STRATEGIC COUNTRY REPORT: NORWAY

Automated Strategic Analyst (v2.2 Parallel)

12 February 2026

Contents

Chapter 1

Geopolitics

Executive Summary

Norway occupies a critical geostrategic position as a guardian of the High North and a key NATO ally, a role that increasingly extends into the digital domain. The nation's geopolitical standing is defined by its active integration into European security initiatives and its pivotal role in Arctic security, where it faces rising tensions and hybrid threats [A Strategic Compass for Security and Defence - EEAS]. While Norway demonstrates robust digital governance and a strong commitment to digital sovereignty through alignment with EU frameworks like Gaia-X [A German Digital Grand Strategy - DGAP], its critical infrastructure faces distinct vulnerabilities.

Intelligence indicates that Norway's subsea infrastructure is susceptible to sabotage, evidenced by the 2022 severing of the fiber optic cable connecting mainland Norway to Svalbard [Countering Russia's Hybrid Threat In Arctic]. A significant strategic challenge lies in the ownership structure of this infrastructure; critical cable landing stations and fiber assets are predominantly privately held, creating legal impediments to direct state-led protection [Seabed Warfare Against Data Cables - Wilson Center]. Furthermore, network analysis reveals a potential "kill switch" risk within the domestic telecommunications sector, specifically regarding Telia Norge AS, which exhibits 100% dependency on a single foreign upstream provider based in Sweden [Internal Graph]. Consequently, Norway's digital geopolitics is characterized by a tension between high-level democratic governance and acute physical and logical infrastructure vulnerabilities.

1.1 Strategic Positioning and Alliances

Norway's geopolitical strategy is deeply entrenched in its alignment with NATO and the European Union, particularly regarding security and defense in the Arctic region. The nation contributes actively to global peace and security efforts, viewing its energy transition and secure energy systems as foundational to its digital infrastructure resilience [Global Energy Transition Gains Ground… - WEF].

In the digital sphere, Norway is pursuing "Digital Sovereignty" to maintain national control

over digital assets and economies. This includes the development of national AI strategies and the exploration of self-sovereign cloud solutions. Norway actively participates in European initiatives such as the Important Project of Common European Interest on Next Generation Cloud Infrastructure and Services (IPCEI-CIS) and Gaia-X, aiming to reduce international connectivity dependencies and foster domestic innovation [International Conference on Digital Sovereignty (ICDS) 2024 - IFE]. Despite these efforts, Norway does not currently serve as a primary "Digital Gateway" for neighboring countries, although it is a signatory to European declarations aiming to strengthen international connectivity [Digital Day 2021… - EC Digital Strategy].

1.2 Critical Infrastructure Vulnerability and Ownership

The security of Norway's physical digital infrastructure is a primary concern. The Baltic Sea and the High North are increasingly viewed as "high risk" zones for infrastructure sabotage [Swedish PM says Baltic sea now 'high risk'… - The Guardian]. The vulnerability of this network was underscored by the disruption of the subsea cable to Svalbard in early 2022, highlighting the fragility of connectivity to strategic outposts [Countering Russia's Hybrid Threat In Arctic].

A complicating factor for national security planners is the ownership structure of these assets. Norway's critical submarine cable landing stations and cross-border fiber infrastructure are primarily privately held. Intelligence suggests that this private ownership model creates legal and operational hurdles for the state to implement comprehensive protection and regulation regimes effectively [Seabed Warfare Against Data Cables - Wilson Center].

1.3 Logical Network Dependencies and Risks

Analysis of Norway's logical network topology reveals specific dependencies that pose strategic risks. While the domestic network ecosystem includes major players like GlobalConnect and Telenor, specific operators show concerning reliance patterns.

High-Risk Dependency: Technical analysis identifies a potential single point of failure for **Telia Norge AS (GET-NO)**. This entity exhibits a **100% dependency (`d.hege` = 1.0)** on a single foreign upstream provider: **TWELVE99 Arelion Sweden AB** (formerly Telia Carrier). This configuration presents a "kill switch" risk, where the disruption of this specific cross-border link to Sweden could sever international connectivity for a significant portion of the network's user base [Internal Graph].

Domestic Interdependence: The top Autonomous System Numbers (ASNs) in Norway by incoming dependency—indicating networks that others rely upon heavily—include CLOUDFLARENET, GlobalConnect, and CDN77. These entities form the backbone of Norway's internal digital routing architecture [Internal Graph].

1.4 Digital Governance and Resilience

Norway consistently ranks high on international indices for digital governance and internet freedom, reflecting its democratic geopolitical alignment. The UN E-Government Survey highlights Norway's robust development of national digital portals and its focus on bolstering cybersecurity [E-Government Survey 2024].

However, resilience remains a challenge. The nation has faced significant cyber incidents, including attacks on parliamentary systems and the industrial giant Norsk Hydro. These events have driven a strategic focus on upgrading networks (including 5G) and enhancing cybersecurity measures to protect critical functions [Shaping Norway's Digital Future | OECD]. The Norwegian National Security Authority (NSM) is central to these efforts, tasked with operationalizing the country's digital sovereignty objectives in the face of hybrid threats [International Conference on Digital Sovereignty (ICDS) 2024 - IFE].

