Nordregio

NORDREGIO POLICY BRIEF 2026:2

TRANSPARENCY vs SECURITY

Enhancing connectivity under the Gigabit Infrastructure Act, NIS2 and 5G

Nicola Wendt-Lucas
Maja Brynteson

Table of contents

This publication is also available online in a web-accessible version at:
https://pub.nordregio.org/pb-2026-2-transparency-vs-security

Summary

The Gigabit infrastructure Act (GIA) is central to the European Union's strategy for universal high-speed digital connectivity, as disparities in access – especially between urban and rural areas – persist. In the sparsely populated Nordic-Baltic region, the GIA holds particular promise: it can help close long-standing digital divides in rural, remote and cross-border communities, thereby unlocking regional development, economic revitalisation and digital inclusion. While the GIA removes barriers and accelerates deployment, it does not require Member States to directly invest in broadband infrastructure. Instead, it obliges authorities to create a streamlined, transparent and coordinated regulatory environment that enables more efficient private-sector rollout. However, in a time of heightened geopolitical sensitivities and insecurities, the GIA's ambitions for transparency, accelerated rollout and market-driven expansion must be reconciled with (cyber)security imperatives, such as those set out in the NIS2 Directive. This brief explores how the countries of the Nordic-Baltic region can balance these objectives to deliver secure, future-proof and regionally inclusive connectivity.

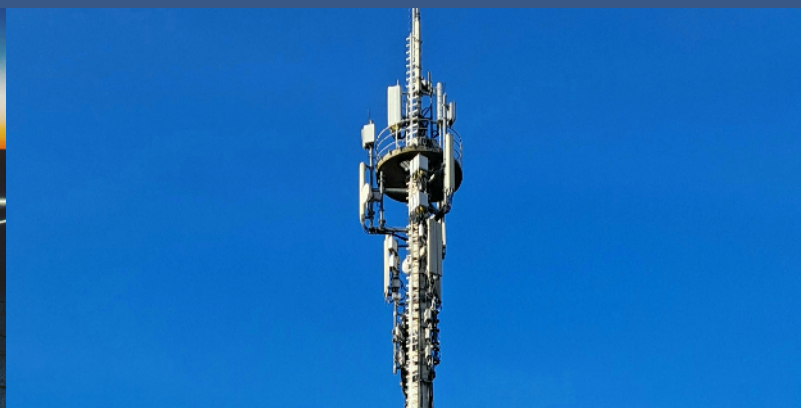
Sammanfattning

Gigabitinfrastrukturakten (GIA) är central i Europeiska unionens strategi för universell höghastighetsanslutning, eftersom skillnader i digital uppkoppling, särskilt mellan urbana och rurala områden, fortfarande kvarstår. I den glest befolkade nordisk-baltiska regionen har GIA särskild potential: den kan bidra till att överbrygga långvariga digitala klyftor i landsbygdsområden, avlägsna regioner och gränsregioner – och därigenom främja regional utveckling, ekonomisk återhämtning och digital inkludering. Samtidigt som GIA undanröjer hinder och påskyndar utbyggnaden kräver den inte att medlemsstaterna direkt investerar i bredbandsinfrastruktur. I stället ålägger den myndigheterna att skapa en strömlinjeformad, transparent och samordnad regleringsmiljö som möjliggör en mer effektiv utbyggnad av infrastrukturen av privata aktörer. Men i tider av ökade geopolitiska spänningar och osäkerheter måste GIA:s ambitioner om transparens, snabb utbyggnad och marknadsdriven expansion balanseras mot (cyber)säkerhetskrav, såsom de som anges i NIS2-direktivet. Denna policybrief utforskar hur länderna i den nordisk-baltiska regionen kan balansera dessa krav för att leverera säker, framtidssäkrad och regionalt inkluderande uppkoppling.

List of acronyms

5G	5th generation mobile network
BCRD	Broadband Cost Reduction Directive
CER	Critical Entities Resilience Directive
DDoS	Distributed Denial of Service
DNA	Digital Networks Act
GIA	Gigabit Infrastructure Act
ICT	Information and Communication Technology
NIS2	Network and Information Security Directive
SIP	Single Information Point
VHCN	Very High-Capacity Network

1. Background and problem statement



Images: Federico Beccari and Michael Schreiber / unsplash.com

The Nordic and Baltic countries – while internationally recognised for their digital leadership – continue to face disparities in access to high-speed internet connectivity. These inequalities are most pronounced in the region's numerous sparsely populated and remote rural areas, including Arctic and sub-Arctic communities, archipelagos and certain cross-border regions. In these locations, residents and businesses often experience limited broadband access, poor mobile coverage (especially 5G) and a lack of long-term, competitive infrastructure investment (European Commission, 2025a). These connectivity gaps not only hinder access to essential public services like healthcare, education and emergency response, but also limit regional economic potential and can be considered a key contributor to the widening urban-rural digital divide (de Jesus & Melander, 2024).

The Gigabit Infrastructure Act (GIA) was introduced by the European Commission in 2024, replacing the Broadband Cost Reduction Directive (BCRD) from 2014. Implementation of the BCRD had been inconsistent across Member States and no longer met the increasing demand for fast and reliable digital connectivity in Europe (European Commission, 2025b). The goal of the GIA is to promote universal access to very high-capacity networks (VHCNs), in line with the connectivity targets set out under the EU's Digital Decade initiative. These targets specify that by 2030, all EU households should have access to a fixed gigabit network and all populated areas should be covered by 5G (European Commission, 2025c). However, affordability issues are likely to persist. As seen in peri-urban and rural areas where gigabit connections are availably but subscription prices remain prohibitive, economic barriers may continue to limit effective access (OECD, 2024).

