A CALL FOR NORDIC DIGITAL RESILIENCE

Policy recommendations for enhanced cooperation on digital security and resilience in the Nordic region

IT-BRANCHEN TEK NORGE TechSverige FiCom

Introduction

In a time of rising security tensions, an intensified hybrid threat landscape, and deeply integrated digital economies, the Nordic region faces one of its most significant challenges in the digital age.

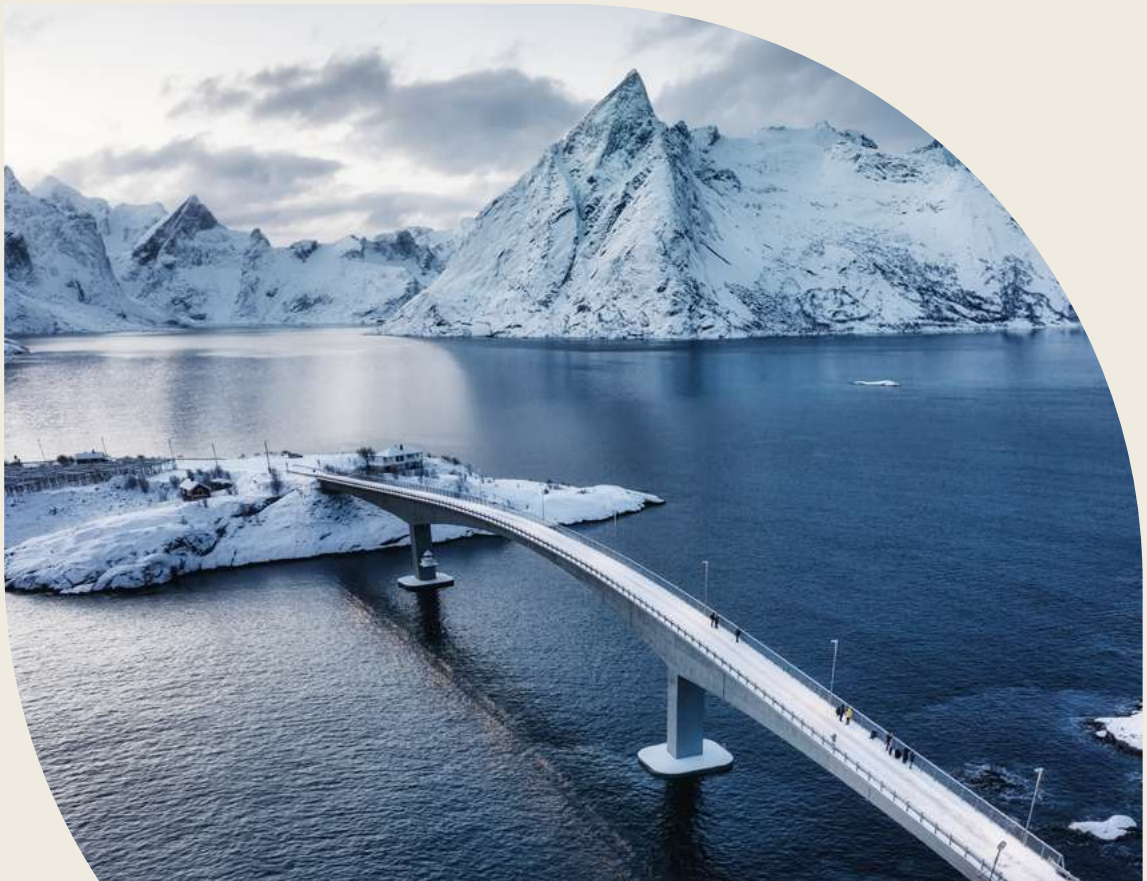
Our societies are increasingly dependent on robust digital infrastructure and secure information systems. Strengthening digital security, resilience, and preparedness therefore requires closer cooperation across the Nordic countries.

Enhanced strategic and operational cooperation is not only desirable – it is necessary to ensure resilience, cohesion, and continuity in an increasingly complex and unpredictable security environment.

