

Engineering Preparedness

Engineering Preparedness for a Contested Nordic-Baltic Region

Author Hanne Shapiro / Hanne Shapiro Futures
For ANE – Association of Nordic Engineers

Contents

01. Executive Summary	4
02. Foreword	6
03. Engineering Preparedness in a New Security Order	8
3.1 The Nordic-Baltic Region in a Contested Europe	8
3.2 Critical Infrastructure as Strategic Target	9
3.3 Hybrid Threats and the Erosion of Civilian-military Boundaries	10
3.4 Rethinking Engineering Capability: Beyond Dual Use	11
3.5 From Regulation to Preparedness Capability: The EU Framework	11
3.6 NATO Enlargement, and the Competence Imperative	13
3.7 Engineers at the front of preparedness	13
3.8 The Capability Challenge	14
04. Engineering the Foundations of Nordic Preparedness	15
4.1 The Omni-Use Logic of Nordic Engineering Strength	16
4.2 Energy Systems Engineering: Depth, Transition, and Preparedness Relevance	16
4.3 Secure Communications and Network Engineering	17
4.4 Digital Public Infrastructure and Civic Systems Engineering	18
4.5 The Innovation Ecosystem as Preparedness Infrastructure	20
4.6 The Nordic Model and the Preparedness Governance Gap	21
4.7 Beyond Capability: The Integration Challenge!	21
05. From Strategic Alignment to Operational Preparedness	23
5.1 The Cooperative Architecture: What Exists	23
5.2 The Gap Between Frameworks and Operational Capacity	24
5.3 Preparedness as a Shared Engineering Capability	25
5.4 From Cooperation to Operational Capacity: Three Preconditions	26
06. Preparedness engineering domains	27
6.1 Systems Continuity Engineering	27
6.2 Operational Technology and Industrial Control Systems Security	28
6.3 Telecommunications, Subsea Infrastructure, and Satellite Engineering	29

Contents

6.4	Civil and Structural Resilience Engineering	30
6.5	Logistics and Supply-Chain Continuity Engineering	30
6.6	Threat-Adaptive Engineering	30
6.7	AI-Enabled Infrastructure Monitoring	30
6.8	Autonomous Systems and Counter-Drone Technologies	31
07.	Frontier Preparedness Engineering and Emerging Competency Needs	32
7.1	Quantum-Secure Communications	32
7.2	Advanced Materials and Rapid Infrastructure Repair	33
7.3	Space-Enabled Situational Awareness and Positioning Resilience	34
7.4	System-of-Systems Modelling and Resilience Analytics	34
7.5	The Hybrid Competence Challenge: What Cuts Across All Domains	36
08.	Engineering Workforce Constraints and Preparedness Capacity	38
8.1	The Structural Workforce Constraint	39
8.2	The Demographic Constraint: Retirement, Succession, and Tacit Knowledge Loss	39
8.3	The Distributional Constraint: Concentration, Fragility, and the Illusion of Aggregate Adequacy	40
8.4	The Preparedness Conversion Challenge	42
8.5	Gender, Diversity, and the Effective Talent Pool	42
8.6	Implications for Preparedness Planning	44
09.	Engineering Capacity and the Future of Preparedness	44
9.1	Reframing Preparedness	45
9.2	Looking Ahead: Preparedness as a Competitiveness and Innovation Strategy	46
10.	Glossary of Key Terms and Abbreviations	47
10.1	Key Concepts	47
10.2	Organisations, Frameworks and Initiatives	48
10.3	Technical Terms	49
10.4	Preparedness Engineering Profiles	49
11.	Bibliography	50

01. Executive Summary

Preparedness has traditionally been understood as a question of infrastructure protection, emergency planning, stockpiles, and defence capability.

These remain necessary, but they are no longer sufficient. In an interconnected, technologically dependent, and contested world, preparedness must increasingly be understood as the capacity to anticipate and prevent disruption to complex societal systems, to sustain their operation under stress, and to restore them when disruption occurs. That capacity depends not only on physical infrastructure, but on the engineering capabilities, innovation ecosystems, industrial capacities, and specialised talent pipelines that enable critical systems to function.