The Digital Networks Act (DNA), adopted in January 2026, modernises the EU's rules for digital connectivity. It aims to reduce market fragmentation, encourage investment and strengthen the resilience of Europe's communications infrastructure. The Act aims to create a single, harmonised framework that supports cross-border operations, simplifies authorisations and streamlines regulation. Key measures include a "Single Passport" for operators, clearer rules for innovative digital services, an EU-level preparedness plan for network resilience and improved conditions for spectrum use. Overall, it is designed to foster a more competitive, innovative and secure digital ecosystem across the Union (European Commission, 2026).

Several instruments introduced under the GIA are aimed at simplifying infrastructure rollout, encouraging private investment and ensuring transparency in deployment (European Commission, 2025b), see Fact Box 1. For example, a telecommunications company deploying fibre can leverage existing infrastructure under the GIA, such as water ducts, instead of initiating new construction works. Essential information about current infrastructure and planned civil works will be made available through digitally accessible "Single Information Points[1]" (SIP) in each country to further facilitate this process. The GIA will further enhance digital accessibility by streamlining and digitising permits for rollout activities, requiring authorities to meet strict deadlines to enable quicker deployment and reduced costs (European Commission, 2025b).

The regulation is especially relevant to the Nordic-Baltic region, where connectivity challenges stemming from regional physical conditions intersect with broader development objectives, such as the goal of the Nordic and Baltic Ministers of Digitalisation for the region to become the most digitally integrated in the world by 2030 (Nordic Council of Ministers, 2024b). The simplified deployment of high-speed digital connectivity in underserved areas will facilitate more affordable and efficient access for Internet Service Providers, potentially enhancing connectivity in rural and economically less prioritised parts of the region. The GIA's emphasis on transparency aims to enhance trans-border collaboration and knowledge-sharing practices, further supporting the rollout process in rural areas while fostering innovation. The harmonised regulatory framework, including Single Information Points, for instance, will help multinational telecom companies and cross-border consortia to plan, build and operate more seamlessly across borders. The regulation also provides for regular reporting, monitoring and benchmarking on an EU level to ensure continuous improvements and mutual learning practices across the Member States (The European Parliament & the Council of the European Union, 2024).

1. In the context of the Gigabit Infrastructure Act (GIA), "Single Information Points" refer to digital platforms provided on a national level that offer essential information about existing infrastructure and planned civil works (The European Parliament & the Council of the European Union, 2024).

FACT BOX 1: THE GIGABIT INFRASTRUCTURE ACT (GIA)

Implementation timeline
Entered into force: 11 May 2024
Fully applicable: November 2025

Purpose
To help achieve the European Union's 2030 Digital Decade connectivity goals by facilitating the rollout of very high-capacity networks, ensuring EU-wide access to fast gigabit connectivity and high-speed mobile data by 2030.

Measures
Render the rollout of gigabit networks simpler, cheaper and faster by
1. reducing bureaucratic hurdles;
2. encouraging the shared use of existing infrastructure;
3. improving the coordination of public works to install fibre; and
4. ensuring that buildings are equipped with high-speed internet.

Expected impact
- Faster and cheaper network deployment
- Reduction in greenhouse gas emissions
- More equal access to fast, stable and affordable internet, generating numerous benefits for citizens and companies, including in terms of digital innovation and inclusion

Source: European Commission, 2025b.

At the same time, the GIA's objectives are being implemented in a region marked by heightened geopolitical sensitivities. In 2024 and 2025, several incidents involving damage to undersea cables connecting the Nordic and Baltic countries in the Baltic Sea raised suspicions of sabotage (Reuters, 2024; SVT Nyheter, 2025). These events highlighted not only the cascading and transboundary effects of attacks on critical infrastructure but also intensified discussions concerning the resilience and protection of such infrastructure, with particular emphasis on telecommunication links between these nations. In addition, incidents may arise not only from deliberate acts of sabotage but also as a result of accidents and wear-and-tear over time.

The increasing risk of hybrid and cyber threats indicates that enhancement of digital connectivity and the increasing reliance on digital services in the Nordic and Baltic countries also introduce new vulnerabilities and hence significant national security considerations. While past events have prompted increased cooperation among the countries, additional measures, including legal ones, will be necessary to address risks in a sustainable and harmonised manner (Aula et al., 2020; Fjäder & Schalin, 2024).

One key instrument in this regard is the latest Network and Information Security Directive (NIS2), which strengthens cybersecurity protocols for essential infrastructures (European Commission, 2025d). While primarily complementing the GIA, certain aspects require a balancing act by the Member States, particularly regarding the GIA's emphasis on transparency and openness and the NIS2's focus on risk containment. Although these two regulatory regimes share an overarching purpose, they can create ambiguities and procedural complexities, posing challenges for maintaining and fostering transparency and cross-border innovation in the context of increased security risks (European Commission, 2024a).

FACT BOX 2: THE NETWORK AND INFORMATION SECURITY DIRECTIVE (NIS2)

Implementation timeline
Entered into force: January 2023
Implementation by October 2024 (however, as of May 2025, transposition is still ongoing in 19 Member States)

Purpose
To enhance cybersecurity resilience across the European Union.

