STRATEGIC COUNTRY REPORT: DENMARK

Automated Strategic Analyst (v2.2 Parallel)

12 February 2026

Contents

Chapter 1

Geopolitics

Executive Summary

Denmark's geopolitical posture in the digital domain is defined by a dual strategy: asserting itself as a "Regional Gateway" through the strategic utility of Greenland and the North Atlantic, while simultaneously pursuing an aggressive "Digital Sovereignty" policy to reduce dependence on United States technology providers.

Geographically, Denmark serves as a critical bridge between North America and Europe, physically anchored by the Havfrue submarine cable system and the Blaabjerg landing station. This connectivity is bolstered by the geopolitical significance of Greenland, which provides the Kingdom of Denmark with leverage in Arctic security and transatlantic monitoring via the GIUK (Greenland-Iceland-United Kingdom) Gap [Source 8].

However, a distinct tension exists between this physical connectivity to the U.S. and Denmark's software and data governance policies. Aligned with broader European Union objectives, Copenhagen is actively attempting to decouple its public sector from non-European tech giants. This is exemplified by the government's initiative to phase out Microsoft products in favor of open-source alternatives, citing national security and regulatory autonomy as primary drivers [Source 2]. While Denmark maintains a robust digital economy with high integration of private sector platforms—specifically Google entities [IYP-GRAPH]—its state-level trajectory is increasingly focused on operational autonomy and resilience against extraterritorial surveillance and vendor lock-in [Source 2, Source 6].

Strategic Geography and Connectivity

The Arctic and North Atlantic Gateway Denmark's status in global digital geopolitics is best characterized as a "Regional Gateway" rather than a "Digital Fortress" or "Vassal State" [Source 8]. This designation is largely derived from the Kingdom's sovereignty over Greenland. The territory hosts the Pituffik Space Base (formerly Thule), a critical U.S. military installation, and sits astride the GIUK Gap, a maritime choke point essential for monitoring Russian naval

and submarine activity [Source 8]. While Greenland possesses growing autonomy and its own foreign security strategy, its resource potential (rare earths) and location maintain Denmark's relevance to major powers like the U.S. [Source 8, Source 9].

Submarine Cable Infrastructure Denmark's physical connectivity relies heavily on the Blaabjerg submarine cable landing station, the country's primary digital entry point [Source 1]. A key asset in this infrastructure is the Havfrue cable system, a consortium-owned cable connecting Denmark directly to the United States and Ireland. Operational since late 2019, Havfrue increases capacity and resiliency for North Atlantic systems, physically linking Denmark to the U.S. digital sphere [Source 7].

Ownership and Oversight The ownership structure of this critical infrastructure is predominantly private. The planning, operation, and maintenance of submarine cables landing in Denmark are almost entirely in the hands of the private sector, with limited direct EU or state oversight regarding specific infrastructure decisions [Source 12]. This reliance on private capital for assets costing hundreds of millions of dollars creates a complex security environment where national strategic interests must be managed alongside commercial imperatives [Source 12, Source 13].

Digital Sovereignty and Decoupling Policies

Phasing Out Non-European Tech Denmark is executing a proactive strategy to enhance control over its digital infrastructure, explicitly targeting a reduction in reliance on U.S. technology providers. A flagship initiative in this domain is the government-wide move to phase out Microsoft Office 365 and Windows in favor of open-source alternatives such as LibreOffice and Linux [Source 2]. This transition is led by the Ministry of Digitalisation and is already being pursued by major municipalities like Copenhagen and Aarhus [Source 2].

Strategic Drivers The shift to open-source software is driven by a combination of security, economic, and regulatory factors: * **Vendor Independence:** Reducing "vendor lock-in" to ensure the state is not beholden to a single foreign commercial entity [Source 2]. * **Data Privacy:** Mitigating concerns regarding extraterritorial surveillance and ensuring compliance with GDPR [Source 2]. * **Resilience:** Aligning with EU-wide efforts to foster a "Digital Single Market" and build sovereign digital public services that are interoperable across Europe [Source 4, Source 6].

Former Prime Minister Mette Frederiksen has been a vocal advocate for this shift, co-signing calls for a digitally sovereign Europe that fosters local innovation rather than relying solely on foreign tech giants [Source 6].

Domestic Digital Architecture Domestically, Denmark reinforces this sovereignty through a highly integrated public-private digital architecture. The system relies on a single national identifier (CPR) and a unified digital key (MitID), which facilitates deep integration between sectors while maintaining state control over the core identity infrastructure [Source 10].

Critical Infrastructure Dependencies

Despite the policy shift toward sovereignty, technical intelligence reveals a continued deep reliance on major U.S. hyperscalers within Denmark's network topology.

ASN Dependency Analysis Analysis of Denmark's Autonomous System Numbers (ASNs) indicates significant dependency on foreign entities. Specifically, Google entities (such as GOOGLE-CLOUD-PLATFORM, ASN 396982, and GOOGLE-AS-AP, ASN 139190) show a 1.0 dependency score on the Danish incumbent ASN 15169 [IYP-GRAPH]. This suggests that while the government seeks to purge Microsoft from administrative systems, the underlying network infrastructure remains heavily intertwined with other U.S. tech giants like Google.