The Nordic-Baltic region is entering a new security environment shaped by geopolitical instability, hybrid threats, cyber disruption, technological rivalry, climate-related risks, and sustained pressure on critical infrastructure. Russia's war against Ukraine, growing concern over critical infrastructure sabotage, intensifying competition over strategic technologies, and increasing dependence on globally interconnected digital systems have exposed new vulnerabilities. At the same time, preparedness is becoming inseparable from broader questions of technological capability, workforce capacity, and societal resilience.

Drawing on developments across the Nordic-Baltic region, European regulatory frameworks including the Critical Entities Resilience Directive (CER) and NIS2, NATO resilience requirements, and evidence from engineering-intensive sectors, this report argues that preparedness is an engineering, workforce, and governance challenge rather than solely a security challenge. The critical question is no longer simply whether societies possess infrastructure, technologies, or emergency plans. It is whether they possess the capabilities required to operate, secure, maintain, adapt, and restore critical systems under conditions of disruption.

The Nordic and Baltic countries possess internationally competitive strengths in advanced energy systems, secure communications, digital infrastructure, industrial automation, cybersecurity, maritime technologies, artificial intelligence, and defence-related industries. However, the report finds that the principal constraint facing the region is not a lack of technological sophistication or innovation capacity. Rather, it is the ability to coordinate, mobilise, and sustain preparedness-relevant capabilities across institutions, sectors, firms, and national systems.

To describe this emerging strategic reality, the report introduces the concept of *omni-use technologies*. Unlike traditional dual-use technologies, which transition between civilian and military applications, omni-use technologies generate

value across multiple societal domains simultaneously. Technologies such as artificial intelligence, advanced telecommunications, cloud and edge computing, autonomous systems, advanced sensing, quantum technologies, and space-based infrastructure simultaneously underpin economic competitiveness, public services, societal resilience, crisis management, and defence capability.

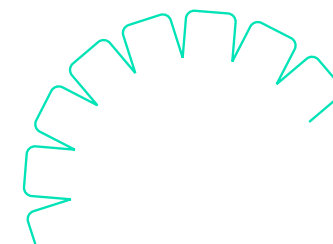
Their strategic significance lies not only in the technologies themselves but in the ecosystems that enable their development, deployment, adaptation, and their resilience. These ecosystems encompass research institutions, industrial supply chains, infrastructure operators, regulatory frameworks, and highly specialised engineering and STEM talent.

This perspective leads to a broader conclusion. Preparedness and economic competitiveness are no longer separate agendas competing for the same resources. The engineers, cybersecurity specialists, data scientists, AI experts, systems architects, telecommunications professionals, and energy specialists who sustain innovation and economic growth are the same professionals required to anticipate, prevent, manage, and recover from disruptions to critical systems. The education, research, and lifelong learning systems that develop and sustain this expertise therefore constitute preparedness infrastructure in their own right.

The report further argues that preparedness must increasingly be viewed through the lens of capability retention and technological sovereignty. For small and highly interconnected economies, technological sovereignty is not a question of self-sufficiency but of retaining sufficient engineering depth, institutional knowledge, operational expertise, and strategic control to preserve freedom of action despite dependence on global technologies, supply chains, and service providers. This challenge is compounded by growing reliance on outsourcing and specialised external providers for critical technical functions. While often economically rational, these arrangements can erode institutional memory and weaken organisations' capacity to mobilise expertise during prolonged disruption. The report identifies a growing preparedness conversion challenge across the region. Although significant engineering and technological strengths exist, the mechanisms required to translate emerging preparedness requirements into workforce development, education and training provision, skills intelligence, and operational capability remain fragmented. Lifelong learning systems, preparedness-relevant training pathways, and cross-border mechanisms for anticipating and addressing capability shortages remain underdeveloped relative to the scale and urgency of emerging demand.

Recent Nordic policy developments reinforce this assessment. In June 2026, the Nordic Ministers for Co-operation acknowledged the fragmented nature of preparedness efforts across the region and launched work on a new Nordic programme for societal security and emergency preparedness aimed at strengthening coordination and integration across sectors and borders. This recognition reflects one of the report's central findings: the preparedness challenge facing the Nordic-Baltic region is increasingly one of operational integration rather than strategic awareness.

The report concludes that preparedness should be understood not primarily as a cost imposed on economic development, but as a strategic investment in competitiveness, resilience, and long-term societal capacity. The Nordic-Baltic region already possesses many of the foundational assets required, including world-class research institutions, advanced industrial capabilities, mature digital infrastructure, and strong traditions of cross-border cooperation. The challenge now is to develop governance arrangements capable of connecting these assets more effectively, sustaining the engineering and STEM ecosystems on which they depend, and transforming fragmented strengths into a coherent preparedness capability for a contested world.