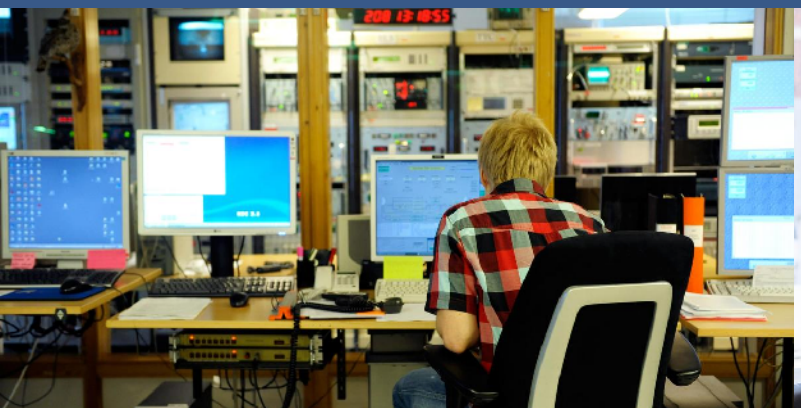
Measures
Key NIS2 measures include:
1. expanding the scope of essential and important entities required to comply with the NIS2;
2. imposing higher demands on cybersecurity standards, including technical, operational and organisational measures, as well as managerial oversight and training;
3. mandatory incident reporting to the respective national competent authority;
4. granting national authorities greater powers to audit, investigate and sanction entities that fail to comply; and
5. deepening EU-level cooperation on incident response, guidance and threat intelligence.

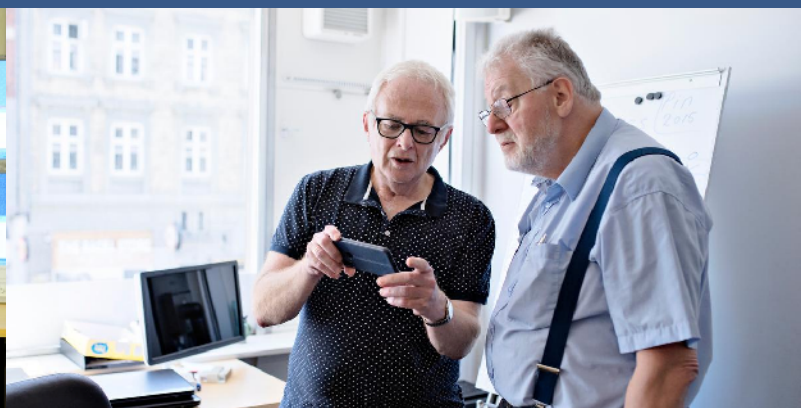
Expected impact
- Improved incident response
- Increased cyber resilience among businesses and entities critical to the economy and society
- Harmonised standards

Source: European Commission, 2025e; The European Parliament & the Council of the European Union, 2022.

These challenges particularly impact the municipalities and local operators responsible for implementation (Sveriges Kommuner och Regioner, 2023b). Under the GIA, municipalities bear significant responsibility for enabling the faster rollout of improved connectivity (European Commission, 2025b). It has been noted that smaller or more rural municipalities may face additional strain due to their limited technical and legal resources for ensuring compliance, while simultaneously attracting new infrastructure investments (Sveriges Riksdag, 2023). Consequently, targeted policy coordination, guidance and support are necessary to realise the transformative potential of the GIA in politically complex areas where it is most required.

2. Analysis





Images: Johannes Jansson and Maud Lervik / norden.org

Balancing different mandates

The GIA states that "*limited access and insufficient network expansion can deepen social inequalities, thus creating a new digital divide between people who are able to benefit fully from an efficient and secure digital connectivity, allowing them to access a wide range of services, and people who are unable to do so. In that regard, the roll-out of VHCNs in rural, remote and scarcely populated regions, as well as in social housing, should be a priority for public investment projects, as a key aspect of social inclusion.*" (The European Parliament & the Council of the European Union, 2024, p.1). The GIA thereby highlights the deep interconnection between social and digital inclusion and draws renewed attention to the persistent challenges linked to the urban-rural digital divide.

Accordingly, the GIA can be regarded as both a digital policy instrument and as a regional development facilitator. By accelerating the implementation of gigabit-speed networks and fifth-generation mobile services in underdeveloped areas, the GIA has the potential to promote economic revitalisation in sparsely populated areas by supporting innovative business models – such as those related to green energy, remote healthcare and smart logistics solutions – and providing the necessary infrastructure to attract labour, thereby fostering growth in previously underserved regions. Furthermore, the GIA may also contribute to broader cohesion objectives by more closely integrating cross-border and transnational regions into the EU's digital and economic framework (The European Parliament & the Council of the European Union, 2024).

However, the very features that make the GIA ambitious – in particular, its commitment to transparency and market facilitation – also give rise to a series of security challenges. The Act requires operators to provide detailed, and often publicly accessible, information

about where infrastructure is being deployed, who is building it and how coverage is progressing (European Commission, 2025b). While such openness is crucial for coordination, collaboration, investment and democratic accountability, it also increases the exposure of sensitive infrastructure components – especially in areas close to critical national assets, border zones or regions with known hybrid threat activity (European Commission, 2023a).

Across the Nordic-Baltic region, critical infrastructure is defined through various national approaches, which are increasingly being harmonised by EU directives such as the NIS2 and the Critical Entities Resilience (CER) Directive (European Commission, 2025d). In **Sweden** and **Finland**, centralised, legislation-based models are applied. For example, **Finland** explicitly lists both public and private entities, including ICT service providers and regional broadband networks (Traficom, 2025). By contrast, the **Baltic states** and **Denmark** employ more decentralised or risk-based approaches. **Latvia's** legislation empowers multiple authorities to designate operators based on risk assessments, while **Estonia's** approach centres on sectoral regulators and ad hoc coordination measures (Cobalt, 2024; Information System Authority, 2022).