References

- [Internal Graph] Internal Knowledge Graph.
- [A German Digital Grand Strategy - DGAP] A German Digital Grand Strategy (https://dgap.org/en/research/publications/german-digital-grand-strategy)
- [A Strategic Compass for Security and Defence - EEAS] A Strategic Compass for Security and Defence - EEAS (https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en)
- [Countering Russia's Hybrid Threat In Arctic] Countering Russia's Hybrid Threat In Arctic (https://europeanleadershipnetwork.org/wp-content/uploads/2023/12/23_11_22_Countering-Russias-Hybrid-Threats-in-the-Arctic15_ES_EK40.pdf)
- [Digital Day 2021… - EC Digital Strategy] Digital Day 2021: Europe to reinforce internet connectivity with … (https://digital-strategy.ec.europa.eu/en/news/digital-day-2021-europe-reinforce-internet-connectivity-global-partners)
- [E-Government Survey 2024] E-Government Survey 2024 (https://desapublications.un.org/sites/default/fi
09/%28Web%20version%29%20E-Government%20Survey%202024%201392024.pdf)
- [Global Energy Transition Gains Ground… - WEF] Global Energy Transition Gains Ground, but Security and Capital … (https://www.weforum.org/press/2025/06/global-energy-transition-gains-ground-but-security-and-capital-challenges-persist/)
- [International Conference on Digital Sovereignty (ICDS) 2024 - IFE] International Conference on Digital Sovereignty (ICDS) 2024 - IFE (https://ife.no/en/event/international-conference-on-digital-sovereignty-icds-2024/)
- [Seabed Warfare Against Data Cables - Wilson Center] Seabed Warfare Against Data Cables - Wilson Center (https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/Seabe
Warfare-Cables%20%281%29.pdf)
- [Shaping Norway's Digital Future | OECD] Shaping Norway's Digital Future | OECD (https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/shaping-

norway-s-digital-future_d6492358/d3af799c-en.pdf)

- [Swedish PM says Baltic sea now ‘high risk’… - The Guardian] Swedish PM says Baltic sea now ‘high risk’ after suspected cable … (https://www.theguardian.com/world/2024/nov/27/swedish-pm-says-baltic-sea-now-high-risk-after-suspected-cable-sabotage)

Chapter 2

Infrastructure

Executive Summary

Norway maintains a highly advanced telecommunications infrastructure, characterized by near-ubiquitous 5G coverage and robust fiber-optic penetration. As of recent assessments, the nation has achieved a 5G population coverage rate of 99.0%, positioning it as a leader in next-generation mobile connectivity [Q3-Source 2]. In the fixed-line sector, Norway ranks among the top European nations, with Fiber to the Home/Building (FTTH/B) penetration exceeding 50% as of late 2021 [Q1-Source 1].

The competitive landscape is defined by four primary operators—Altibox, Ice Communication, Telia, and Telenor—who recently secured critical spectrum licenses in the 2.6 GHz and 3.6 GHz bands to support continued network expansion [Q4-Source 1]. Despite this maturity, the sector faces strategic imperatives to modernize legacy systems and address potential spectrum scarcity to sustain economic growth [Q11-Source 2]. National goals remain focused on high-speed broadband universality, aiming to close remaining gaps in rural and industrial access through public-private partnership models [Q9-Source 4].

2.1 Mobile Network Infrastructure and Spectrum Allocation

Norway's mobile infrastructure is underpinned by aggressive 5G deployment and strategic spectrum management. The most recent 5G spectrum auction concluded with the allocation of frequencies in the 2.6 GHz and 3.6 GHz bands, generating approximately NOK 3.89 billion in revenue. These allocations are critical for capacity and speed, distributed among four key operators:

- **Altibox AS:** Secured 50 MHz in the 2.6 GHz band and 100 MHz in the 3.6 GHz band.
- **Ice Communication Norge AS:** Allocated 80 MHz in the 3.6 GHz band.
- **Telia Norge AS:** Won 2 x 30 MHz in the 2.6 GHz band and 100 MHz in the 3.6 GHz band.

- **Telenor Norge AS:** Secured the largest blocks, with 2 x 40 MHz in the 2.6 GHz band and 120 MHz in the 3.6 GHz band [Q4-Source 1].

While the deployment of mid-band and low-band spectrum has facilitated 99.0% population coverage [Q3-Source 2], specific intelligence regarding the deployment of high-band (mmWave) spectrum remains limited [Q3-Source 1].

2.2 Fixed-Line and Broadband Architecture

Norway's fixed-line infrastructure is heavily oriented toward fiber optics. The country is one of only seven European nations to surpass a 50% penetration rate for FTTH/B [Q1-Source 1]. This aligns with long-standing national broadband goals, which targeted 100 Mbit/s speeds for at least 90% of households by 2020 [Q9-Source 4].

The core of Norway's internet traffic exchange is anchored by the **Norwegian Internet Exchange (NIX)** located in Oslo. As the primary national Internet Exchange Point (IXP), NIX facilitates peering between ISPs, content providers, and enterprise networks, although specific details on secondary peering locations remain sparse [Q5-Source 1].

To address connectivity in remote communities and industrial zones where private investment is not financially viable, the state relies on frameworks that encourage Public-Private Partnerships (PPPs). These models are essential for expanding the national fiber backbone into underserved areas, ensuring that the benefits of digital infrastructure are not confined to urban centers [Q9-Source 1].

2.3 Strategic Challenges and Opportunities

Despite its advanced status, Norway's infrastructure sector faces challenges common to mature digital economies. Potential impediments to future growth include the management of legacy network technologies and the financial burdens associated with high spectrum auction costs, which can constrain capital available for physical build-outs [Q11-Source 2]. Furthermore, regulatory frameworks must evolve to prevent bureaucratic delays in deploying new wireless facilities [Q11-Source 2].

Conversely, significant opportunities exist in leveraging this infrastructure for **Digital Public Infrastructure (DPI)**. By strengthening foundational digital systems—such as identity and data sharing platforms—Norway can accelerate inclusive digital transformation [Q11-Source 4]. Additionally, there is a strategic opening to align infrastructure development with climate action, utilizing digital technologies to "green" the energy consumption of the ICT sector itself [Q11-Source 1].

