measures were designed to **encourage private investment** in route diversification and reduce the country's exposure to single-path failure[45]. Since then, new routes have been added, including the Havsil cable to Denmark (completed in 2022), and connections to the UK, continental Europe, and North America. This has lowered the risk of one route failing and taking the whole system down.

Inside Norway, new fiber projects have improved the trunk network even across difficult terrain, improving the redundancy of the national backbone. Unlike Denmark or Sweden, Norway often needs custom solutions in rural areas, which don't scale easily to more urban settings. Furthermore, Norwegian policy historically has been that all long haul, backbone infrastructure should be on Norwegian soil. That means all North-South routes are in parallel through the narrow land in mid-Norway. Although there are many cables they are concentrated in a 6km wide land area. That concentration level in such a small distance constitutes a high risk by itself related to sabotage, fires, flooding, and other natural disasters. To establish reliable resilience the distance between cable routes should be far longer – meaning into Sweden and/or Finland.

Also, public investments in non-commercially attractive redundant routes would be needed to increase and guarantee security.

45. Norwegian Ministry of Trade, Industry and Fisheries (2018). *Norwegian data centres – sustainable, digital powerhouses.* Oslo: Government of Norway.

However, critical vulnerabilities remain. The country's geography includes several natural chokepoints where vital infrastructure is concentrated in narrow corridors. One notable example is the corridor near **Svinesund**, the main land bridge to Sweden, where multiple fiber paths, power links, and transport routes converge in a geographically constrained zone.

Any disruption here—whether physical or cyber-enabled—could impact both domestic and international connectivity.

Public investment in redundant, non-commercially attractive paths remains necessary to ensure systemic resilience—especially in these physically exposed and strategically sensitive areas.

> Diversity in vendors and systems protects against connectivity loss, but it comes at a cost. True resilience is a societal decision, not just an operational one.
>
> **–Olav Lysne**
> **Professor at University of Oslo**

Subsea and cross-border infrastructure security

Norway depends on undersea cables for both international and domestic connectivity, including the vital link to Svalbard. To enhance resilience, it has deepened cooperation with Nordic-Baltic partners and the U.S., focusing on real-time information sharing, joint repair capabilities, and improved monitoring. Norway also advocates for global standards to strengthen planning and accelerate repairs.

Nationally, maritime authorities track ship movements near sensitive routes and work with telecom operators to assess risks. The twin cable system to Svalbard proved its value in 2022, when one cable failed but service continued uninterrupted[46].

Still, Norway's long, rugged coastline and limited subsea surveillance create major challenges. Sabotage or damage can go undetected, and patrol coverage remains incomplete. Key priorities include boosting surveillance, expanding repair capacity, and advancing technologies for faster detection and response—efforts that rely on close coordination with allies and industry.

46. Peter B. De Selding, "Update: Undersea Fiber Link to Svalbard Returns to Full Redundant Service with Temporary Fix Awaiting Cable Vessel," *Space Intel Report*, January 13, 2022. URL: https://www.spaceintelreport.com/space-norway-to-start-repairs-of-failed-undersea-cable-in-february-backup-cable-maintains-full-service/.

Incident response, communication, and coordination

Norway uses a cross-sector approach to manage major digital disruptions. This model ensures coordination between regulators, private operators, and emergency services[47]. In the event of a large-scale outage or cyberattack, national emergency protocols allow authorities to assume control, issue guidance, and orchestrate the response[48].

A secure notification system enables public alerts through platforms like Varsling and Nødvarsel, supported by FM radio and satellite backup. A reporting infrastructure is in place for operators to provide incident updates to authorities, although the structure and visibility of a centralized crisis dashboard remain under development. Norway also conducts regular joint crisis simulations with Nordic partners to improve cross-border coordination[49]. Strengthening collective response to incidents like subsea cable disruptions has become a strategic priority, particularly following recent tensions in the Baltic region[50].