02. Foreword

In 2025, the Association of Nordic Engineers published *Reclaiming Europe's Edge: Competitiveness through STEM Talent* (ANÉ, 2025). That report argued that shortages of STEM talent are not simply an education challenge but a strategic challenge affecting competitiveness, innovation, technological sovereignty, and long-term economic resilience.

The question addressed in this report is a natural extension of that argument: If engineers are critical to competitiveness, what role do they play in preparedness?

Across Europe, preparedness has moved from the margins to the centre of public policy. Russia's full-scale invasion of Ukraine, growing hybrid pressure against critical infrastructure, the increasing vulnerability of digital systems, and intensifying geopolitical competition have fundamentally altered assumptions about security and resilience. The question of who keeps the lights on, the networks running, the water flowing, and the supply chains functioning under conditions of disruption has become a strategic concern.

At the same time, preparedness can no longer be understood solely through a military lens. Modern societies depend on highly interconnected infrastructure systems: energy grids, telecommunications networks, financial services, transport systems, cloud infrastructure, digital public services, and the engineering capabilities that sustain these. When these systems fail, the consequences quickly extend beyond individual sectors, organisations, and national borders.

This report adopts a Nordic-Baltic perspective because preparedness operates at the scale of interconnected regional systems rather than individual national infrastructures. The strategic environment reinforces this reality. Since 2022, the Baltic Sea has emerged as a critical operational space where infrastructure protection, communications resilience, energy security, and freedom of movement are increasingly interconnected. Finland and Sweden's accession to NATO has further integrated Nordic and Baltic preparedness challenges within a common security framework. Yet the rationale for a Nordic-Baltic perspective extends beyond defence cooperation. It reflects the growing reality that resilience, continuity, and recovery depend on infrastructure systems, engineering capabilities, and professional networks that operate across borders.

Preparedness in this report refers to the capacity of societies to anticipate disruption and to sustain, adapt, coordinate, and restore essential functions during periods of crisis or prolonged pressure. It is therefore as much about prevention as response: whether engineering skills, systems, and cooperation are robust enough to keep disruption from escalating into systemic failure. While military capability forms part of preparedness, the primary focus of this report is civilian preparedness: the infrastructure systems, institutions, professional capabilities, and engineering competencies required to maintain societal continuity under adverse conditions.

The anticipatory dimension of preparedness carries a governance consequence. Acting on foresight rather than on events requires the capacity to identify emerging risks, interpret early signals, and invest in capabilities before the need for them has been demonstrated. Because the relevant infrastructures, technologies, and skills cut across energy, digital, transport, education, research, and defence portfolios, no single ministry can exercise this form of anticipatory governance alone (Tonurist and Hanson, 2020). Preparedness therefore depends on coordination across ministerial boundaries and between public and private actors, a theme to which the report returns in its concluding chapter.

The same cross-boundary logic also applies to the professionals who keep these infrastructures and systems running. Preparedness is therefore a systems engineering challenge of the first order. It demands engineers capable of sustaining, protecting, adapting, and restoring essential services across organisational and national boundaries, often under conditions for which neither peacetime operations nor traditional crisis management systems were designed.

The gap between what this reality demands of engineering capacity and what existing institutions are currently configured to deliver defines the core analytical focus of this report.

The report makes three principal contributions.

First, it advances the concept of *omni-use engineering*, recognising that the same engineering ecosystems underpin economic activity, digital transformation, societal resilience, and security functions simultaneously. The traditional distinction between civilian and security domains remains important, but it no longer adequately captures how critical infrastructure systems operate in practice.

Second, it reframes the availability and depth of specialised engineering expertise as a preparedness variable. The critical constraint facing the Nordic-Baltic region is often not technology or infrastructure itself, but the availability of specialised engineering expertise capable of sustaining, coordinating, restoring, and renewing the systems on which resilience depends.

Third, it argues that preparedness is fundamentally an operational integration challenge. The central question is whether expertise distributed across firms, infrastructure operators, universities, public institutions, and national systems can be mobilised effectively when disruption occurs.



Acting on foresight rather than on events requires the capacity to identify emerging risks, interpret early signals, and invest in capabilities before the need for them has been demonstrated.