The leading tech industry organisations in Denmark, Finland, Norway, and Sweden have therefore launched the Joint Nordic Initiative for Digital Resilience. Through this initiative, the tech industry aims to take responsibility, strengthen public-private collaboration, and enhance cross-border cooperation on critical capabilities for our common defence, digital security, and resilience.

However, concrete barriers – such as inconsistent security clearance processes across the Nordic countries – continue to limit effective cooperation on security and preparedness.

In this paper, we highlight key barriers and present policy recommendation to strengthen Nordic cooperation on digital resilience and the development, operation, and protection of critical digital infrastructure.



Policy Recommendations

The policy recommendations are divided into two sections: Measures to improve framework conditions for digital infrastructure across the Nordic region (1-4), and measures to strengthen Nordic cooperation on cyber security and preparedness (5-6).

01 Working towards a more harmonised and proportionate regulatory framework for digital infrastructure in the Nordic region

Despite the Nordic region's high level of digital integration, differences in national regulatory frameworks continue to create friction for cross-border deployment of digital infrastructure. Digital infrastructure and telecom operators face divergent legislation, permit-granting procedures, approval timelines, and documentation requirements when projects span multiple Nordic countries, leading to delays, higher administrative costs, and reduced predictability for investments.

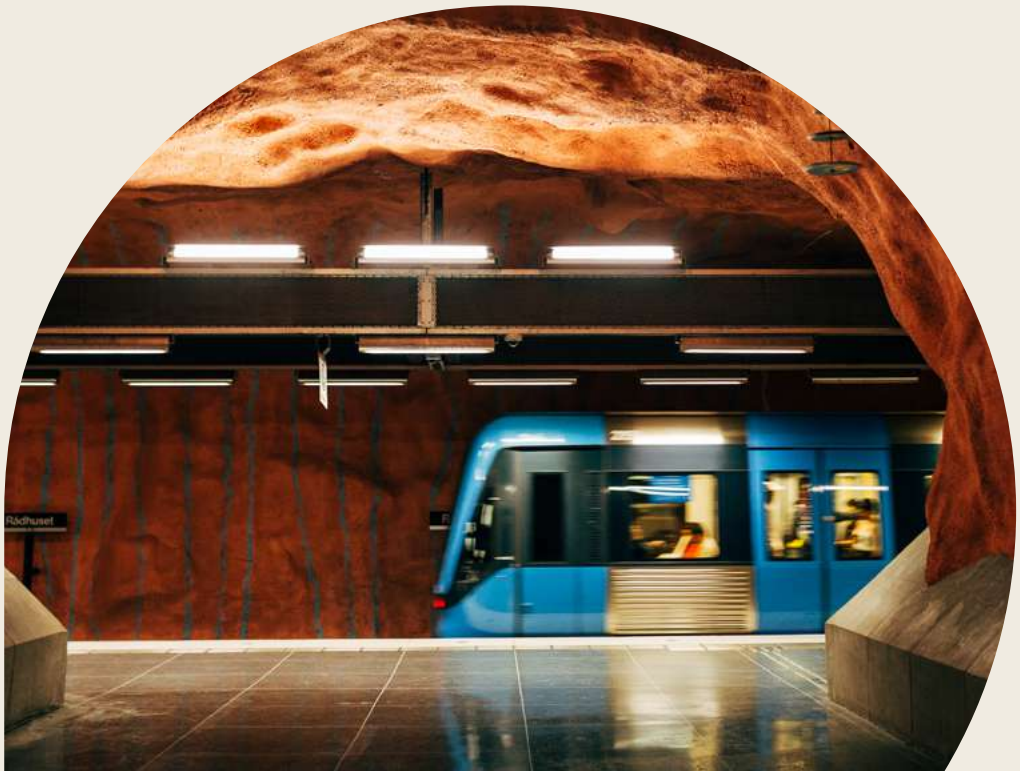
Variation in national rules governing rights of way, environmental assessments, and infrastructure coordination further complicates such projects, thereby limiting the ability to develop coherent cross-border infrastructure at scale.

These challenges highlight the need for closer alignment of regulatory approaches across the Nordic region to enable more efficient and predictable deployment of critical digital infrastructure.