Transit and Resilience Danish incumbent ASNs (e.g., ASN 42541) serve as transit points for various dependent entities, including local providers like TOKE-DK and Hafnium [IYP-GRAPH]. While no single point of failure among foreign providers was explicitly identified in the available dataset, the concentration of dependency on specific incumbent nodes highlights potential vulnerabilities in the event of targeted disruptions to these primary ASNs [IYP-GRAPH].

References

- [Source 1] Cable landing point - Wikipedia (https://en.wikipedia.org/wiki/Cable_landing_point)
- [Source 2] Denmark moves to replace Microsoft software as part of digital sovereignty strategy (https://dig.watch/updates/denmark-moves-to-replace-microsoft-software-as-part-of-digital-sovereignty-strategy)
- [Source 3] The Danish Digital Journey (https://en.digst.dk/policy/the-danish-digital-journey/)
- [Source 4] Interoperability as a cornerstone of a digitally sovereign Europe (https://danish-presidency.consilium.europa.eu/en/news/interoperability-as-a-cornerstone-of-a-digitally-sovereign-europe/)
- [Source 5] The discursive struggle for digital sovereignty - DIIS (https://www.diis.dk/en/research/the-discursive-struggle-digital-sovereignty)
- [Source 6] What is digital sovereignty and how are countries approaching it? (https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/)
- [Source 7] Expanding our global infrastructure with new regions and subsea cables (https://cloud.google.com/blog/topics/inside-google-cloud/expanding-our-global-infrastructure-new-regions-and-subsea-cables)
- [Source 8] Explainer: The Geopolitical Significance of Greenland - Belfer Center (https://www.belfercenter.org/research-analysis/explainer-geopolitical-significance-greenland)
- [Source 9] Greenland, Rare Earths, and Arctic Security - CSIS (https://www.csis.org/analysis/greenland-rare-earths-and-arctic-security)
- [Source 10] Following the citizen's journey makes Denmark a world leader in e-government (https://govinsider.asia/intl-en/article/following-the-citizens-journey-makes-denmark-a-

world-leader-in-e-government)
- [Source 11] LibreOffice 25.8 Backgrounder - TDF Community Blog (https://blog.documentfoundation.org/
25-8-backgrounder/)
- [Source 12] Security threats to undersea communications cables and infrastructure
(https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.p
- [Source 13] Submarine communications cable - Wikipedia (https://en.wikipedia.org/wiki/Submarine_com
- [IYP-GRAPH] Internal Knowledge Graph - ASN Dependency Analysis

Chapter 2

Infrastructure

Executive Summary

Denmark possesses a highly advanced telecommunications infrastructure, characterized by European leadership in 5G availability and ambitious national broadband targets. As of Q4 2024, Denmark recorded a 5G population coverage of 83.4%, the highest among Nordic nations, driven by the timely release of mid-band spectrum and a strategic avoidance of Dynamic Spectrum Sharing (DSS) [Source 1]. The physical infrastructure landscape includes a concentrated hyperscale presence, notably a major Google facility in Fredericia [Source 2]. National connectivity goals are aggressive, aiming for 98% gigabit coverage for households and businesses by 2025, supported by a market-based rollout strategy and the National Broadband Pool for rural subsidies [Source 3]. While domestic mobile network obligations are strictly regulated to eliminate coverage gaps, specific technical data regarding national fiber backbone redundancy and active Internet Exchange Points (IXPs) remains limited in open sources.

2.1 Digital Infrastructure and Data Centers

Denmark's digital infrastructure is anchored by specific hyperscale investments rather than a widely distributed network of colocation facilities. Intelligence indicates a concentration of hyperscale capacity in the Fredericia region, which hosts a major Google data center [Source 2]. Unlike other Western markets where providers like Equinix maintain extensive facility lists, specific Danish locations for such major colocation providers are not publicly detailed in current technical findings, suggesting a market structure heavily reliant on specific hyperscale operators or domestic integrators [Source 4].

Connectivity to these facilities is supported by fiber networks such as those operated by GlobalConnect Carrier, which links data centers across the region, although specific topological maps of these fiber routes are not currently available [Source 5].

2.2 Mobile Network Development (5G/4G)

Denmark has established itself as a premier market for 5G deployment. The country's mobile infrastructure strategy is distinguished by the prioritization of mid-band spectrum assets, allowing operators to achieve high availability without relying disproportionately on DSS technology, which shares frequencies between 4G and 5G [Source 1].

Spectrum Allocation and Auctions The most recent spectrum auctions generated over DKK 2 billion, distributing frequencies across the 2100 MHz, 3.5 GHz, 26 GHz, 1500 MHz, and 2300 MHz bands. The primary license winners were Hi3G, TDC Net, and TT Network [Source 6].