Built to Withstand:

03. Engineering Preparedness in a New Security Order

This chapter develops the analytical foundation of the report by examining how resilience and preparedness connect across the Nordic-Baltic region's critical infrastructure, and why engineers and engineering competence sit at the centre of that relationship.

It draws on the evolving security environment, the dual-use and, as the argument progressively establishes, omni-use technology architecture, the EU regulatory framework, and the competence requirements that follow from the region's changed strategic position.

3.1 The Nordic-Baltic Region in a Contested Europe

For three decades following the Cold War, the Nordic-Baltic region experienced an extended period of strategic stability. NATO and EU enlargement, economic integration, and strong domestic institutions fostered confidence, sometimes implicit and sometimes explicit, that large-scale territorial conflict was unlikely to return to Northern Europe. Even major warning events, including Russia's 2008 war in Georgia and the 2014 annexation of Crimea, were often interpreted as serious but containable disruptions to a broader European settlement.

That confidence has been comprehensively shattered. Russia's full-scale invasion of Ukraine in February 2022 confirmed that conventional warfare had returned to Europe, that borders could again be contested by force, and that European security rested on assumptions no longer valid (Ringsmose and Rynning, 2023). For the Nordic and Baltic states, several of which share borders with Russia or Belarus and all of which depend on maritime and digital connectivity vulnerable to interference, the implications were immediate.

What distinguishes the Nordic-Baltic security environment since 2023 is not only the persistence of risk but the emergence of a sustained sub-threshold pressure pattern against infrastructure and societal functions. NATO has explicitly framed recent incidents as sabotage affecting energy and communication cables and launched Baltic Sentry to strengthen surveillance and deterrence in the Baltic Sea region. The Baltic Sea has moved from being primarily a corridor of commerce and connectivity to a theatre where strategic signalling and disruption can be executed with plausible deniability.

The region's structural vulnerability is shaped by three characteristics. Geographic exposure, encompassing Finland's long border with Russia, Norway's Arctic proximity, and the Baltic states' frontier positions, creates a permanent requirement

for vigilance and resilience planning. Infrastructure interdependence links the region's economies into tightly coupled systems: power interconnectors, undersea data cables, and maritime supply routes mean that disruption in one segment can generate cascading effects across borders. Adversaries may also exploit such incidents for intelligence gathering, identifying vulnerable assets before targeting connections that could isolate the region in a hybrid or blockade scenario. The Nordic model has historically prioritised resilience over asset protection, viewing infrastructure not as critical individual units but as integral parts of vital societal functions. This approach has been supported by comparatively high levels of institutional and social trust, which have traditionally facilitated coordination between public authorities, infrastructure operators, and citizens during periods of disruption, yet the initial response to the Baltic cable incidents of 2023 and 2024 was improvised and uncoordinated, exposing the limits of existing preparedness.

The broader global order reinforces this picture. A sharpening US-China technology rivalry, transatlantic uncertainties over burden-sharing, and the diffusion of advanced capabilities to non-state actors all converge to make the Nordic-Baltic strategic position simultaneously more exposed and more consequential to European security as a whole (Bigo and Guild, 2023), rendering it vulnerable to hybrid disruption as a critical node in Europe's deterrence and connectivity architecture.

3.2 Critical Infrastructure as Strategic Target

The systematic targeting of critical infrastructure represents a qualitative evolution in how coercion and pressure are exercised in Europe. During the Cold War, critical infrastructure was typically framed as a wartime target, destroyed in the opening stages of large-scale conflict to paralyse mobilisation and industrial capacity. Today the logic is inverted: infrastructure becomes attractive precisely because it can be disrupted continuously, below escalation thresholds, while still imposing real costs and undermining public confidence (U.S. Helsinki Commission, 2024).

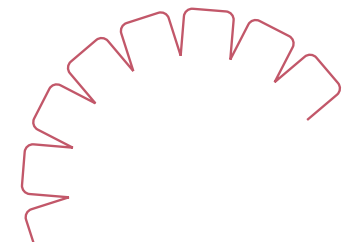
For the Nordic-Baltic region, critical infrastructure preparedness spans five interdependent domains: energy systems, telecommunications, transport and logistics, water and sanitation infrastructure, and digital infrastructure. The operational implication is that preparedness is cross-sectoral by design. Cascading failure risk is no longer theoretical; it is an inherent feature of tightly coupled infrastructure systems.