Certain legal acts take precedence over the EU Gigabit Infrastructure Regulation (European Commission, 2025b). In **Sweden**, this hierarchy is addressed in the "Gigabit Enquiry Report", published as part of the Swedish Government Official Reports, which states that "*If a provision in Directive 2002/77/EC, the Code, or the NIS2 Directive conflicts with the GIA, the provisions of the directives shall take precedence. This means, in our view, that the Electronic Communications Act and the legislation that will implement the NIS2 Directive take precedence over the GIA, to the extent that the Swedish legislation transposes the said directives.*" (SOU, 2025, p.107).

Furthermore, several authorities in **Sweden** note that ensuring sufficient expertise in cybersecurity and supervision poses a major challenge. They report that it is difficult to recruit appropriately qualified specialists, particularly for newly established supervisory authorities. In addition, the authorities need resources to maintain and develop employees' skills over time (Statskontoret, 2025).

Strengthening cyber defence will require substantial investment to maintain a high and consistent level of cybersecurity. KL, the interest organisation of the **Danish** municipalities, expects municipal expenditures to be significant, while noting that the exact amount will depend on future sector-specific rules (KL, 2024).

Municipalities must balance the transparency requirements under the GIA with the stringent cybersecurity obligations under the NIS2 without placing excessive strain on local resources. According to an **Estonian** respondent, this can be achieved by adopting a need-to-know approach to data sharing. While certain information should remain publicly accessible to fulfil the transparency objectives of the GIA, technical details should be available on a need-to-know basis. For example, in the case of Single Information Points (SIP), data may be presented at an aggregated level, with more detailed technical specifications available exclusively upon direct request to the infrastructure owner (Estonian respondent).

Variations in implementation

In **Finland**, the Ministry of Transport and Communications (Traficom) is tasked with preparing the government's proposal for an amendment to national legislation, which is presently based on the Broadband Cost Reduction Directive (BCRD). The new legislation, which is aligned with the GIA, entered into force on 12 November 2025. To meet the requirements of both the BCRD and the GIA, Traficom has proactively developed a Single Information Point (SIP), which has operated in accordance with the GIA since 2017. According to Finnish authorities, the new national legislation based on the GIA is largely consistent with existing frameworks regarding data security and transparency. Access to data is primarily restricted under national law in relation to critical infrastructure. Notably, no significant challenges have been reported in balancing these aspects within the GIA context. The established SIP does not include detailed physical infrastructure location data; instead, requests for such data are transmitted to the relevant network operator, and strong electronic identification is required for SIP users. This approach has helped avoid conflicts between requirements under the GIA and national security or public data access legislation (Finnish respondent).

The differing approaches to the NIS2 influence how infrastructure is classified and protected. In **Finland**, a regional broadband provider might automatically be subject to critical infrastructure obligations, whereas in **Estonia** its designation may depend on factors such as size, sectoral risk or national interest (Finnish respondent & Estonian respondent). These variations shape how the NIS2 obligations are operationalised, determining which entities are subject to cybersecurity rules, how responsibilities are assigned and what resources are available for compliance. This issue is particularly pertinent in the context of the GIA, under which entities such as local utilities, infrastructure owners or regional broadband providers – which may or may not be classified as critical under national law – are now expected to open up physical infrastructure for shared use while also securing it to the standards required by the NIS2.

For example, a municipally owned broadband provider in rural **Latvia** – without clear designation as a critical entity – might be required under the GIA to grant access to its network ducts to third-party providers yet lack the cybersecurity protocols mandated by the NIS2 to manage potential risks or prevent unauthorised tampering. Conversely, a regional network operator in **Finland**, already classed as a critical entity under national law, could face conflicting obligations: under the NIS2, it may restrict data access or infrastructure sharing to preserve system integrity, while the GIA obliges it to accommodate co-deployment or disclose asset maps to other providers.

In **Lithuania**, the Ministry of Defence is responsible for transposing the NIS2 into national legislation, with primary legislation – specifically the cybersecurity law – already amended accordingly. As of spring 2025, the GIA had not yet been fully implemented. Practical measures are being coordinated across several Lithuanian ministries to ensure that the articles of the EU regulation are not only implemented but also workable in practice. While the regulation is directly applicable, these ministries are actively involved in developing operational steps to make its provisions functional (Lithuanian respondent).

In countries with clear designation mechanisms, GIA stakeholders may already be subject to critical entity rules and equipped to manage the associated obligations. In other countries, gaps in designation or coordination can leave rural operators uncertain about how to balance transparency and security in practice – an issue that particularly affects rural regions (European Commission, 2024b). These tensions could have consequences that significantly shape the long-term impact of the GIA. Delays or reluctance to grant access due to security concerns may slow broadband expansion in underserved rural areas, undermining the GIA's core objective. At the same time, higher costs associated with meeting both transparency and cybersecurity requirements could reduce incentives for infrastructure sharing or raise prices for end users (Frontier Economics, 2022).

Furthermore, inconsistent enforcement across countries risks fragmenting the single market for broadband infrastructure, with some regions embracing openness and others restricting access. Insufficiently secured infrastructure sharing could increase vulnerability (NIS Cooperation Group, 2024). On the other hand, these challenges also present opportunities: they may catalyse stronger Nordic-Baltic collaboration on harmonised cybersecurity standards, enhanced joint threat intelligence sharing and coordinated incident response (Nordic Council of Ministers, 2024a).