However, as a non-EU member, Norway sometimes has limited access to joint regulatory planning and infrastructure protection frameworks. Sweden's NATO accession has nonetheless improved the climate for regional digital coordination[51]. Domestically, responsibilities for digital infrastructure security are distributed across multiple agencies and sectors, which can hinder rapid response in fast-moving crises[52]. Furthermore, as a non EU member, Norway does not have access to EU CEF funding, which are important subsidy programs to increase resilience and diversity in critical digital infrastructure. This will put more pressure on Norwegian government to increase national contributions for the same purposes.

To address this, the government is modernizing its emergency communication capabilities. Planned upgrades include satellite-based fallback channels and real-time monitoring dashboards—tools designed to preserve situational awareness even when core systems are degraded.

Like much of Europe, Norway remains strategically reliant on a handful of global providers for cloud, AI, and data services—most of which operate outside EU jurisdiction. In a geopolitical crisis, access to these critical platforms could be delayed, restricted, or even severed.

There are few sovereign or regional alternatives that match the scale of these "hyperscalers," leaving Norway—and the Nordics—exposed to significant vulnerabilities. Reducing this dependency must be a strategic priority.

Investing in regionally hosted infrastructure, cross-border redundancies, and Nordic–EU public-private partnerships is essential to building long-term resilience. Because these projects may not offer near-term commercial returns, they will require public funding and regulatory support.

This is not just about continuity—it is a matter of national security. Digital autonomy will depend on shared responsibility, interoperable systems, and resilient infrastructure built across trusted borders.

47. Regjeringen (2023) *National Digitalisation Strategy 2023–2030.*
48. Regjeringen (2024) *Support and Cooperation in National Contingency Planning.*
49. Regjeringen (2023) *OECD Peer Review of Norwegian Digital Resilience*.
50. Regjeringen (2023) *Strategy for Subsea Infrastructure Protection.* [Internal summary – cited in OECD Peer Review].
51. Regjeringen (2023) *Nordic Digital Security Cooperation Outlook.*
52. NSM (2023) *Cross-sector Responsibilities in National Crisis Management.*

> Enterprise use of AI is accelerating, but much of this infrastructure is located abroad. That creates a significant vulnerability if access were to be denied.
>
> **–Risto Siilasmaa**
> **Founder of F-Secure and WithSecure Corporations, chair of WithSecure and former chair of Nokia**

4.2 Future considerations

The outage scenarios in Chapter 3 reveal more than technical fragility—they expose systemic blind spots in governance, coordination, and operational readiness. Scenario 2 shows how fallback mechanisms begin to unravel within hours. Scenario 3 makes clear that without regional alignment and real-time response capabilities, institutional trust and national stability are at risk.

To meet the scale of these challenges, Norway must shift from fragmented preparedness to integrated resilience—anchored in national security strategy, infrastructure design, crisis governance, and cross-border cooperation. This will require moving beyond current mitigation efforts toward high-impact, system-wide transformation.

Four structural priorities must guide this shift:

1. **Digital infrastructure must be treated as a core pillar of national security**
   Cyber and telecom systems are recognized as critical but must now be fully integrated into national crisis budgets, risk assessments, and defense planning. Inter-agency coordination must improve, and systemic vulnerabilities—like single-route dependencies or outdated legacy systems—must be mapped and addressed.

2. **Resilience strategy must go beyond cables to include software and control systems**
   While Norway has diversified its international routes and reinforced domestic fiber, key gaps remain. Vulnerabilities in rural areas, chokepoints at landing stations, and overdependence on specific software platforms could trigger cascading failures. Infrastructure design must support dynamic rerouting and prioritization of emergency services—potentially requiring limited, temporary exceptions to net neutrality under crisis conditions.

3. **Crisis response must be coordinated in real time and stress-tested across sectors**
   Institutional tools like Varsling and satellite fallback systems exist, but Norway needs unified dashboards, standardized escalation protocols, and national simulations that integrate telecom, energy, and civil protection. The Telecom Preparedness Council should be embedded in national crisis response playbooks.

4. **Resilience must be regional by design, not national by assumption**
   Norway's geographic exposure—longer cables, dispersed infrastructure, and slower repair times—makes it more vulnerable than its Nordic neighbors. Regional fallback capacity, shared repair teams, and joint routing protocols are essential. Norway must also embrace distributed sovereignty: hosting key functions (e.g. routing, storage, data centers) across trusted allied countries to ensure continuity under stress.