References

- [**Q1-Source 1**] FTTH/B Global Ranking 2022 - FTTH Council Europe (https://www.ftthcouncil.eu/know

centre/all-publications-and-assets/1463/ftth-b-global-ranking)
- [**Q3-Source 1**] The Envy of Europe: Nordics Lead in 5G Availability and Network … (https://www.ookla.com/articles/nordics-5g-q1-2025)
- [**Q3-Source 2**] 5G Observatory report 2025 - Shaping Europe's digital future (https://digital-strategy.ec.europa.eu/en/policies/5g-observatory-2025)
- [**Q4-Source 1**] The Norwegian 5G auction has concluded - Nkom (https://nkom.no/aktuelt/the-norwegian-5g-auction-has-concluded)
- [**Q5-Source 1**] List of Internet exchange points - Wikipedia (https://en.wikipedia.org/wiki/List_of_Inter
- [**Q9-Source 1**] Innovative business models for expanding fiber-optic networks and … (https://documents1.worldbank.org/curated/en/674601544534500678/pdf/Main-Report.pdf)
- [**Q9-Source 4**] ARCTIC BROADBAND (https://arcticeconomiccouncil.com/wp-content/uploads/2017/03/AEC-Report_Final-LR.pdf)
- [**Q11-Source 1**] Digital Transformation Overview: Development news, research, data (https://www.worldbank.org/en/topic/digital/overview)
- [**Q11-Source 2**] Delivering Digital Infrastructure Advancing the Internet Economy (https://www3.weforum.org/docs/WEF_TC_DeliveringDigitalInfrastructure_InternetEconomy_Repor
- [**Q11-Source 4**] Digital Public Infrastructure and Development: A World Bank Group … (https://documents1.worldbank.org/curated/en/099031025172027713/pdf/P505739-84c5073b-9d40-4b83-a211-98b2263e87dd.pdf)
- [**IYP-GRAPH**] Internal Knowledge Graph

Chapter 3

Market

Executive Summary

The Norwegian telecommunications market is characterized by a distinct oligopolistic structure, resulting in a high-cost environment for domestic consumers compared to regional peers. Intelligence indicates that the market is "uniquely concentrated" relative to other Nordic nations, primarily dominated by two incumbent operators, Telenor and Telia [Source 1]. This duopoly allows for sustained high Average Revenue Per User (ARPU), recorded at approximately €17.50 as of December 2023, despite Norwegian consumers exhibiting the lowest mobile data usage in the Nordic region [Source 1].

While network infrastructure remains robust, with Norway ranking 30th globally for both mobile and fixed broadband speeds [Source 3], the competitive landscape is stagnant. High entry barriers and the slow expansion of the third operator, Ice, have prevented significant price disruption [Source 3]. Consequently, domestic mobile data pricing remains significantly higher than rates available to foreign visitors roaming on the same networks, highlighting a disparity driven by market structure rather than technical cost [Source 2].

3.1 Market Structure and Competitive Landscape

The Norwegian telecom sector exhibits strong oligopolistic tendencies, with market power heavily consolidated among legacy providers. Telenor, the market leader, captures approximately 47% of the market's EBITDA margin, underscoring its dominant financial position [Source 3]. Together, Telenor and Telia control 77% of bundled mobile subscriptions, effectively dictating market dynamics [Source 3].

Efforts to introduce a third competitive force have yielded limited results to date. The third-largest player, Ice, continues to strengthen its position but remains dependent on national roaming agreements. Intelligence suggests that Ice's expansion has been too slow to sufficiently discipline the established operators or force a shift in pricing strategies [Source 3]. This structural rigidity is identified as the primary root cause for the lack of price competition and the

high revenue-per-gigabyte yield enjoyed by incumbents [Source 1].

3.2 Pricing Dynamics and Consumer Costs

Pricing analysis reveals a significant premium on domestic mobile data services. While the global average price for 1GB of data was approximately USD 2.59 in early 2024, and Western European averages hovered around USD 2.08 [Source 3][Source 4], Norwegian domestic entry-level plans are notably expensive. Open-source intelligence indicates that the cheapest domestic subscription offering 1GB of data costs between 99 and 119 NOK (approx. USD 9.00 - 11.00), a stark contrast to the lower rates available in neighboring Finland [Source 2].

A notable anomaly exists wherein foreign visitors using roaming SIMs in Norway often secure significantly lower rates (e.g., 10GB for roughly 77 NOK) than Norwegian residents paying for local subscriptions [Source 2]. This pricing structure supports the high ARPU observed in the market. The high ARPU is not driven by high consumption—Norwegians consume the least data in the Nordics—but rather by high unit costs imposed by the concentrated market structure [Source 1].

3.3 Infrastructure and Network Performance

Despite the high costs, the quality of service in Norway remains competitive on a global scale, though not market-leading. According to the Ookla Speedtest Global Index, Norway ranks 30th worldwide for both fixed broadband and mobile network speeds.

- **Mobile Performance:** The median mobile download speed is recorded at 114.48 Mbps, with a median upload speed of 14.48 Mbps [Source 1][Source 3].
- **Fixed Broadband:** The median fixed broadband download speed is 112.45 Mbps, with a symmetrical median upload speed of 112.45 Mbps [Source 1][Source 3].

While these metrics indicate a capable infrastructure suitable for modern digital demands, the market lacks the aggressive performance-based competition seen in top-tier markets. There is currently no specific intelligence available regarding 5G availability or consistency awards for Norwegian operators in global comparison reports for 2023, further suggesting a market that is stable but not currently distinguishing itself through exceptional technological leaps [Source 1].