Coverage Obligations and Private Networks To ensure comprehensive national coverage, regulators have imposed strict build-out obligations: * **Population Targets:** Operators were mandated to achieve 60% population coverage by the end of 2023 and 75% by the end of 2025 [Source 6]. * **White Spot Elimination:** Licenses included requirements to establish coverage in 122 specific underserved areas (providing at least 30 Mbps download/3 Mbps upload) by February 1, 2024 [Source 6]. * **Private 5G Provisioning:** TT Network is obligated to rent 60 MHz of the 3.5 GHz band and 400 MHz of the 26 GHz band to non-telecom entities (e.g., universities, private enterprises) to facilitate private network development [Source 6].

2.3 Broadband and International Connectivity

National Broadband Strategy Denmark's "Digital Strategy" sets high benchmarks for fixed-line connectivity. The National Broadband Plan targets 100% coverage of households and businesses with 100/30 Mbps connections and 98% coverage with 1 Gbps download speeds by 2025 [Source 3]. The deployment strategy emphasizes technological neutrality and market-driven rollouts. To address the "digital divide," the government established the National Broadband Pool in 2016 to subsidize infrastructure in rural areas where commercial rollout is not viable [Source 3].

International Links Information regarding Denmark's submarine cable infrastructure is limited, though regulatory documents confirm the existence of the "Havfrue" system, a consortium-owned cable system involving Danish entities, which facilitates transatlantic connectivity [Source 7].

References

- [Source 1] The Envy of Europe: Nordics Lead in 5G Availability and Network Performance (https://www.ookla.com/articles/nordics-5g-q1-2025)
- [Source 2] Locations of Google Data Centers (https://datacenters.google/locations)
- [Source 3] Digital connectivity in Denmark | Shaping Europe's digital future (https://digital-strategy.ec.europa.eu/en/policies/digital-connectivity-denmark)
- [Source 4] Colocation and connectivity in global, AI-ready data centers - Equinix (https://www.equinix.com/data-centers)

- [Source 5] Explore our network - GlobalConnect Carrier (https://globalconnectcarrier.com/our-network/)
- [Source 6] Denmark awards 5G frequency bands - Specure GmbH (https://specure.com/denmark-awards-5g-frequency-bands/)
- [Source 7] PUBLIC NOTICE - Federal Communications Commission (https://docs.fcc.gov/public/attachm 351000A1.pdf)

Chapter 3

Market

Executive Summary

The Danish telecommunications market is characterized by high-performance mobile infrastructure and competitive pricing, despite a notable opacity regarding recent operator-level financial data. Denmark ranks among the top 10 countries globally for median mobile download speeds, recording speeds of approximately 113.44 Mbps as of late 2022 [8]. Consumer pricing for mobile data is exceptionally low compared to other Western markets; the average price for 1GB of data is below $2, significantly cheaper than the United Kingdom ($6.66) and the United States ($12.37) [1].

Structurally, the market faces pressure toward consolidation. While no significant "disruptor" operators have recently entered the market to fracture pricing models, analysts indicate that the Danish market, alongside Spain and Italy, requires industry consolidation to sustain investment levels [5]. However, regulatory hurdles remain high, evidenced by the withdrawal of the attempted merger between Telia and Telenor in 2015 [4]. Current intelligence indicates a lack of definitive 2024 data regarding specific subscriber market shares and Herfindahl-Hirschman Index (HHI) scores, as regulatory revenue data for the preceding year has not yet been released [2]. Consequently, the market is currently defined by intense price competition, commoditization of services, and a strategic focus on 5G deployment amidst stagnating Average Revenue Per User (ARPU) trends [9][10].

Pricing and Affordability

Denmark maintains a highly competitive pricing environment for mobile data. The cost of 1GB of mobile data is consistently below $2, positioning Denmark as a low-cost leader in Western Europe, though slightly more expensive than Finland ($1.16) and Poland ($1.32) [1]. For basic connectivity, a standard mobile data plan offering 10GB is estimated to cost approximately 69 Danish Kroner (DKK), or roughly €9 [3].

This low-price environment suggests a high degree of commoditization within the sector. In-

telligence suggests that the market is driven by intense competition which limits the ability of operators to raise baseline prices, leading to stagnant ARPU growth [9]. While specific affordability metrics for the bottom 40% of the population are not explicitly detailed in current reporting, the low entry price for data plans suggests high accessibility relative to peer nations [3].

Market Structure and Competition

The Danish market structure is mature but faces significant headwinds regarding profitability and fragmentation. Unlike markets such as France, which experienced upheaval through the entry of disruptors like Free, Denmark has not seen a similar recent market entrant impact pricing or service offerings [4]. Instead, the competitive landscape is shaped by established incumbents struggling with the "commoditization" of connectivity services [9].

There is a distinct trend and strategic intent toward consolidation. Intelligence reports highlight that Denmark is viewed as a market where "industry consolidation is needed" to improve economic viability for operators [5]. This is part of a broader European trend where maturing markets and the need for scale to support infrastructure investments are driving a new era of Mergers and Acquisitions (M&A) [6]. However, previous consolidation efforts, such as the 2015 attempted merger between Telia and Telenor, failed due to regulatory opposition, highlighting the tension between competition authorities' desire for low prices and the industry's need for scale [4].

Current granular data on operator market share is limited. Regulatory reporting for 2023/2024 revenue is delayed, and differences in reporting standards for Fixed Wireless Access (FWA)—classified as mobile broadband in Denmark but fixed in neighboring Norway—complicate direct revenue comparisons [2].