The following three initiatives are designed to operationalize these principles—providing a coherent roadmap toward a more resilient, secure, and sovereign digital future.

Key Strategic Initiatives to Redefine Norway's Digital Resilience

A Digital resilience certification

Although Norway is not formally bound by EU directives such as NIS2 or CER, it is actively aligning with them through its national legal framework complemented by the Security Act. In 2023, the Ministry of Justice confirmed that the Critical Entities Resilience (CER) Directive is considered EEA-relevant and acceptable for Norwegian implementation[53]. To advance preparedness, the National Security Authority (NSM) should lead the development of a national certification program to assess and verify the resilience of digital infrastructure across different sectors—drawing inspiration from both CER and NIS2[54]. To support adoption and a culture of resilience, the **Norwegian Government** and **the authorities** should act as an **enabler** and **play an active role** in helping companies build the required capabilities—through subsidies for smaller and regional operators with limited funds and capabilities, technical guidance, co-funding schemes, and shared infrastructure models. Without this support, systemic resilience goals risk falling short.

The certification should go beyond policy compliance and test actual operational resilience under stress. It would apply to telecom carriers, cloud platforms, data centers, and eID providers. Key criteria should include proven business continuity plan, dual-homing, automated failover, off-grid continuity, physical security, and incident response coordination. Standards must also address perimeter control, backup power, and environmental safeguards.

As AI and automation become embedded in critical services, the framework must address new risk surfaces. Certified operators should be required to follow structured model governance protocols, ensuring that AI models—especially open-source variants—are secure, traceable, and auditable. Local, air-gapped recovery systems must be in place to protect data during major incidents. Secure rollback processes, fault isolation, and misconfiguration scanning should be mandatory components of certified infrastructure.

And importantly, the certification must be designed in a **non-bureaucratic and accessible way** - simple to adopt, transparent to assess, and practical for operators of all sizes to implement. Its purpose should be to raise resilience, **not increase administrative burden**.

Over time, the certification should evolve from a checklist of best practices into a **national benchmark for proven continuity, operational trust, and digital sovereignty**—capable of demonstrating that Norway's critical infrastructure can remain functional even under sustained and complex disruption.

53. Regjeringen.no (2023). *Liste over vesentlige tjenester under CER-direktivet.* Ministry of Justice and Public Security.
54. DSB (2023). *CER og NIS2-direktivene: Hva betyr de for samfunnssikkerheten?* Directorate for Civil Protection.

> If we want a higher standard of protection, someone has to pay for it. Expecting private operators to upgrade 500 sites alone to Level 4 physical security is unrealistic. Co-investment is the only viable path.
>
> **–Søren Henriksen**
> **Quantum Lead, GlobalConnect**

> It makes little sense to think about telecom or subsea cables only in national terms—these are fundamentally regional infrastructures.
>
> **–Tobias Liebetrau**
> **Research at the Centre for Military Studies, Department of Political Science, UNICPH**

B Nordic Digital Resilience Shield

Digital threats ignore borders—and so must resilience. Norway should actively support the creation of a Nordic Digital Resilience Shield: a structured multilateral agreement to coordinate protection, redundancy, and recovery of shared digital infrastructure across the region. Among the three initiatives, the Nordic Digital Resilience Shield is the pivotal measure— a joint government effort that translates policy ambition into operational, cross-border resilience.

Unlike existing frameworks, the Shield would emphasize operational continuity, not just strategic dialogue. Key features could include:

- **Joint surveillance** of subsea cables and terrestrial corridors through pooled naval patrols, intelligence exchange, and real-time monitoring systems.
- **Cross-border failover for digital identity and e-government services,** enabling the continuity of essential public functions—such as health access, payments, and emergency alerts—through pre-designated, secure infrastructure hosted in trusted neighboring countries. All sensitive personal data would remain physically located within the country; only orchestration layers and access continuity mechanisms would rely on cross-border fallback nodes—connected through resilient international links (e.g. dedicated fiber corridors, satellite, or institutional gateways)[55].

55. As implemented by Estonia and Monaco through their "data embassy" in Luxembourg, which ensures continuity while maintaining national data jurisdiction.