This dynamic is further underscored by real-world threats. Ransomware attacks on **Swedish** municipalities (Region Norrbotten, 2025), DDoS campaigns targeting **Estonian** public services (Information System Authority, 2023) and infrastructure disruptions in **Lithuania** (Kottasová et al., 2024) have exposed the vulnerability of local-level actors. These developments highlight the importance of harmonising national definitions, ensuring local compliance capacity and embedding infrastructure development within a robust, regionally coordinated security framework to facilitate digital expansion through the GIA.

Local implications and considerations

While complementary, these regulatory regimes may still inadvertently stall progress. Local actors – tasked with implementing rollout plans, partnering with vendors and reporting on progress – may face ambiguity over what information can be shared and what must be secured. In regions already struggling with underinvestment and limited administrative capacity, such friction can delay projects, discourage private-sector involvement and expose communities to unmanaged risk (Regeringskansliet, 2023; Sveriges Kommuner och Regioner, 2023a).

Several countries have reported delays arising from unclear guidance and transparency obligations associated with the NIS2's cybersecurity requirements (European Commission, 2025e). The burden on municipalities and regions is acute. Many local governments – especially those in sparsely populated or economically lagging areas – lack the technical expertise, legal advisory capacity and financial resources to navigate the dual demands of infrastructure openness and cybersecurity compliance (European Commission, 2023b). Ongoing examinations and policy dialogue across the Nordic-Baltic region are beginning to unpack these tensions. For example, in **Denmark**, municipalities are now classed under

the NIS2 but reportedly lack the expertise, budget and staff to meet the new cybersecurity requirements, especially in smaller or rural communities (CBS, 2025).

The municipal burden is not merely a matter of compliance paperwork but reflects deeper structural capacity challenges. Smaller municipalities in the Nordic-Baltic region often operate with limited IT departments, and cybersecurity is frequently managed as an add-on responsibility rather than as a dedicated function (European Commission, 2023b). This creates a double bind: while the GIA obliges local authorities to facilitate infrastructure access and transparency, the NIS2 classifies them as essential service providers, thereby requiring investments in advanced security measures, incident reporting and risk management systems. For wealthier urban municipalities, these requirements can be absorbed through existing administrative frameworks; for rural or underfunded regions, they impose additional strain on already constrained budgets (CBS, 2025; Sveriges Kommuner och Regioner, 2024).

Estonia intends to provide financial assistance to entities that are new to Estonian cybersecurity law, including the majority of providers of public electronic communications networks and publicly available electronic communications services. This support will not extend to municipal entities, as they are already required to comply with existing cybersecurity obligations. The funding will primarily cover two areas: (1) conducting a review of current cybersecurity measures and developing a roadmap to achieve the required standards, and (2) supporting the implementation of activities identified within that roadmap (Estonian respondent).

For example, in **Sweden**, all municipalities and regions will be subject to the NIS2 requirements – not only for those sections of their activities that fall under NIS2 sectors but also for the organisation as a whole. This presents significant challenges for smaller municipalities. Recognising the financial constraints associated with implementing cybersecurity measures in line with the NIS2, the Swedish government has decided on permanent budget increases for all municipalities and regions (Swedish respondent). In addition, the Swedish government considers that maintaining a consistent level of cyber resilience among key operators may generate long-term cost savings for these operators, although short-term expenditures may be required to meet the requirements of the NIS2 (Regeringen, 2025).

In **Finland**, Traficom reports that the main impact has been the development and monitoring of the SIP to ensure network operators submit their information as required. According to Finnish respondents, the use of decentralised systems – where requests for detailed infrastructure data are transmitted directly to the relevant parties – is encouraged. The monitoring of SIP usage is facilitated through strong electronic identification, thereby enhancing security and accountability. Sensitive infrastructure details are not stored within the SIP itself; rather, the SIP is designed to function as a gateway, allowing controlled access to such data. This approach, as described by the Finnish sources, has proven effective in safeguarding critical information while enabling efficient processing of legitimate requests (Finnish respondent).

The result is a growing discrepancy in implementation capacity. Some municipalities are able to advance GIA rollout plans relatively smoothly, while others postpone or scale back