Infrastructure and Service Quality

Denmark boasts robust mobile network performance. The country is a global leader in mobile speeds, with median download speeds recorded at 113.44 Mbps, placing it in the top tier of global rankings [8]. This high performance is critical for the deployment of advanced 5G services, although the economic viability of such deployments in rural areas remains a challenge without network sharing or consolidation [10].

In the fixed broadband sector, while general speeds are high, specific quality of service (QoS) issues have been identified regarding latency and packet loss. User reports indicate that despite high frame rates and acceptable ping times (30-60ms), packet loss can severely degrade real-time applications such as online gaming and video conferencing [7]. This suggests that while raw throughput is high, routing and network stability remain variable for latency-sensitive use cases. There is currently no definitive comparative data available to assess mobile network latency and packet loss against these fixed broadband metrics [7].

References

- [1] India beats UK and US on mobile data price - BBC (https://www.bbc.com/news/technology-47416250)
- [2] Assessment of Norwegian fixed broadband pricing in a Nordic context (https://www.regjeringen.no/con of-norwegian-fixed-broadband-pricing-in-a-nordic-context-by-tefficient-5-sep-2024.pdf)
- [3] What's up with smartphone data plans? : r/Netherlands - Reddit (https://www.reddit.com/r/Netherla
- [4] Emerging trends in communication market competition | OECD (https://www.oecd.org/content/dam/ trends-in-communication-market-competition_3f2df010/4ad9d924-en.pdf)
- [5] Telecom tycoons on the move? | ING Think (https://think.ing.com/articles/telecom-tycoons-on-the-move/)
- [6] Preparing For A New Era In Telco M&A - Oliver Wyman (https://www.oliverwyman.com/our-expertise/insights/2025/nov/european-telco-ma-transformation-next-growth-wave.html)
- [7] PLEASE HELP! My ISP insists that the Packet Loss is not from their end - Reddit (https://www.reddit.com/r/HomeNetworking/comments/pno1nt/please_help_my_isp_insists_that_th
- [8] The Speedtest Global Index Shows These Countries Sped Up - Ookla (https://www.ookla.com/articles/ index-internet-speed-growth-2022)
- [9] Commoditization in mobile telecoms | Strategy& - PwC Strategy (https://www.strategyand.pwc.com/g telecoms-commoditization.html)
- [10] Competition and investment in the Danish mobile market (https://digst.dk/media/anppemw3/final_ confidential.pdf)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 4

Localization

Executive Summary

Denmark maintains a highly advanced digital infrastructure, characterized by a top-tier ranking in the United Nations E-Government Development Index [Source 1]. Unlike some jurisdictions that have enacted strict, standalone data localization mandates, Denmark primarily aligns its data residency and sovereignty posture with the broader European Union framework, specifically the General Data Protection Regulation (GDPR) [Source 2]. There is no evidence of specific Danish laws imposing stronger localization requirements than those found in standard EU regulations [Source 2].

However, the Danish strategic landscape is influenced by growing concerns regarding digital sovereignty and the extraterritorial application of foreign laws, such as the U.S. CLOUD Act. While Denmark is considered a trusted partner in U.S. AI diffusion policies [Source 3], the transfer of personal information to third countries has become increasingly burdensome following the annulment of the Privacy Shield framework [Source 4]. Domestically, Denmark exhibits a strong preference for national digital identity through the widespread adoption of the .dk country code top-level domain (ccTLD), managed under strict regulatory oversight [Source 5].

Legal Framework and Data Sovereignty

Regulatory Alignment and Extraterritorial Risks Denmark's approach to data localization is not defined by a single national "sovereign cloud" law but rather by adherence to EU standards. The Danish government and regulatory bodies operate under the GDPR, which does not inherently mandate data localization within Denmark but imposes strict conditions on international transfers [Source 2]. A significant strategic concern for the Danish and broader EU jurisdiction is the conflict between local privacy protections and the extraterritorial reach of the U.S. CLOUD Act. This legislation allows U.S. authorities to request data from U.S. service providers regardless of where the data is physically stored, creating a conflict with GDPR Article 48 regarding lawful data transfers [Source 6].

Cloud Usage and Compliance The Danish Data Protection Agency issued a "Guide on the use of Cloud Services" in March 2022 to assist entities in navigating these complexities [Source 4]. Furthermore, the Danish Financial Supervisory Authority (FSA) has implemented cyber stress testing to ensure the financial sector's resilience against ICT disruptions, indicating a sector-specific focus on infrastructure security rather than a blanket localization mandate [Source 4]. From a taxation perspective, the Danish Tax Board has ruled that a data center operated by a Danish company for a nonresident entity does not necessarily constitute a "permanent establishment" for tax purposes, clarifying the fiscal treatment of hosting infrastructure [Source 7].

Digital Infrastructure and Public Sector Hosting

E-Government and Data Security Denmark is ranked as a global leader in digital government, alongside the Republic of Korea and Estonia, driven by robust online services and telecommunication infrastructure [Source 1]. Despite this high level of digitization, specific market share data regarding the hosting of public records on local versus foreign hyperscale clouds remains opaque.