References

- [Source 1] Assessment of Norwegian mobile revenues in a Nordic context 2024 (https://www.regjeringen.no/contentassets/311eeb54f87341d187b04361c7f62038/assessment-of-norwegian-mobile-revenues-in-a-nordic-context-by-tefficient-5-sep-2024.pdf)
- [Source 2] Why is it much more expensive to be a Norwegian mobile customer … (https://www.reddit.com/r/norge/comments/1n85g3u/hvorfor_er_det_mye_dyrere_%C3%A5_v%C3%

- [Source 3] Analysis of the market for access and call origination on public … (https://nkom.no/ekom-markedet/markeder/marked-15-tilgang-til-mobilnett/_/attachment/download/7
0be5-4ef5-80e4-c9d9492c68fe:22aa94db94c7c1bb350621ceedd62e4ecce1e30e/Annex%201%20Analysis%20c
- [Source 4] The Cost of 1GB Mobile Data Worldwide - Voronoi (https://www.voronoiapp.com/money/The-Cost-of-1GB-Mobile-Data-Worldwide-2884)
- [Source 5] The Cost of 1GB Of Mobile Data in 237 Countries - Broadband Deals (https://bestbroadbanddeals.co.uk/mobiles/worldwide-data-pricing/)
- [Source 6] Speedtest Global Index – Internet Speed around the world (https://www.speedtest.net/global-index)
- [Source 7] Norway's Mobile and Broadband Internet Speeds - Speedtest Global … (https://www.speedtest.net/global-index/norway)
- [Source 8] 5G Global Mobile Network Experience Awards 2023 | Opensignal (https://cdn.opensignal.com/public/data/reports/national/data-2436/2023_5gglobalmobilenetworkexpe
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 4

Localization

Executive Summary

Norway's localization landscape is defined by a rigorous adherence to digital sovereignty, driven by its membership in the European Economic Area (EEA) and strict alignment with the General Data Protection Regulation (GDPR) [Source 1 (Q1)]. The strategic environment is characterized by a tension between the operational necessity of utilizing foreign hyperscale cloud providers—primarily Microsoft Azure and AWS—and the legal imperatives to protect national data from extraterritorial reach, specifically regarding US surveillance laws like FISA 702 and the CLOUD Act [Source 1 (Q1)].

To mitigate these risks, the Norwegian government has implemented a strategy prioritizing the hosting of critical e-government services (e.g., health registries, tax records) within domestic borders [Source 1 (Q5)]. This has necessitated the establishment of local cloud regions by global providers, such as Microsoft's "Norway East" and "Norway West" [Source 2 (Q5)]. While the .no domain serves as a robust, trusted symbol of national digital identity requiring physical presence for registration [Source 4 (Q8)], the legal framework remains precarious due to the instability of international data transfer mechanisms like the EU-US Data Privacy Framework [Source 1 (Q1)]. Consequently, Norway's strategic posture is shifting toward "trusted architects of virtual sovereignty" and multi-cloud approaches to prevent vendor lock-in and ensure compliance with European privacy standards [Source 5 (Q10)].

4.1 Legal Framework and Data Sovereignty

Norway's legal framework for data localization is fundamentally shaped by its EEA obligations and the GDPR, creating a complex compliance environment for cross-border data flows. The primary strategic concern for Norwegian intelligence and regulatory bodies is the conflict between European privacy rights and US surveillance legislation.

Extraterritorial Risks and US Law Norwegian entities face significant legal uncertainty regarding data transfers to the United States. The Norwegian Data Protection Authority (Datatil-

synet) has issued explicit warnings regarding the stability of the EU-US Data Privacy Framework (DPF), citing the potential for revocation similar to the invalidation of the Safe Harbor and Privacy Shield frameworks [Source 1 (Q1)]. The core conflict lies in US laws such as FISA 702 and the CLOUD Act, which allow US authorities to compel American technology companies to provide data regardless of whether it is stored on servers in Norway or elsewhere [Source 1 (Q1)]. This extraterritorial reach is viewed as incompatible with GDPR requirements, as it exposes Norwegian data to foreign government access without adequate judicial redress [Source 1 (Q1)].

Regulatory Enforcement and Compliance Datatilsynet maintains a strict enforcement posture. Following European trends, the authority has scrutinized the use of US-based services (e.g., Google Analytics) that necessitate data transfers, warning that such practices may violate GDPR [Source 1 (Q1)]. To maintain compliance, Norwegian entities utilizing foreign infrastructure must often rely on Standard Contractual Clauses (SCCs) accompanied by rigorous "transfer impact assessments" (TIAs) to evaluate the risk of public authority access in the third country [Source 2 (Q1)]. Furthermore, the National Security Act (2019) provides a mechanism for the government to screen and potentially block foreign ownership or control of critical infrastructure, reflecting a broader concern for national security beyond mere data privacy [Source 3 (Q9)].

4.2 Cloud Infrastructure and Public Sector Localization

Norway's public sector strategy explicitly favors the localization of data processing and storage to ensure service continuity and sovereignty.

Domestic Hosting of Critical Services The Norwegian government's data center strategy mandates that critical e-government services be hosted within Norway. This policy is driven by the goal of increasing productivity and value creation domestically while mitigating the risks associated with international data transfers [Source 3 (Q5)]. Consequently, primary data centers hosting sensitive national registries—including health and tax data—are located within Norwegian borders [Source 1 (Q5)].