- **Mutual DNS** (Translation of website names into IP addresses, essential for directing traffic to the correct server) **caching and agreed routing paths** ensuring that key Norwegian digital services (like health, payments, or public websites) remain reachable even if the country's own systems are attacked or go offline. By storing critical network metadata and pre-agreeing routing paths with trusted Nordic partners, essential traffic could bypass domestic failures—without transferring protected data across borders.
- **Harmonized crisis escalation protocols** and shared playbooks for coordinated regional response.
- **Sovereign cloud enclaves or regional trusted zones** for emergency backup and public-sector metadata hosting, ensuring compliance with Norwegian privacy law.

The Shield would draw inspiration from established Nordic security cooperation structures—such as NORDEFCO and the Nordic Battle Group—but apply that same spirit of operational readiness to the digital domain. For Norway, with its dispersed infrastructure and long-haul fiber dependency, regional fallback mechanisms are not optional—they are critical to continuity. Execution should be validated at **cross-sector** and **cross-border** levels; sector-specific checks remain within national verification programs, while the Shield focuses on regional orchestration.

As the paper's simulated scenarios, but also real life events, have shown, the ripple effects of digital failure in one country can be felt far beyond its borders. Planning for continuity together is no longer a luxury. It is a strategic necessity.

> Ukraine proved the point—you can't talk about digital sovereignty without also having trusted cross-border backups.
>
> **–Tobias Liebetrau**
> **Research at the Centre for Military Studies, Department of Political Science, UNICPH**

> Nordic countries share to some extent similar threat landscapes. Countries like Israel and Singapore show what's possible when private and public actors work together on aggregate cyber robustness and systemic resilience.
>
> **–Thomas Flarup**
> **Executive VP at Terma, former Head of the Danish Centre for Cyber Security (CFCS), and former Management Board Member at ENISA**

National "Black Sky" simulations

While Norway conducts sector-specific preparedness exercises, it currently lacks a **comprehensive, recurring national simulation** to test how the country would respond to a **prolonged, cross-sector digital disruption**[56]. A structured "Black Sky" Exercise Series would address this gap—designed to expose systemic vulnerabilities through realistic, multi-day stress scenarios that extend beyond the scope of tabletop drills[57].

These exercises should run for prolonged periods of time and include participation from across the national critical infrastructure landscape: telecoms, energy, finance, healthcare, transportation, municipalities, and emergency services. Unlike conventional rehearsals, Black Sky simulations would test fallback communications, manual continuity procedures, offline workflows, and interagency coordination under live operational pressure. The focus would be not just on preparedness plans—but on proving whether those plans can hold under sustained stress.

Each scenario should reflect credible, real-world risks already observed or projected for Norway. These include: cyber-physical sabotage targeting control systems; undersea cable cuts that sever international routing; loss of access to foreign cloud platforms critical to national operations; and **simultaneous failures** in power, telecom, and public safety systems. Such simulations would surface hidden interdependencies across sectors, reveal assumptions that break down in crisis, and help identify where institutions need to invest in improved protocols, staffing, and tools.

Exercises should explicitly test resilience at three complementary levels—sector, cross-sector, and cross-border. At the sector level, operators validate their own continuity plans under isolation; at the cross-sector level, joint simulations expose dependencies and coordination gaps between energy, telecom, finance, health, and transport; and at the cross-border level, Nordic partners participate to test regional coordination and shared fallback mechanisms.

Over time, the Black Sky program should evolve to include **Nordic and transnational partners**, reflecting the reality that most major digital disruptions will not stop at national borders. Shared infrastructure—such as cloud services, cross-border cables, and routing systems—demands **shared response frameworks**. Regional resilience must be **rehearsed, not just planned**.

Establishing this program would signal a shift in Norway's posture—from reactive preparedness to proactive, system-level readiness. It would build institutional confidence, strengthen public trust, and ensure that Norway is not only protected—but proven capable—of functioning through the most severe disruptions to its digital backbone.