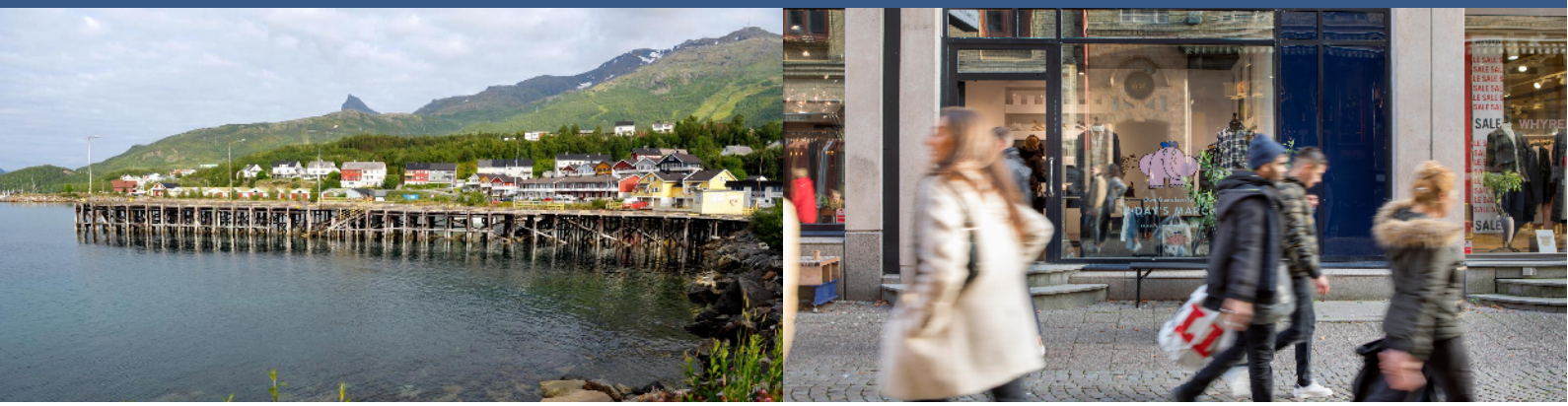
projects until national authorities provide clearer interpretive guidance or additional financial support. In practice, this means that the areas most in need of rapid broadband deployment – remote or rural areas and sparsely populated communities – are also most likely to experience delays. Such uneven capacity risks widening existing regional digital divides. Scalable governance frameworks that can balance openness with resilience are therefore needed. Without a harmonised interpretive framework at the EU level, local actors remain vulnerable to legal uncertainty and operational fragmentation.

In relation to both the GIA and the NIS2, national authorities play a crucial role in ensuring effective implementation at the local level. Through the provision of guidelines, dissemination of information and structured communication, they can offer essential support to municipalities in interpreting and complying with EU and national legislation, as well as in understanding the obligations these frameworks impose (Swedish respondent).

To fully unlock the development and strategic potential of the GIA in the Nordic-Baltic region, it is therefore essential to clarify its implications for cybersecurity, particularly in rural and remote areas. This will require clear interpretive guidance, stronger alignment between digital and regional policy goals and concrete support for local actors on the frontlines of building and securing Europe's digital frontier.

National governments should provide clear guidance and disseminate best practices on these matters, complemented by the organisation of workshops and seminars to build capacity. While financial support is also important, budgetary constraints may limit the extent to which governments can offer such assistance, necessitating careful evaluation of this option. It is anticipated that EU funds could be utilised for this purpose; in such cases, the requirements for accessing financial support should be designed to minimise administrative burdens, ensuring applicants are not subjected to excessive bureaucracy (Estonian respondent).

3. Policy recommendations



Images: Johannes Jansson / norden.org and Marie Ullnert / imagebank.sweden.se

To support effective implementation of the Gigabit Infrastructure Act alongside evolving cybersecurity obligations under the NIS2, particularly in rural and cross-border contexts, the following points should be considered to ensure alignment between connectivity goals and resilience requirements:

1. Align GIA implementation with regional governance and risk frameworks:

The GIA is not a purely technical infrastructure rollout tool – its ambitions are deeply embedded in national and regional risk management cultures and administrative capacities. This is of particular importance for rural areas and cross-border scenarios, where resource constraints and jurisdictional complexities are most pronounced. Policymakers should prioritise the harmonisation of GIA rollout with established frameworks to foster sustainable infrastructure development and effective risk mitigation.

2. Provide operational guidance on the GIA–NIS2 interplay for local authorities:

Legal uncertainties can be mitigated by offering actionable, operational-level tools. This includes not only clarifying where responsibilities sit under each directive but also providing concrete examples of how local authorities can integrate resilience requirements into connectivity planning. Showcasing good practice from early adopters, particularly in rural or cross-border areas facing similar resource and capacity constraints, can help authorities translate regulatory obligations into practical workflows.

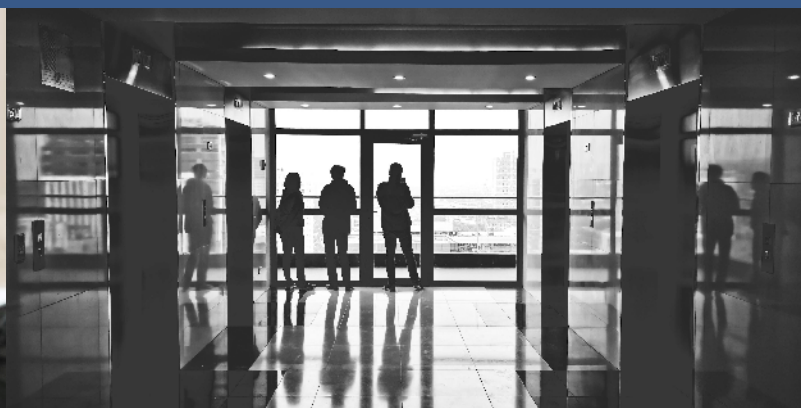
3. Strengthen rural cybersecurity capacity through shared services and preparedness:

Rural or smaller stakeholders, such as municipalities, may be uncertain of their legal status or under-equipped to handle NIS2-level responsibilities. Addressing these vulnerabilities requires structured institutional support, including technical assistance programmes and cross-border knowledge-sharing hubs. These initiatives should focus on enhancing cybersecurity preparedness, clarifying legal responsibilities, and providing access to expert recourses.

4. Monitor and evaluate GIA–NIS2 interaction over time:

Regular impact assessments, performed by for example national and regional authorities, can evaluate how the GIA affects cybersecurity resilience over time, informing future updates and deployment strategies. Clear division of responsibility, who gathers data - who validates compliance, who follows up on identified risks - helps ensure that evaluations are not only systematic but also actionable.