Hyperscale Presence and Market Dynamics While specific market share statistics for domestic versus foreign cloud providers are unavailable, global hyperscalers dominate the high-end infrastructure market. Microsoft Azure has established specific regions in Norway (East and West) to cater to data residency requirements [Source 1 (Q2)]. AWS and Google Cloud also maintain a significant presence in the broader market [Source 4 (Q2)]. The government's National Digitalisation Strategy (2024-2030) acknowledges this reliance and promotes a "Cloud-First, Multi-Cloud" approach. This strategy aims to leverage the advanced capabilities of global providers while avoiding vendor lock-in and maintaining the ability to shift workloads to ensure sovereignty [Source 4 (Q10)].

Sector-Specific Trends In the healthcare sector, there is a specific recommendation to increase the adoption of modern, cloud-hosted Electronic Health Records (EHRs) [Source 1 (Q11)]. However, this modernization is constrained by the strict requirement that patient data remain protected under Norwegian and EEA law, reinforcing the need for localized cloud instances

provided by hyperscalers or compliant domestic alternatives [Source 1 (Q11)].

4.3 Internet Ecosystem and Digital Identity

The localization of Norway's internet ecosystem is characterized by a centralized traffic exchange infrastructure and a highly trusted national top-level domain.

Traffic Exchange and Routing Internet traffic exchange in Norway is geographically centralized in Oslo. Most interconnection between market players occurs via private settlement-free peering, while paid traffic exchange is conducted primarily at the public Internet Exchange Point (IXP) in Oslo [Source 4 (Q6)]. Despite a preference for local interconnection to keep traffic within national borders, regional peering outside of Oslo remains limited due to a lack of peering partners at smaller IXPs [Source 4 (Q6)]. This centralization presents a potential resilience vulnerability, although it facilitates monitoring and management of domestic traffic flows.

The .no Domain as a Sovereign Asset The country code top-level domain (ccTLD) `.no` is a critical component of Norway's digital identity. It is perceived as highly trusted by consumers and businesses, serving as the default choice for entities with a Norwegian presence [Source 4 (Q8)]. Strict registration rules require a physical address and a Personal ID or VAT ID within Norway, effectively localizing the ownership of these domains and ensuring that `.no` websites are operated by entities subject to Norwegian law [Source 4 (Q8)]. While the domain itself is secure, the adoption of advanced security protocols like DNSSEC among businesses remains inconsistent, with some entities using less robust algorithms or shared keys [Source 3 (Q8)].

References

- [Source 1 (Q1)] Norwegian DPA warns against EU-US data transfers - Piwik PRO (https://piwik.pro/blog/norwegian-dpa-warns-against-eu-us-data-transfers/)
- [Source 2 (Q1)] New Standard Contractual Clauses - Questions and Answers overview (https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en)
- [Source 1 (Q2)] Choose the Right Azure Region for You - Microsoft Azure (https://azure.microsoft.com/en-us/explore/global-infrastructure/geographies)
- [Source 2 (Q2)] Public Cloud Regions and Data Centers | Oracle (https://www.oracle.com/cloud/public-cloud-regions/)
- [Source 3 (Q2)] Rackspace Technology | Multicloud Solutions Provider (https://www.rackspace.com/)
- [Source 4 (Q2)] Public cloud revenue: Spending boom for AWS, Azure and Google … (https://www.techmonitor.ai/cloud/public-cloud-revenue-aws-azure-google-cloud/)
- [Source 1 (Q4)] 2020 United Nations E-Government Survey (https://www.un.org/en/desa/2020-united-nations-e-government-survey)
- [Source 1 (Q5)] Norwegian data centres - Regjeringen.no (https://www.regjeringen.no/contentassets/0eab-gb/pdfs/h-2510-e-datasenterstrategi.pdf)

- [Source 2 (Q5)] Choose the Right Azure Region for You - Microsoft Azure (https://azure.microsoft.com/en-us/explore/global-infrastructure/geographies)
- [Source 3 (Q5)] Norwegian data centres - sustainable, digital powerhouses (https://www.regjeringen.no/en/data-centres-sustainable-digital-powerhouses/id2867155/?ch=2)
- [Source 3 (Q6)] Internet Exchange Points - Euro-IX (https://www.euro-ix.net/media/filer_public/ab/d7/5b42-4c32-af47-7114e9a3c340/ixp_report_2020_.pdf)
- [Source 4 (Q6)] Market study on the Norwegian Internet ecosystem (https://www.wik.org/en/publications/ueber-das-norwegische-internet-oekosystem)
- [Source 3 (Q8)] An Exploration of the Adoption of DNSSEC by Businesses within the … (https://mauricon.org/conferences/index.php/iconic/article/download/3/3)
- [Source 4 (Q8)] .no Domain | Register your .no Name - GoDaddy IN (https://www.godaddy.com/en-in/tlds/no-domain)
- [Source 3 (Q9)] 2024 Investment Climate Statements: Norway (https://www.state.gov/reports/2024-investment-climate-statements/norway)
- [Source 1 (Q10)] The Digital Transformation of Norway's Public Sector (EN) - OECD (https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/07/the-digital-transformation-of-norway-s-public-sector_0db3fff0/1620e542-en.pdf)
- [Source 3 (Q10)] The Digital Norway of the Future – National Digitalisation Strategy … (https://www.regjeringen.no/contentassets/c499c3b6c93740bd989c43d886f65924/en-gb/pdfs/digitaliseringsstrategi_eng.pdf)
- [Source 4 (Q10)] Boosting Efficiency and Quality in EU Public Services: (https://ecipe.org/wp-content/uploads/2025/03/ECI_OccasionalPaper_04-2025_LY04.pdf)
- [Source 5 (Q10)] Vincenzo Aquaro's Post - LinkedIn (https://www.linkedin.com/posts/vincenzo-aquaro-79603563_strategic-sovereignty-ai-activity-7427171859487518720-m1r-)
- [Source 1 (Q11)] Norwegian EHR Market Analysis - regjeringen.no (https://www.regjeringen.no/contentas 2023-norwegian-ehr-market-analysis-final-report-v1.0.pdf)