> The tricky part is getting all the operators and authorities to see that what looks like minor interference might be actually part of a much larger strategy.
>
> **–Jacob Kaarsbo**
> **Security Policy Advisor And former Head of Analytics at the Danish Defence Intelligence Agency**

56. NSM (2024). *Digitalsikkerhetsstrategi – status og videreutvikling.* National Security Authority.
57. OECD (2023). *Peer Review of Norway's National Digital Resilience.*

Securing Norway's digital future demands a holistic transformation—moving from piecemeal upgrades to system-wide fortification. The country must hardwire resilience into its infrastructure, governance, and crisis management—not only to protect its own connectivity, but to support a more secure and connected European digital system.

This shift requires embedding shared responsibility into Norway's DNA—spanning sectors, borders, and governance frameworks. It also requires investments in critical capabilities that the market may not find profitable—like cross-border data centers or backup systems. **Public funding will be essential, because digital resilience is no longer just a technology. It is a matter of national security.**

Operators must reduce risk that the digital infrastructure is disrupted by single points of failure. This means building redundancy with Norway's regional allies—not just in physical infrastructure, but also in software, platforms, and data storage. These backups should cross borders, too. For example, Norway could place key systems in trusted neighboring countries like Sweden, creating stronger regional safety nets.

The vulnerabilities Norway faces are not unique. But its geographical position, regional credibility, and technical capacity offer a strong foundation to contribute meaningfully. By helping shape a shared Nordic-European digital security alliance, Norway can reinforce collective continuity in the face of increasingly systemic risks.

Our parallel whitepapers on **Denmark** and **Sweden** reveal similar trends. All three countries face many of the same risks—from overreliance on external platforms to cross-border chokepoints to uneven crisis coordination. While each country's situation is different, the picture is clear: **strengthening digital resilience in the Nordics cannot be achieved through national action alone. It will require collective solutions, built on trust, shared investment, and coordinated action.**

Authors

Martin Lippert
Group CEO

Per Morten Torvildsen
EVP NetCo

Sofia Lisa Dinesen
SVP Group Strategy and M&A, Sustainability,
Communications and Public Affairs

Acknowledgements

We extend our sincere thanks to the individuals whose insights and perspectives enriched the development of this whitepaper. Their contributions helped ground the analysis in real-world experience and strategic foresight.

We are particularly grateful to:

- **Olav Lysne,** Professor at the University of Oslo, for his critical reflections on digital infrastructure fragility and the societal dimensions of resilience.
- **Tomas Lamanauskas,** Deputy Secretary-General of the International Telecommunication Union (ITU), for highlighting our common responsibility for digital resilience.
- **Risto Siilasmaa,** founder of F-Secure and WithSecure Corporations, chair of WithSecure and former chair of Nokia for his foresight on AI infrastructure risks and sovereignty.
- **Jacob Kaarsbo,** Security Policy Advisor, for his candid perspective on hybrid threats and institutional readiness.
- **Søren Henriksen,** EVP at GlobalConnect, for his comprehensive view on infrastructure vulnerabilities, sector-level readiness, and the importance of public-private coordination in enhancing resilience
- **Thomas Flarup,** Executive VP at Terma, former Head of the Danish Centre for Cyber Security (CFCS), and former Management Board Member at ENISA ENISA for his insights on structural exposure, sectoral fragmentation, and the operational challenges of building system-wide digital resilience.
- **Tobias Liebetrau,** Research at the Centre for Military Studies, Department of Political Science, UNICPH for his reflections on cross-border backup and the role of relational trust in resilience.

We also acknowledge the many professionals across sectors—public, private, and academic—whose input and engagement helped shape the scenarios and recommendations presented in this report.

While the views expressed in this paper remain those of the authors, these contributions were essential in helping ensure the work reflects the urgency and complexity of today's digital resilience challenge.