4. Conclusion



Images: Magnus Fröderberg / norden.org and Yves Denzel / unsplash.com

The Gigabit Infrastructure Act represents a strategic opportunity to enhance regional cohesion, economic resilience and digital inclusion. For the Nordic-Baltic region, its implementation should address cybersecurity risks and the impact of high-speed connectivity on rural and remote communities. Policymakers must balance transparency in deployment with infrastructure protection, ensuring that digital policies align with regional development strategies to achieve both secure and equitable digital outcomes. This also positions the Nordic-Baltic region to take the lead in establishing a harmonised approach to security standards, ensuring that infrastructure deployments are efficient, inclusive and resilient against emerging cybersecurity threats.

The most significant challenges are faced by rural areas, which often contend with limited administrative capacity, ambiguous guidance, and overlapping regulatory obligations under both the GIA and NIS2. Without targeted support, there is a tangible risk of delayed rollouts and increased vulnerability, widening existing digital divides. To mitigate these risks, national and regional actors should provide clear operational guidance, harmonise security standards and strengthen local capacity through shared services and funding support.

By aligning regulatory frameworks and long-term investment strategies, the Nordic-Baltic region can shape the direction of secure and inclusive digital infrastructure development. The establishment of harmonised security frameworks and the delivery of robust support to local actors will ensure that infrastructure rollouts are not only efficient and equitable but also resilient in the face of evolving cybersecurity threats.

Bibliography

Aula, I., Amundsen, R., Buvarp, P., Harrami, O., Lindgren, J., Sahlén, V., & Wedebrand, C. (2020). *Critical Nordic Flows: Collaboration between Finland, Norway and Sweden on Security of Supply and Critical Infrastructure Protection*. the Finnish National Emergency Supply Agency; the Norwegian Ministry of Trade, Industry and Fisheries; and the Swedish Civil Contingencies Agency.

CBS. (2025, September 18). *Denmark is not ready for EU's new cyber security rules*. CBS - Copenhagen Business School. https://www.cbs.dk/en/cbs-agenda/areas/news/denmark-is-not-ready-eus-new-cyber-security-rules

Cobalt. (2024). *Summary of Latvia's new national cyber security law*.

de Jesus, A., & Melander, S. (2024). *From Vision to Practice – Insights from Nordic-Baltic 5G applications across sectors* (No. 2024:11). Nordregio. https://pub.nordregio.org/r-2024-11-from-vision-to-practice-insights-from-nordic-baltic-5G-applications-across-sectors/index.html

European Commission. (2023a). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures to reduce the cost of deploying gigabit electronic communications networks and repealing Directive 2014/61/EU (Gigabit Infrastructure Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0094

European Commission. (2023b). *Regions' and cities' digital resilience is key to prevent cyber-attacks and secure the continuity of local public services*. https://ec.europa.eu/newsroom/eucor/items/845491/en

European Commission. (2024a). *White Paper - How to master Europe's digital infrastructure needs? | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs

European Commission. (2024b). *The CER and NIS2 Directives enter into application*. https://ec.europa.eu/newsroom/cipr/items/859754/en

European Commission. (2025a). *Digital Decade DESI visualisation tool*. https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/key-indicators/charts/analyse-one-indicator-and-compare-countries?indicator=rid_c_fbbtc&indicatorGroup=rid&breakdown=hh_deg3&period=2021&unit=pc_hh&country=AT,BE,BG,CY,CZ,DE,DK,EE,EL,ES,EU,FI,FR,HR,HU,IE,IT,LT,LU,LV,MT,NL,PL,PT,RO,SE,SI,SK

European Commission. (2025b). *Gigabit Infrastructure Act | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/gigabit-infrastructure-act

European Commission. (2025c). *Support for digital connectivity | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/digital-connectivity-support

European Commission. (2025d). *NIS2 Directive: Securing network and information systems | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

European Commission. (2025e). *NIS2 Directive transposition in EU countries | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/nis-transposition

European Commission. (2026). *The Digital Networks Act*. https://digital-strategy.ec.europa.eu/en/policies/digital-networks-act

Fjäder, C., & Schalin, J. (2024). *Building resilience to hybrid threats: Best practices in the Nordics*. Hybrid CoE Working Paper 31.

Frontier Economics. (2022). *Assessing the economic impact of EU initiatives on cybersecurity*.

Information System Authority. (2022). *Cyber defence of critical infrastructure | RIA*. https://www.ria.ee/en/cyber-security/cyber-defence-critical-infrastructure

Information System Authority. (2023). *September was a month of denial-of-service attacks in Estonian cyberspace | RIA*. https://ria.ee/en/news/september-was-month-denial-service-attacks-estonian-cyberspace

KL. (2024). *Bilag – til KLs høringssvar til hovedlov om NIS2*. https://www.kl.dk/media/wx5pggru/bilag-kls-hoeringssvar-vedr-implementering-af-nis2-i-danmark.pdf

Kottasová, I., Stockwell, B., & Murphy, P. P. (2024, November 18). *Two undersea cables in Baltic Sea disrupted, sparking warnings of possible 'hybrid warfare'*. CNN. https://www.cnn.com/2024/11/18/europe/undersea-cable-disrupted-germany-finland-intl

NIS Cooperation Group. (2024). *Cybersecurity and resiliency of Europe's communications infrastructures and networks*.

Nordic Council of Ministers. (2024a). *Joint statement, Nordic and Baltic Ministers of Digitalisation*. https://www.government.se/contentassets/df62239cac10424b89825436635981cd/ncm-digital_joint-statement_subsea-communication-cables_2024.pdf

Nordic Council of Ministers. (2024b). *Nordic-Baltic Cooperation Programme for Digitalisation 2025 to 2030*.