Therefore, we suggest the following:

» Nordic policymakers should investigate opportunities to simplify and harmonise regulatory frameworks for digital infrastructure across the Nordic countries. This includes examining regulatory asymmetries that negatively affect cross-border fibre and subsea cable deployment, such as divergent permitting timelines, approval processes, and funding eligibility criteria.

  Greater Nordic coordination in these areas would not only accelerate infrastructure investments but also enhance redundancy and resilience across the region.



02 A unified Nordic security clearance model

Technology companies operating in the Nordic region need a consistent and predictable framework for assessing and verifying the reliability of their personnel in infrastructure activities. Security clearance frameworks are intended to determine who can be trusted to design, build, operate, maintain, inspect, and repair critical systems and physical infrastructure.

Currently, security clearance processes vary and are not mutually recognised across the Nordic countries. The digital industry (especially within telecoms) reports that without uniform processes, the mobility of experts is hampered, and chains of cooperation are weakened across borders. This e.g. weakens the ability to exchange threat information and build situational awareness and the capacity to respond quickly to cyberattacks on digital infrastructure.

Therefore, we suggest the following:

» *Immediate Nordic recognition of security clearances*: The Nordic countries should identify the key differences in clearance, classification, and access management practices, and agree on a joint operational model that works across these gaps. The Nordic countries must immediately enable cross-border acceptance of personnel security clearances, e.g. building on the 2010 General Security Agreement on the mutual protection and exchange of classified information between Denmark, Finland, Iceland, Norway, and Sweden. In practice, and given that time is of the essence, this agreement should either be revised or supplemented with an appendix that also covers classified personnel, objects, and infrastructure.

  In the short term, a mutually accepted agreement-level solution will allow smooth cross-border operations without major legislative overhauls and support the resilience of our critical digital infrastructure.

» A *common security clearance* model: The long-term ambition for the Nordic countries should be to adopt a unified and interoperable personnel-clearance framework with harmonised criteria, processing standards and times, and effective mutual recognition mechanisms. This would enable expert mobility and cross-border work without unnecessary and time-consuming duplication. This will require changes to national security legislation in the affected countries. In the short term, however, practical steps can and should be taken within existing legal frameworks to accelerate convergence. These could include greater transparency and comparison of national clearance levels, convergence of clearance categories where possible, and fast-track recognition mechanisms for pre-cleared personnel.

03

Facilitation of cross-border data operations and remote network management

Considering the increasing hybrid threats to our digital infrastructure in the Nordic region, ensuring that operators can monitor, manage, and re-route network traffic across borders in real time is becoming essential for maintaining secure and resilient services.

The Nordic countries should therefore strengthen their collective capacity to protect and sustain critical digital infrastructure. From a resilience perspective, cross-border connectivity increases redundancy and reduces single points of failure, enabling rapid incident response and traffic re-routing during outages, cyberattacks, or physical damage, and ensuring continuity of essential services.

Therefore, we suggest the following:

» Together with the digital infrastructure and telecom industry, Nordic policymakers should investigate the possibilities of more harmonised, mutually recognised, and practical framework conditions that allow cross-border infrastructure and operations as well as remote network management, while safeguarding national security and sovereignty concerns, including data access/data residency requirements.

04 Nordic coordination of supply chains for critical technology and digital infrastructure

Increasing geopolitical uncertainty, supply-chain disruptions, and growing dependencies on external actors highlight the need for a more coordinated Nordic approach to critical technologies and digital infrastructure components.

As governments increase efforts and plans to strengthen resilience, supply security, and strategic autonomy in this area, we therefore suggest the following:

» Nordic policymakers should explore closer coordination of supply-chain resilience measures, reflecting the cross-border nature of digital infrastructure. This could include aligning risk assessments, sharing information on critical dependencies, and promoting common approaches to supplier requirements. Where possible, contractual mechanisms (e.g. procurement criteria, security requirements, redundancy obligations) should be used to strengthen resilience, rather than introducing new legislation that may fragment the market further.

» Nordic policymakers should strengthen coordination between civilian and military preparedness requirements, including alignment with NATO and EU frameworks. Given that Nordic digital infrastructure and its supply chains are closely interconnected across borders, greater alignment is needed to avoid conflicting national requirements, to ensure continued cross-bordr access to critical components and services in crisis situations, and to provide clarity for operators under Host Nation Support commitments.