Protection of Sensitive Data In the absence of a unified "National Cloud" strategy, specific agencies maintain rigorous localization protocols. Statistics Denmark, the central authority on Danish statistics, exemplifies strict data localization. The agency explicitly states that confidential information is never stored outside its secure zone and utilizes encrypted lines for data retrieval. Statistics Denmark maintains ISO 27001 certification and acts as the sole data controller for the information it processes, ensuring sensitive citizen data remains within Danish legal jurisdiction [Source 8].

National Identity in Cyberspace (.dk)

Domain Market Dominance Denmark exhibits a distinct preference for local digital identity. The .dk ccTLD is described as "extremely popular," with over 1.2 million registered domains in a country with high internet penetration (approx. 97% of households) [Source 5]. The registry is managed by DK Hostmaster, which enforces stringent registration policies. Unlike generic top-level domains (gTLDs), .dk registrants must provide valid identification (VAT ID for companies or tax numbers for individuals), and the registry actively prohibits typosquatting [Source 5]. This rigorous management fosters a trusted local digital environment, although specific comparative statistics between .dk and .com usage for businesses are not definitively available.

References

- [Source 1] 2020 United Nations E-Government Survey (https://www.un.org/en/desa/2020-united-nations-e-government-survey)

- [Source 2] Data protection under GDPR - Your Europe - European Union (https://europa.eu/youreurope/
with-customers/data-protection/data-protection-gdpr/index_en.htm)
- [Source 3] What to Know About the New U.S. AI Diffusion Policy and Export … (https://www.cfr.org/articles/what-know-about-new-us-ai-diffusion-policy-and-export-controls)
- [Source 4] 2025 Investment Climate Statements: Kingdom of Denmark (https://www.state.gov/reports/20
investment-climate-statements/denmark)
- [Source 5] Register .dk domains and benefit from the ccTLD of Denmark (https://www.internetx.com/en/
domains/)
- [Source 6] The CLOUD Act and Transatlantic Trust - CSIS (https://www.csis.org/analysis/cloud-act-and-transatlantic-trust)
- [Source 7] Danish Tax Board rules Danish data center does not create a … (https://globaltaxnews.ey.com/n
6271-danish-tax-board-rules-danish-data-center-does-not-create-a-permanent-establishment-for-nonresident-company)
- [Source 8] Information security and data confidentiality - Statistics Denmark (https://www.dst.dk/en/OmDS/kvalitet-og-styring/datasikkerhed-i-danmarks-statistik)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 5

Security

Executive Summary

Denmark exhibits a dichotomy between a mature strategic governance framework and significant technical vulnerabilities within its core routing infrastructure. While the nation demonstrates strong preparedness in policy and regulation—ranking 16th on the National Cyber Security Index with a score of 89.17—its technical defenses against routing attacks are critically underdeveloped [Source 2]. Intelligence indicates that 0.0% of Danish IP prefixes are covered by Route Origin Authorizations (ROAs) via the Resource Public Key Infrastructure (RPKI), leaving the national network highly susceptible to BGP hijacking [IYP-GRAPH].

The threat landscape is dominated by state-sponsored and politically motivated actors targeting critical infrastructure. Notable incidents include a coordinated attack on 22 energy companies in May 2023, linked to Russian military intelligence (Sandworm), and DDoS campaigns against the healthcare sector by groups such as 'Anonymous Sudan' [Source 1][Source 3]. The centralization of routing dependencies, particularly around GlobalConnect A/S, creates potential chokepoints that adversaries could exploit to disrupt national connectivity [IYP-GRAPH].

5.1 Strategic Cyber Posture and Governance

Denmark maintains a robust cybersecurity posture relative to its digital development. The country holds the 16th position on the National Cyber Security Index (NCSI) with a score of 89.17, which exceeds its general Digital Development Level score of 85.59 [Source 2]. This ranking reflects a proactive approach to cyber resilience and a strong commitment to cybersecurity policy, further evidenced by the implementation of the National Strategy for Cyber and Information Security 2022-2024 [Source 3][Source 4].

Despite high-level governance, the operational landscape faces challenges regarding the adoption of specific security norms. While European Internet Exchange Points (IXPs) are increasingly adopting Mutually Agreed Norms for Routing Security (MANRS), there is no definitive data confirming the compliance of individual Danish networks, suggesting a potential gap between

national strategy and operator-level implementation [Source 1 - Euro-IX].

5.2 Critical Infrastructure and Threat Landscape

Denmark's critical infrastructure is a primary target for sophisticated cyber operations. The threat environment is characterized by high activity from state-backed actors and criminal groups utilizing advanced attack vectors.

Energy and Healthcare Sector Targeting In May 2023, Denmark experienced its largest cybersecurity incident to date: a coordinated attack targeting 22 energy companies. This operation exploited zero-day vulnerabilities in Zyxel firewalls and demonstrated a level of sophistication attributed to the Sandworm group, a unit of Russia's GRU. Compromised infrastructure was subsequently weaponized to launch DDoS attacks against international targets [Source 1]. Additionally, the healthcare sector has faced politically motivated DDoS attacks, specifically against hospitals in February 2023 by the group 'Anonymous Sudan'. These attacks utilized financially backed infrastructure and open proxies to obfuscate origins [Source 3].