Chapter 5

Security

Executive Summary

Norway presents a mixed cybersecurity profile characterized by strong institutional frameworks and sector-specific defense mechanisms, contrasted by significant structural vulnerabilities in network centralization and protocol adoption. The nation holds a National Cyber Security Index (NCSI) score of **67.53**, reflecting a capable baseline for cyber defense [Source 4]. However, critical infrastructure analysis reveals a high degree of upstream dependency, particularly on foreign and consolidated entities such as Cloudflare and GlobalConnect, creating potential single points of failure [Internal Graph].

While the operational landscape is bolstered by a mature ecosystem of Computer Emergency Response Teams (CERTs)—including KraftCERT and FinansCERT—collaborating through international forums [Source 6], technical network hygiene metrics are concerning. Intelligence indicates a complete absence of Autonomous System Numbers (ASNs) that simultaneously maintain Internet Exchange Point (IXP) membership and implement DNSSEC, suggesting a gap in proactive network hardening [Internal Graph].

5.1 National Cybersecurity Posture and Institutional Defense

Norway's strategic approach to cybersecurity is anchored in a robust institutional response capability. The country achieves a score of **67.53** on the National Cyber Security Index (NCSI), placing it in a tier of nations with established cyber defense mechanisms [Source 4].

The operational defense relies heavily on a decentralized but highly collaborative network of sector-specific CERTs. Key entities include **KraftCERT** (focusing on power and critical infrastructure) and **FinansCERT Norge** (now Nordic Financial CERT), which secure the financial sector. These organizations, alongside major telecommunications players like **Telenor CERT** and **Nets CERT**, leverage internal threat intelligence and malware analysis to monitor the threat landscape [Source 6].

To augment national defense strategies, these entities actively participate in international information sharing. Norwegian security teams are integrated into the **FIRST** (Forum of Incident Response and Security Teams) ecosystem, utilizing platforms such as **MISP** (Malware Information Sharing Platform) to facilitate the rapid exchange of indicators of compromise (IoCs) and context regarding attacker tactics, techniques, and procedures (TTPs) [Source 5] [Source 7].

5.2 Critical Infrastructure and BGP Resilience

A strategic analysis of Norway's internet infrastructure reveals acute risks related to Border Gateway Protocol (BGP) centralization and upstream dependencies.

Upstream Dependency Risks: Technical analysis highlights a high concentration of dependency on a limited number of upstream providers. **Cloudflare (CLOUDFLARENET)** serves as a critical node, holding upstream dependencies for **956 ASNs**. This is followed by **GlobalConnect AB (AS12552)**, which supports **747 dependencies** [Internal Graph].

Hegemony and Centralization: Several Norwegian entities exhibit a "hegemony score" of 1.0, indicating a 100% reliance on specific upstream providers. This absolute dependency creates potential chokepoints for BGP hijacking or service disruption. Entities identified with this vulnerability include: * **Blix Group AS** (BLIXFIBER-AS) * **Bredbandsfylket AS** (Bredbandsfylket-Troms) * **OKDN-AS** * **BrainStorm Network, Inc** (ONEPROVIDER-AS)

This centralization suggests that a targeted attack or technical failure affecting Cloudflare or GlobalConnect could have cascading effects across the Norwegian digital landscape [Internal Graph].

5.3 Network Hygiene and Protocol Adoption

Despite the maturity of its incident response capabilities, Norway exhibits notable gaps in technical preventative measures regarding network protocol security.

DNSSEC and IXP Participation: While **144 ASNs** in Norway are active members of Internet Exchange Points (IXPs)—a positive indicator of connectivity and peering—technical data reveals that **zero (0)** of these ASNs have implemented Domain Name System Security Extensions (DNSSEC) [Internal Graph]. This lack of intersection between IXP membership and DNSSEC deployment indicates a significant lapse in proactive network hygiene, leaving the routing infrastructure vulnerable to DNS spoofing and cache poisoning attacks.

Data Limitations: Current intelligence collection has not yielded definitive metrics regarding the volume of Distributed Denial of Service (DDoS) attacks specifically targeting Norway, nor is there sufficient data to quantify the current Resource Public Key Infrastructure (RPKI) validation rates among Norwegian ISPs [Source 2] [Source 3].

References

- [Source 1] Global Cybersecurity Index 2024 - ITU (https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf)
- [Source 2] Q3 2023 in Review: DDoS Attacks Report by StormWall (https://stormwall.network/resources/report-q3-2023)
- [Source 3] RPKI I-ROV Filtering World Map - APNIC Labs Measurements (https://stats.labs.apnic.net/rp
- [Source 4] Global Cybercrime Report 2024: Which Countries Face the Highest … (https://www.mixmode.ai/blog/global-cybercrime-report-2024-which-countries-face-the-highest-risk)
- [Source 5] Program Overview: Oslo 2019 FIRST Technical Colloquium (https://www.first.org/events/collo
- [Source 6] Program Overview (https://www.first.org/events/colloquia/oslo2017/program)
- [Source 7] Experts in CTI, VOC, and CSIRT - Orange Cyberdefense CERT (https://www.orangecyberdefense.com/no/loesningsomraader/orange-cyberdefense-cert)
- [Internal Graph] Internal Knowledge Graph (IYP-GRAPH)