Bibliography

- Bapty, R. (2023). Rising 5G Availability & Consistency Boosts Norwegians' Overall Experience. *Opensignal*, September 11. https://www.opensignal.com.
- Business Norway. (2025). *The Rise of Remote Patient Monitoring*. https://businessnorway.com.
- DSB. (2023). *CER og NIS2-direktivene: Hva betyr de for samfunnssikkerheten?*
- ECB. (2023). *Cloud Outsourcing and Financial Stability Risks.*
- ENISA & European Commission. (2023). *Joint Report on Infrastructure Single Points of Failure.*
- ENISA. (2023). *Cyber Crisis Management: Lessons from Cross-Border Exercises.*
- Energifakta Norge. (2023). *Kraftproduksjon i Norge.*
- European Commission. (2022). *Directive (EU) 2022/2557 on the Resilience of Critical Entities (CER).*
- European Commission. (2024). *Digital Decade 2024: Broadband Coverage in Europe 2023.* https://digital-strategy.ec.europa.eu.
- European Commission. *(2024). DESI Indicators: 5G Coverage (2024).*
- European Commission. (2023). *Strategy for Subsea Infrastructure Protection*. [internal summary, cited in OECD Peer Review]
- Eurostat. (2020). *How Much Do Households Spend on Communications?*
- Grand View Research. *(2024). Norway Telehealth Kiosk Market Size & Outlook, 2023–2030.*
- Indra Sistemas. (2025). *23 Norwegian Airports to Be Remotely Operated.* https://www.indracompany.com.
- Invest in Norway. (2025). *Power System in Norway.* https://businessnorway.com.
- Justis- og beredskapsdepartementet. (2024). *Regjeringen styrker kontantberedskapen.*
- Mobile Europe. (2025). Norway on Course for 100Mbps for All by End 2025, May 7. https://www.mobileeurope.co.uk.
- Norges Bank. (2024). *Retail Payment Services 2023,* Memo 1/2024.
- Norwegian Centre for E-health Research. (2023). *Telehealth Experiences from Norway – Where Do We Go From Here?*
- Norwegian Datacenter Industry. (2024). *The Data center Industry in Norway 2023–2024.* https://norwegian.dcindustry.no.
- Norwegian Directorate for Education and Training – Udir. (2023). *Digitalisation in the Norwegian Education Sector.*
- NOU – Norges offentlige utredninger. (2015). *Digital sårbarhet – sikkert samfunn (NOU 2015:13).*
- NVE – Norges vassdrags- og energidirektorat. (2023). *Kraftberedskapsplan og sårbarhetsanalyse.*
- NSM – Norwegian National Security Authority. (2023). *Cross-sector Responsibilities in National Crisis Management.*
- NSM. (2024). *Cybersecurity Skills Gap in Norway: National Assessment and Strategy Update.*

- NSM. (2024). *Digitalsikkerhetsstrategi – status og videreutvikling.*
- NSM. (2025). *National Cyber Threat Assessment – Telecom Sector.*
- NSM. (2025). *NCC-NO: Building Capacity for Critical Infrastructure.*
- OECD. (2023). *Peer Review of Norway's National Digital Resilience.*
- Peter B. de Selding. (2022). Update: Undersea Fiber Link to Svalbard Returns to Full Redundant Service. *Space Intel Report.*
- Ponemon Institute. (2023). *Cost of Data center Outages.*
- Regjeringen. (2023). *Digitaliseringsstrategi 2023–2030.*
- Regjeringen. (2023). *Nordic Digital Security Cooperation Outlook.*
- Regjeringen. (2023). *OECD Peer Review of Norwegian Digital Resilience.*
- Regjeringen. (2024). *Support and Cooperation in National Contingency Planning.*
- Regjeringen.no. (2023). *Liste over vesentlige tjenester under CER-direktivet.* Ministry of Justice and Public Security.
- Science Norway. (2024). *People Are Receiving More Digital Healthcare in Europe.*
- Statnett. (2022). *Sikkerhetsstrategi for kraftsystemet [Security Strategy for the Power System].*
- Statistics Norway. (2023). *ICT Use and Infrastructure Indicators.*
- Telenor. (2024). *Telenor Targets Growing Threats with Cybersecurity Company.* Mobile World Live.
- Telenor. (2024). *The NIS2 Clock Is Ticking in the EU – Where Will Compliance Take Us in the Nordics?* Telenor Digital Security.
- Transparency International. (2023). *Corruption Perceptions Index: Norway.*
- European Commission. *EU Trade Relations with Norway: Facts, Figures and Latest Developments.*
- Regjeringen. (2023). *Strategy for Subsea Infrastructure Protection.*


GlobalConnect