OECD. (2024). *OECD Digital Economy Outlook 2024 (Volume 2): Strengthening Connectivity, Innovation and Trust*, OECD Publishing, Paris, https://doi.org/10.1787/3adf705b-en.

Regeringen. (2025). *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag* (No. Prop. 2025/26:28).

Regeringskansliet. (2023). *Förordningen om gigabitinfrastruktur 2022/23:FPM64*. https://data.riksdagen.se/fil/0CE54F27-FCE5-40FD-8324-10CF7933ABFD

Region Norrbotten. (2025, September 9). *Region Norrbotten drabbad av cyberattacken mot Miljödata*. https://www.norrbotten.se/sv/region-norrbottens-nyhetsarkiv/region-norrbotten-drabbad-av-cyberattacken-mot-miljodata/

Reuters. (2024, November 18). Two telecoms cables in Baltic Sea severed, raising suspicions of sabotage. *The Guardian*. https://www.theguardian.com/world/2024/nov/18/telecoms-cable-in-baltic-sea-may-have-been-severed-says-finnish-owner

SOU. (2025). *Snabbare bredband i hela landet: Åtgärder för effektivare utbyggnad av gigabitinfrastruktur* (No. 2025:110). Regeringskansliet.

Statskontoret. (2025). *Tillsynsmyndigheternas kostnader till följd av NIS2-direktivet* (No. 2025:8).

Sveriges Kommuner och Regioner. (2023a). *Förslag till förordning om gigabit infrastruktur KOM(2023)94) SKR:s sammanfattande ställningstaganden*. https://www.regeringen.se/contentassets/c15d17f51ee24064881cc64443cbed2c/sveriges-kommuner-och-regioner.pdf

Sveriges Kommuner och Regioner. (2023b, December 21). *Gigabit Infrastructure Act, GIA* [Text]. https://skr.se/skr/naringslivarbetedigitalisering/digitalisering/euforordningareudirektivdigitalisering/forslag/gigabitinfrastructureactgia.70284.html

Sveriges Kommuner och Regioner. (2024). *Kommunernas informationssäkerhetsarbete* [Text]. https://extra.skr.se/skr/tjanster/rapporterochskrifter/publikationer/kommunernasinformationssakerhetsarbete.79736.html

Sveriges Riksdag. (2023). *Förordningen om gigabitinfrastruktur (Fakta-pm om EU-förslag 2022/23:FPM64: COM(2023) 94)*. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/fakta-pm-om-eu-forslag/forordningen-om-gigabitinfrastruktur_ha06fpm64/

SVT Nyheter. (2025, January 27). Detta vet vi: Kabelbrotten i Östersjön. *SVT Nyheter*. https://www.svt.se/nyheter/inrikes/detta-vet-vi-kabelbrotten-i-ostersjon

The European Parliament & the Council of the European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

The European Parliament & the Council of the European Union. (2024). *Regulation (EU) 2024/1309 of the European Parliament and of the Council of 29 April 2024 on measures to reduce the cost of deploying gigabit electronic communications networks, amending Regulation (EU) 2015/2120 and repealing Directive 2014/61/EU (Gigabit Infrastructure Act) (Text with EEA relevance)*.

Traficom. (2025, April 3). *Digital infrastructure, digital services and ICT services*. NCSC-FI. https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/digital-infrastructure-digital-services-and-ict-services

Appendix A

List of informants

Finnish respondent: Representant from the Finnish Transport and Communications Agency, Traficom

Estonian respondent: Representant from the Ministry of Justice and Digital Affairs

Lithuanian respondent: Representant from the Communications Regulatory Authority of the Republic of Lithuania

Swedish respondent: Representant from the Ministry of Finance, Division for Digital Infrastructure and Security

About this publication

Transparency vs Security: Enhancing connectivity under the Gigabit Infrastructure Act, NIS2 and 5G

Authors: Nicola Wendt-Lucas, Maja Brynteson
Quality assurance: Maria Bobrinskaya

Nordregio policy brief 2026:2
ISSN: 2001-3876
DOI: http://doi.org/10.6027/PB2026:2.2001-3876

Communication: Sara Melander, Nordregio
Layout: Marija Zelenkauskė. Nordregio

This policy brief is published as part of the "Nordic-Baltic Connectivity for Smarter and Inclusive Societies (N-B CONNECT) " research project, led by Nordregio. Running from 2024 to 2026, the project focuses on the socioeconomic effects of improving digital connectivity in a rural context. N-B CONNECT is funded by the Nordic Council of Ministers (MR Digital).

This report examines the potential benefits and challenges for rural communities in the Nordic and Baltic countries in relation to the Gigabit Infrastructure Act. It is one of several outputs from N-B CONNECT. For further details, please see: www.nordregioprojects.org/digihub/

The authors wish to thank the national experts who generously contributed their time and expertise to this study.

Nordregio

Nordregio is a leading Nordic and European research centre for regional development and planning, established by the Nordic Council of Ministers in 1997. We conduct solution-oriented and applied research, addressing current issues from both a research perspective and the viewpoint of policymakers and practitioners. Operating at the international, national, regional and local levels, Nordregio's research covers a wide geographic scope, emphasising the Nordic and Baltic Sea Regions, Europe and the Arctic.

Nordregio
Holmamiralens Väg 10
Skeppsholmen
Stockholm, Sweden
www.nordregio.org