Chapter 6

Governance

Executive Summary

Norway's governance framework regarding the digital domain is characterized by a dualistic approach: a strong commitment to international legal standards for cybercrime and a simultaneous expansion of domestic state surveillance capabilities. Norway has fully ratified the Council of Europe Convention on Cybercrime (Budapest Convention), establishing a robust legal basis for criminalizing cyber offenses and facilitating international cooperation [Source 1]. However, recent legislative changes, specifically the Intelligence Service Act (ISA) 2020 and amendments to the Electronic Communications Act (ECA), have significantly broadened the state's power to collect and retain citizen data [Source 2]. These developments have precipitated a conflict between national security imperatives and individual privacy rights, raising concerns regarding alignment with the General Data Protection Regulation (GDPR) and European human rights standards [Source 2]. While oversight mechanisms exist, including judicial review, the operational independence of regulatory bodies and the sufficiency of safeguards against "mission creep" remain subjects of active parliamentary and legal debate [Source 2] [Source 5].

6.1 International Legal Framework and Cybercrime Commitments

Norway has integrated key international conventions into its domestic legal order to combat cyber threats. By ratifying the Budapest Convention, the state has committed to criminalizing specific offenses such as illegal system access, data interference, and computer-related fraud [Source 1]. The country has also ratified the First Protocol to the Convention, which mandates the criminalization of acts of a racist and xenophobic nature committed through computer systems, thereby providing a legal mechanism to counter online hate speech [Source 1].

In the context of European integration, Norway is aligning its regulatory environment with European Union directives. The Norwegian Communications Authority (Nkom) serves as the national supervisory board for issuers of electronic identification (eID) means, operating within

the framework of the eIDAS Regulation [Source 4]. Furthermore, Norway is in the process of implementing the Audiovisual Media Services Directive (AVMSD) to protect minors on video-sharing platforms and has appointed a Digital Services Coordinator in anticipation of incorporating the Digital Services Act (DSA) into the EEA Agreement [Source 3].

6.2 State Surveillance and Data Retention Legislation

A significant shift in Norway's governance posture is evident in the expansion of intelligence gathering powers. The Intelligence Service Act 2020 (ISA) introduced "facilitated collection" of cross-border electronic communication. Chapters 7 and 8 of the ISA, which govern these powers and judicial review, entered into force in January 2022 [Source 2]. Additionally, 2021 amendments to the Electronic Communications Act (ECA) imposed duties on telecommunication operators and internet providers to record IP addresses and disclose this data to police and prosecutors under specific circumstances [Source 2].

Further proposals have sought to enhance the Police Security Service (PST) capabilities, specifically regarding the collection and processing of "openly available information" online for intelligence purposes [Source 2]. These legislative moves have drawn criticism for potential "mission creep" and the ambiguity surrounding what constitutes openly available data. Historical precedents, such as the PST's illegal collection of passenger lists between 2010 and 2019, are cited by critics as evidence of the risks associated with expanded surveillance mandates [Source 2].

6.3 Privacy Rights, Oversight, and Civil Liberties

The expansion of surveillance powers has created friction with established privacy frameworks, particularly the GDPR. While Norway is subject to GDPR, its national security legislation operates under exemptions that critics argue may not meet the strict proportionality and necessity tests required by European courts [Source 2]. Concerns focus on the broad scope of data collection, long retention periods, and the potential limitation of data subject rights [Source 2].

Despite these concerns, there is no evidence that the Norwegian state engages in authoritarian digital control tactics such as internet shutdowns or the widespread blocking of social media platforms [Source 6]. The governance debate is instead centered on legislative oversight. The implementation of Section 7-3 of the ISA (bulk interception) was subject to a pause before re-entering into force in September 2022, reflecting an active parliamentary struggle to balance technological realities—such as encryption and the speed of data—with the protection of civil liberties [Source 5]. While judicial review mechanisms are in place, their adequacy in the face of mass surveillance capabilities remains a contested issue within Norway's legal and political spheres [Source 2].

References

- [Source 1] Cybercrime Programme Office of the Council of Europe (C-PROC). (2024). *Cybercrime and the Budapest Convention.* (https://rm.coe.int/cyber-rp-breakfast-nov2024-final/1680b28562)
- [Source 2] Wessel-Aas, J. (2022). *The Development of Digital Mass Surveillance in Norway.* FIU Law Review. (https://ecollections.law.fiu.edu/cgi/viewcontent.cgi?article=1555&context=lawreview
- [Source 3] Better Internet for Kids. (n.d.). *Norway - Policy monitor country profile.* (https://better-internet-for-kids.europa.eu/en/knowledge-hub/norway-policy-monitor-country-profile)
- [Source 4] European Commission. (n.d.). *The Norwegian Digitalisation Agency (DIGDIR) Notification Form.* (https://ec.europa.eu/digital-building-blocks/sites/download/attachments/507183385 form%20BankID.pdf?version=1&modificationDate=1647274365234&api=v2)
- [Source 5] Larsson, S., et al. (2024). *A comparative analysis of the debates in UK, Finland and Norway.* (https://link.springer.com/article/10.1057/s41284-024-00443-3)
- [Source 6] V-Dem Institute. (n.d.). *Country Graph.* (https://v-dem.net/data_analysis/CountryGraph/)

Chapter 7

Strategic Synthesis & Roadmap

Chapter 8

Section 7: Strategic Synthesis & Roadmap

To: The Office of the Prime Minister / The President **From:** Chief Strategy Officer **Date:** October 26, 2025 **Subject:** STATE OF THE DIGITAL NATION – The "Glass Fortress" Paradox

---

8.1 1. Executive Summary: The "Big Picture" Diagnosis

The Narrative: Norway stands as a global paradox in the digital age. We are a "Digital Fortress" built on a foundation of glass. On the surface, we are a world leader: 99% 5G coverage, robust fiber penetration, and a high-trust governance model that aligns with our democratic values. We are the envy of Europe regarding connectivity speeds and energy potential.