Prevalent Attack Vectors The most significant vectors impacting Danish infrastructure involve the exploitation of unpatched vulnerabilities. Intelligence highlights specific weaknesses in: * Internet-facing PLCs and HMIs within critical infrastructure. * Microsoft ecosystem vulnerabilities (Outlook, SharePoint, Windows). * Third-party vendor compromises and stolen OAuth 2.0 tokens. * Command injection flaws in power company systems [Source 2].

5.3 Network Sovereignty and Routing Security

Technical analysis of Denmark's routing architecture reveals severe deficiencies in the validation of routing information and the presence of critical infrastructure chokepoints.

BGP Vulnerabilities and Chokepoints Current technical data indicates a critical lack of RPKI deployment, with 0.0% of Danish IP prefixes covered by ROAs. This absence of cryptographic validation means the network is defenseless against accidental or malicious route hijacks [IYP-GRAPH]. Furthermore, the network topology exhibits high interdependency. GlobalConnect A/S (AS31027) acts as a critical chokepoint, with 660 other Autonomous System Numbers (ASNs) showing 100% dependency on it. Other significant nodes include M247 Europe SRL and TDC Holding A/S. Disruption of these specific ASNs could result in widespread cascading outages [IYP-GRAPH].

DNS Traffic Analysis Analysis of DNS query traffic originating from Denmark shows a high concentration of queries to domestic media and education domains, specifically `lectio.dk` (100% of analyzed share), `tv2.dk`, and `dr.dk`. While no immediate patterns of DNS spoofing were detected in the sample, the lack of widespread RPKI validation and the absence of confirmed DNSSEC validation rates leaves users vulnerable to cache poisoning and man-in-the-middle attacks, which could compromise data integrity and user trust [IYP-GRAPH][Source 3 - Catchpoint].

References

- [Source 1] Denmark Faces Largest Cybersecurity Incident to Date (https://westoahu.hawaii.edu/cyber/glo weekly-exec-summary/denmark-faces-largest-cybersecurity-incident-to-date/)
- [Source 1 - Euro-IX] Internet Exchange Points - Euro-IX (https://www.euro-ix.net/media/filer_public/ab/d7/abd70b77-5b42-4c32-af47-7114e9a3c340/ixp_report_2020_.pdf)
- [Source 2] NCSI :: Ranking - National Cyber Security Index (https://ncsi.ega.ee/ncsi-index/)
- [Source 2 - CSIS] Significant Cyber Incidents | Strategic Technologies Program - CSIS (https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents)
- [Source 3] Advanced Persistent Threat Groups Behind DDoS Attacks … - Imperva (https://www.imperva.com/blog/advanced-persistent-threat-groups-behind-ddos-attacks-on-danish-hospitals/)
- [Source 3 - Catchpoint] A Guide to Using DNSSEC to Secure DNS - Catchpoint (https://www.catchpoint.com/dns-monitoring/dnssec-validation)
- [Source 3 - LinkedIn] Martin Lippert's Post - LinkedIn (https://www.linkedin.com/posts/martin-lippert_new-threat-assessment-confirms-the-severity-activity-7399748357146968064-cllY)
- [Source 4] The Danish National Strategy for Cyber and Information Security (https://en.digst.dk/media/bxxcnby2/digst_ncis_2022-2024_uk.pdf)
- [IYP-GRAPH] Internal Knowledge Graph

Chapter 6

Governance

Executive Summary

Denmark's digital governance framework is characterized by strict alignment with European Union standards, robust international cooperation on cybercrime, and a strong constitutional emphasis on freedom of expression. The nation has fully integrated the General Data Protection Regulation (GDPR) through the domestic Danish Data Protection Act, establishing the Danish Data Protection Agency as the primary enforcement body for both public and private sectors [Source 1 (DataFisher)]. Internationally, Denmark has ratified the Budapest Convention, facilitating expedited cross-border investigations and harmonized legal frameworks for cybercrime [Source 1 (UNTC)].

While the telecommunications sector operates under a mandate for regulatory independence derived from the European Electronic Communications Code (EECC) [Source 1 (DLA Piper)], specific mechanisms exist that allow for political intervention in cases of frequency scarcity [Source 3 (Digst)]. There is no evidence of state-sponsored internet shutdowns or widespread social media blocking in the last five years [Source 1 (Yale)]. However, the specific legal architecture governing state surveillance and "kill switch" authority remains opaque within the current intelligence picture [Source 1 (Venice Commission)].

6.1 Legal Framework and International Commitments

Denmark's data privacy landscape is governed by the Danish Data Protection Act, which reinforces GDPR principles including consent, data subject rights, and accountability. The Danish Data Protection Agency actively investigates potential violations and issues penalties, ensuring that both public and private entities adhere to these rigorous standards [Source 1 (DataFisher)].