05 Increased cooperation on cyber threat management and response

The Nordic countries are strongly interconnected, and cyber threats increasingly target digital infrastructure across borders. Our ability to detect and respond to cyberattacks therefore depends on timely access to relevant threat intelligence and incident-related information across authorities, digital infrastructure and telecom operators and the cyber security industry throughout the region.

A Nordic-Baltic Cyber Consortium has recently been announced, which will facilitate shared access to commercial cyber threat intelligence and establish a joint data-sharing platform for national cyber authorities.

However, information sharing between public authorities and the private sector remains uneven and often constrained by legal, procedural, and trust-related barriers, limiting the ability to respond quickly and effectively to incidents.

To further strengthen Nordic cooperation on cyber security and resilience, we suggest the following:

- Nordic policymakers should facilitate a structured and timely sharing of threat intelligence and incident-related information with the digital infrastructure and telecom operators and the cyber security industry in accordance with applicable legal and classification frameworks. A prerequisite is a trusted platform for information sharing, both nationally as well as in a Nordic context. Such a platform should enable lawful, secure, and proportionate exchange of relevant data. Clear governance structures, legal safeguards, and defined roles and responsibilities are essential to ensure that information sharing strengthens resilience without undermining national mandates or security requirements.

- The Nordic countries should increase knowledge sharing of best practices regarding national organisation, prevention, incident management, and preparedness efforts within the field of cyber security. This, in turn, will enable dialogue and increased understanding of how national cyber frameworks interact in cross-border situations to help clarify roles, escalation paths, and coordination points, thereby reducing the risk of national cyber measures inadvertently limiting robustness at the Nordic system level.

- Nordic policymakers should initiate the development of a structured, multilateral agreement to coordinate protection, redundancy, and recovery of shared digital infrastructure across the Nordic region. Among other things, this should include harmonized crisis escalation protocols and shared playbooks for coordinated regional response.

- Together, the Nordic countries should expand and improve cooperation on cyber threat management and response in the EU and NATO context.

06 Joint Nordic cyber security and preparedness exercises

Cyber incidents affecting digital infrastructure can escalate rapidly across borders with cascading effects on critical services, supply chains, and societal functions. In such scenarios, unclear roles, misaligned procedures, or delays in cross-border coordination can significantly amplify impacts. Regular, realistic exercises are therefore essential to ensure that existing frameworks function as intended under operational pressure.

National preparedness and contingency frameworks are generally well developed in the Nordic countries, and Nordic cooperation on preparedness and resilience is advancing through frameworks such as Haga and NORDEFCO and through a growing number of joint exercises at the EU and Nordic-Baltic level.

However, these efforts remain distributed across sectors and formats, and do not yet constitute a regular Nordic exercise track specifically focused on cyber incidents affecting cross-border digital infrastructure, where public authorities and operators can jointly test regulatory interfaces, decision-making chains, and operational coordination in real time.

To further strengthen Nordic cooperation on cyber security and resilience, we suggest the following:

» Nordic policymakers should initiate the design and carrying out of controlled Nordic cyber preparedness exercises, limited in both scope and geography, with a primary focus on coordination rather than technology, bringing together public authorities, defence actors, and private digital infrastructure, telecom, and cyber security operators. The purpose would be to test how existing rules and processes work in cross-border scenarios and to identify practical bottlenecks before they arise in real crisis situations.

About the Joint Nordic Initiative for Digital Resilience

The Joint Nordic Initiative for Digital Resilience brings together the leading tech industry organisations in Denmark, Finland, Norway, and Sweden to enhance Nordic cooperation on digital infrastructure, cyber security, and preparedness. The initiative is founded on a shared recognition that stronger public-private collaboration and closer cross-border cooperation are essential to protect critical digital infrastructure and reinforce societal resilience in an increasingly complex security environment.

The initiative is driven by IT-Branchen (Denmark), TEK Norge (Norway), TechSverige (Sweden), and FiCom (Finland). Together, the organisations represent a broad Nordic tech sector committed to contributing actively to the region's common digital security and resilience.

IT-BRANCHEN TEK NORGE TechSverige FiCom