The Paradox: "Sovereign Intent vs. Operational Dependency" However, our technical reality contradicts our geopolitical ambition. While we legislate for "Digital Sovereignty," our logical infrastructure is dangerously dependent on foreign entities. 1. **Physical Vulnerability:** Our critical subsea cables (Svalbard) are privately owned and have already been sabotaged. 2. **Logical Vulnerability:** A massive portion of our traffic relies on single foreign upstream providers (e.g., Telia's 100% dependency on Sweden, the "Cloudflare Hegemony"). 3. **Market Stagnation:** A comfortable duopoly (Telenor/Telia) keeps consumer prices artificially high, stifling the domestic digital economy despite our advanced infrastructure.

The Diagnosis: We have built a Ferrari engine (Infrastructure) but put it in a chassis we do not fully own (Foreign Dependency) and are driving it with the handbrake on (Oligopolistic Pricing).

8.2 2. SWOT Analysis: The Strategic Cheat Sheet

STRENGTHS (Internal)	WEAKNESSES (Internal)
Energy & Location: Abundant green energy and cold climate make us the ideal "Green Data Battery" for Europe.	**The Duopoly Tax:** Telenor and Telia dominance results in high ARPU and low innovation pressure.
Infrastructure Maturity: Near-ubiquitous 5G and Fiber (FTTH/B >50%) provide a flawless physical layer.	**Cyber Hygiene Gaps:** Zero (0) ASNs at IXPs use DNSSEC. We are wide open to routing attacks (spoofing).
Institutional Trust: Strong CERT ecosystem (KraftCERT, FinansCERT) and high government trust.	**Legal/Physical Disconnect:** Critical subsea assets are privately held, limiting state defense options.

OPPORTUNITIES (External)	THREATS (External)
The "Arctic Gateway": Positioning Norway as the secure data transit hub between North America, Europe, and Asia.	**Hybrid Warfare:** Sabotage of subsea cables in the High North (Russian threat vector).
Sovereign AI Cloud: Leveraging non-EU status to build a "Data Haven" that is GDPR compliant but shielded from US FISA reach.	**The "Kill Switch":** Telia's 100% reliance on Swedish upstream providers creates a single point of failure.
DPI Export: Packaging our Digital Public Infrastructure (ID, Tax) as a product for emerging economies.	**US Extraterritoriality:** CLOUD Act/FISA 702 undermining our data sovereignty despite local hosting.

8.3 3. Strategic Roadmap: The Policy Agenda

8.3.1 Phase 1: Immediate Actions (0–12 Months) – "Hardening the Target"

Goal: Close the most dangerous security gaps without legislative overhaul.

- **Directive 1 (The "Kill Switch" Audit):** Immediately audit **Telia Norge AS** and **Blix Group AS** regarding their 100% upstream dependency. Mandate a "Multi-Path" redundancy requirement for all Tier-1 operators to ensure no single cross-border link can sever national connectivity.
- **Directive 2 (Hygiene Mandate):** The National Communications Authority (Nkom) must enforce **DNSSEC adoption** for all ISPs and critical infrastructure providers within 6 months. The current 0% adoption rate at IXPs is a national security negligence.
- **Directive 3 (Cable Security):** Designate all subsea cables to Svalbard and the continent as "Critical National Capabilities." Deploy permanent sensor monitoring on these lines (using Navy/NATO assets) regardless of private ownership.

8.3.2 Phase 2: Structural Reforms (12–36 Months) – "Breaking the Stagnation"

Goal: Lower costs for citizens and secure physical ownership.

- **Market Reform:** Aggressively incentivize a third and fourth mobile network operator. Use spectrum auction subsidies specifically for *new* entrants to break the Telenor/Telia pricing lock. High prices are slowing our digital economy.
- **The "Golden Share" Strategy:** The State should acquire "Golden Shares" or controlling stakes in the landing stations and fiber backbones currently held by private equity. We cannot outsource the security of our physical borders.
- **Data Sovereignty Shield:** Establish a state-backed "Sovereign Cloud" entity (Public-Private Partnership) that guarantees data residency *and* immunity from US CLOUD Act requests, specifically for health, police, and military data.

8.3.3 Phase 3: Long-Term Vision (3–5 Years) – "The Arctic Data Haven"

Goal: Transform Norway from a consumer of tech to a global host.

- **Green AI Hub:** Leverage our hydropower to attract high-density AI compute workloads that are being pushed out of mainland Europe due to energy costs.
- **Digital Foreign Policy:** Use our position outside the EU (but aligned with it) to mediate data transfer agreements. Become the "Switzerland of Data"—neutral, secure, and powered by green energy.

8.4 4. Final Verdict

8.4.1 Investability Score: HIGH (Defensive/Infrastructure)

Explanation: Norway is a "Safe Haven" asset. While the consumer market is saturated and expensive (hard for retail entrants), the infrastructure sector (Data Centers, Fiber) is prime for investment due to energy stability, political predictability, and the inevitable demand for AI compute hosting.

8.4.2 Maturity Score: MATURE (But Complacent)

Explanation: We have "completed" the physical build-out (5G/Fiber). However, we are complacent on the logical layer (Security/Routing). We are a wealthy homeowner who installed a steel door (Infrastructure) but left the window unlocked (BGP/DNSSEC) and gave the spare key to a neighbor (Foreign Dependency).

Signed,

Chief Strategy Officer