On the international stage, Denmark's ratification of the Budapest Convention on Cybercrime has significant operational implications. This commitment obligates Denmark to provide mutual legal assistance in obtaining electronic evidence and harmonizes its national laws with international standards regarding offenses such as illegal access and data interference [Source

1 (UNTC)]. Conversely, there is no definitive evidence that Denmark has ratified the Malabo Convention (African Union Convention on Cyber Security and Personal Data Protection), suggesting its strategic focus remains centered on European and Trans-Atlantic frameworks [Source 1 (World Privacy Forum)].

6.2 Telecommunications Regulation and Licensing

The regulatory environment for telecommunications is structured to ensure transparency and impartiality, pursuant to the implementation of the EECC Directive (Directive (EU) 2018/1972) via Act no. 1833 of December 8, 2020 [Source 1 (DLA Piper)]. The Danish Business Authority (DBA) plays a central role in regulating competition within this sector [Source 4 (World Bank)].

Licensing procedures are managed by the Danish Agency for Digital Government (Digst). Applications for numbering resources and frequency licenses are submitted directly to the agency. While the standard procedure prioritizes a "first-come, first-served" approach, the process contains a mechanism for political consideration. In instances of frequency scarcity, the Minister of Digital Affairs retains the authority to determine the assignment method (e.g., auction or tender) based on "essential public interest considerations," indicating that objective technical criteria can be superseded by political priorities under specific conditions [Source 3 (Digst)].

6.3 Digital Rights, Censorship, and Content Regulation

Denmark's approach to online content is rooted in the Danish Constitution, which guarantees freedom of expression. Censorship is generally limited to specific legal infractions such as defamation and hate speech, with recent regulatory focus shifting toward copyright enforcement and unlicensed gambling rather than political suppression [Source 1 (EBSCO)]. Intelligence indicates no definitive evidence of internet shutdowns or widespread blocking of social media platforms in Denmark over the past five years [Source 1 (Yale)].

Despite these protections, the legal framework surrounding state surveillance remains less transparent in the public domain. While Denmark operates under the broader umbrella of European human rights and data protection laws, specific domestic legislation detailing the government's authority to intercept digital communications or implement "kill switches" is not explicitly detailed in available open-source intelligence [Source 1 (Venice Commission)]. Furthermore, while discussions regarding digital sovereignty and age-based social media restrictions are ongoing in the region, no specific recent legislation fundamentally altering the balance between national security and individual rights has been identified [Source 1 (WEF)].

References

- [Source 1 (DataFisher)] How GDPR Compliance is Enforced In Scandinavia and the Nordics (https://datafisher.com/news/how_gdpr_compliance_is_enforced_scandinavia_and_the_nord
- [Source 1 (UNTC)] UNTC (https://treaties.un.org/Pages/showDetails.aspx?objid=0800000280071e5b&cl

- [Source 1 (World Privacy Forum)] Global Table of Countries with Data Privacy Laws, Treaties, or … (https://worldprivacyforum.org/posts/countries-with-data-privacy-laws/)
- [Source 1 (DLA Piper)] Electronic Communication Networks and Services | DLA Piper (https://denmark.dlapiper.com/en/news/electronic-communication-networks-and-services)
- [Source 1 (Digst)] Numbering - Danish Agency for Digital Government (https://en.digst.dk/telecom/teleco
- [Source 3 (Digst)] Licences - Danish Agency for Digital Government (https://en.digst.dk/telecom/spectrur
- [Source 4 (World Bank)] Library Search | Public Private Partnership - World Bank PPP (https://ppp.worldbank.org/library-search?f%5B0%5D=lib_country%3A498&f%5B1%5D=lib_country%
- [Source 1 (EBSCO)] History of Censorship in Denmark | Politics and Government - EBSCO (https://www.ebsco.com/research-starters/politics-and-government/history-censorship-denmark)
- [Source 1 (Yale)] The Kill Switch - Yale Law School (https://law.yale.edu/sites/default/files/area/center/i switch.pdf)
- [Source 1 (Venice Commission)] REPORT ON A RULE OF LAW AND HUMAN RIGHTS COMPLIANT … (https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2024)043-e)
- [Source 1 (WEF)] What is digital sovereignty and how are countries approaching it? (https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/)

Chapter 7

Strategic Synthesis & Roadmap

Chapter 8

Section 7: Strategic Synthesis & Roadmap

To: The Prime Minister / Office of the Executive **From:** Chief Strategy Officer **Date:** October 26, 2025 **Subject:** STATE OF THE NETWORK – The "Sovereign Gateway" Paradox

---

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

The Narrative: A Digital Powerhouse with a Glass Jaw Denmark stands as a global tier-one digital state. We possess the best 5G coverage in the Nordics, a highly digitized citizenry, and critical geopolitical leverage via Greenland and the Havfrue cable system. We are the physical bridge between the North American digital sphere and the European continent.

However, our strategy suffers from a dangerous **Strategic Dissonance**. While your administration is expending significant political capital to achieve "Digital Sovereignty" at the software layer (e.g., phasing out Microsoft for open-source solutions), our foundational network layer is critically exposed. We are locking the digital office doors while leaving the network basement windows wide open.

The Paradox: "High Policy, Low Hygiene" The central contradiction of the Danish digital state is **Advanced Governance vs. Primitive Defense**. * **The Policy:** We rank 16th globally in cyber policy and are aggressively pursuing EU-aligned data autonomy. * **The Reality:** Our routing security is non-existent. With **0.0% RPKI coverage**, the Danish national network is defenseless against BGP hijacking. We are building a "Sovereign" digital government on top of infrastructure that can be rerouted by foreign adversaries without cryptographic resistance.

8.2 2. SWOT Analysis: The Strategic Cheat Sheet

STRENGTHS (Internal)	WEAKNESSES (Internal)
5G Supremacy: 83.4% population coverage; global leader in mobile speeds and low data costs.	**The "Zero-RPKI" Gap:** Complete lack of Route Origin Authorization leaves the entire national grid vulnerable to hijacking.
Geopolitical Real Estate: Greenland and the GIUK Gap provide irreplaceable leverage in NATO/US relations.	**Single Point of Failure:** Extreme dependency on **GlobalConnect A/S** creates a chokepoint where a single failure cascades across 660 dependent networks.
Trusted ID Layer: MitID and CPR provide a unified, state-controlled digital identity backbone.	**Market Commoditization:** Telco price wars have eroded margins, limiting the private sector's ability to self-fund security upgrades.

OPPORTUNITIES (External)	THREATS (External)
The Arctic Data Haven: Leverage Greenland's autonomy and climate to host secure, green hyperscale data centers, moving beyond just military utility.	**Sandworm & Sabotage:** Proven interest by Russian GRU (Sandworm) in targeting Danish energy and healthcare sectors.
EU Sovereignty Leader: Position Denmark as the pilot model for the EU's "interoperable but sovereign" public stack.	**The "Sovereignty Trap":** Aggressive decoupling from US tech (Microsoft) without a mature local alternative risks administrative paralysis.
Nearshoring Hub: Attract sensitive EU data workloads that require GDPR compliance + NATO physical security.	**Cable Severance:** Physical threat to the Blaabjerg landing station and Havfrue cable in the North Sea.

8.3 3. Strategic Roadmap: The Policy Agenda

8.3.1 Phase 1: Immediate Actions (Months 1-6) - "Hardening the Gateway"

- **Objective:** Close the security gap between policy and reality.
- **Action 1 (Executive Decree):** Mandate **RPKI implementation** for all Critical Infrastructure providers (Energy, Telecom, Health) and ISPs serving the state. We must move from 0% to 100% coverage on critical prefixes within 180 days.
- **Action 2 (Audit the Chokepoint):** Commission a classified resilience audit of **GlobalConnect A/S**. If this node fails, Denmark goes dark. We must identify and subsidize a secondary redundancy path immediately.
- **Action 3 (The "Sandworm" Shield):** Deploy active threat hunting teams to the Energy sector OT (Operational Technology) networks, specifically targeting the Zyxel vulnerabilities identified in the May 2023 attacks.

8.3.2 Phase 2: Medium Term (Months 6-24) - "Structural Realignment"

- **Objective:** Balance sovereignty with functionality.
- **Action 1 (Sovereignty Reality Check):** Pause the "Microsoft Exit" for critical defense and intelligence systems until the open-source alternatives are stress-tested for enterprise-grade security. Do not sacrifice operational capability for ideological purity.
- **Action 2 (Market Consolidation):** Direct the Competition Authority to view Telco M&A more favorably. The market is too fragmented to support the necessary security investments. We need fewer, stronger, more profitable operators who can afford to defend the network.
- **Action 3 (Greenland Digital Accord):** Negotiate a specific "Digital Compact" with Nuuk. Offer Danish funding for Arctic fiber redundancy in exchange for guaranteed Danish/NATO oversight of data center investments in Greenland (blocking adversarial capital).

8.3.3 Phase 3: Long Term (Years 2-5) - "The Secure North"

- **Objective:** Denmark as the secure digital vault of Europe.
- **Action 1 (The "Havfrue" Doctrine):** Expand submarine cable landings beyond Blaabjerg to disperse physical risk. Incentivize landings on the East Coast to create a true "ring" of connectivity.
- **Action 2 (Sovereign Cloud Construction):** Instead of just banning foreign software, co-invest with Sweden and Norway to build a **Nordic Sovereign Cloud**. Pool demand to create a commercially viable alternative to US Hyperscalers, rather than relying on fragmented municipal servers.

8.4 4. Final Verdict

8.4.1 Investability Score: HIGH

Explanation: Despite the security flaws, Denmark represents a "Blue Chip" digital asset. The fundamentals—energy, connectivity, legal framework, and 5G penetration—are world-class. The risks identified (RPKI, routing) are technical and fixable with political will, not structural rot. Investors can rely on the stability of the state and the high digital literacy of the workforce.

8.4.2 Maturity Score: MATURE (With Specific Vulnerabilities)

Explanation: Denmark is not "Emerging." It is a fully mature digital society that has become complacent. The infrastructure is advanced, but the security hygiene has lagged behind the pace of digitization. We are a Ferrari with the doors unlocked. The focus must shift from "Digital Transformation" (building new things) to "Digital Resilience" (protecting what we built).