Box 3.1: Preparedness in a Cross-Sector Context

Cross-sector interdependence means that failure in one domain rapidly propagates into others. A telecommunications outage disables the digital control systems that manage power grids; a power grid failure cascades into water treatment and transport management; disruption of digital government platforms undermines the coordination capacity needed to manage any of the above.

Three features of this interdependence are particularly relevant to engineering workforce planning. First, the engineers who understand interdependency boundaries are highly specialised, and they are hard to recruit. Second, most preparedness planning has been organised within sectoral boundaries, creating governance gaps precisely at the cross-sector interfaces where cascading failure is most likely to originate. Third, the implementation of the EU Critical Entities Resilience Directive (CER Directive) now creates binding legal obligations for operators to assess and manage these interdependencies, generating demand for exactly the cross-domain engineering competence that existing educational pathways do not produce at scale.

Sources: European Commission (2022) CER Directive (EU 2022/2557); ENISA (2024) NIS Investments 2024.



3.3 Hybrid Threats and the Erosion of Civilian-military Boundaries

Hybrid operations exploit ambiguity: ambiguous attribution, ambiguous thresholds, ambiguous domains. They also exploit an institutional legacy in which civilian infrastructure and military security were governed as separate domains. That separation no longer reflects operational reality (Joenniemi and Lehti, 2023).

In the Nordic-Baltic region, hybrid pressure now includes cyber operations, electronic interference including GPS jamming, sabotage risks to undersea infrastructure, disinformation campaigns, and deliberate reconnaissance activity. The U.S. Helsinki Commission has mapped nearly 150 hybrid operations on NATO territory since February 2022, underscoring the breadth and persistence of this challenge (U.S. Helsinki Commission, 2024).

The erosion of civilian-military boundaries carries direct implications for the engineering profession. Engineers in energy, telecoms, transport, and software are no longer only delivering civilian services. They are defending vital national security functions under persistent pressure, a shift with implications both for required technical skills and for the professional and ethical context of engineering practice.

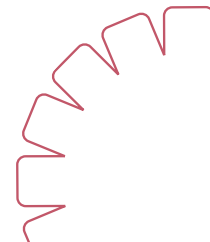
This transformation must be understood as a civilian, not a military, challenge. The engineers who keep power grids operating, communications networks running, and digital infrastructure secure are civilian professionals working within civilian institutions. Preparedness depends on sustaining this civilian engineering capacity: recruiting and retaining engineers in civilian roles, building civilian professional development systems, and creating civilian governance structures that can coordinate the workforce when needed. Engineering capacity has too often been treated as secondary to military capability in preparedness debates, despite being foundational to societal resilience.

Box 3.2: OT/ICS Security: The Hidden Frontline

Operational Technology (OT) and Industrial Control Systems (ICS) represent the engineered interface between the digital and physical worlds. Supervisory Control and Data Acquisition (SCADA) systems, programmable logic controllers, and distributed control systems operate power plants, water treatment facilities, railway signalling, and manufacturing lines. For decades, these systems were air-gapped from IT networks and thus insulated from conventional cyber threats. Convergence with IT and cloud environments has eliminated that insulation.

The security implications are profound and only partially addressed. OT/ICS environments differ from conventional IT in critical respects: availability is paramount over confidentiality; patching cycles are measured in years, not days; legacy equipment with twenty-to-thirty-year lifetimes cannot simply be replaced; and the consequences of a security failure may be physical damage, environmental harm, or loss of life rather than data breach.

Engineering these environments securely requires a hybrid competence profile combining deep domain knowledge of industrial processes with cybersecurity expertise, a profile that no existing educational programme produces systematically at scale. Nowhere is the preparedness skills shortage more acute than in OT/ICS security, where demand far outstrips the available workforce. Sources: ENISA (2024) NIS Investments 2024; European Commission (2022) NIS2 Directive (EU 2022/2555).



3.4 Rethinking Engineering Capability: Beyond Dual Use

Preparedness is often discussed in terms of defence procurement, crisis management, or civil protection. The language of dual-use captures part of this reality, but no longer fully describes the way critical infrastructure systems now operate.

The concept of dual-use originated in export control frameworks, where it referred to technologies or knowledge with both civilian and military applications. Applied to engineering competence, it carried a similar meaning: the same expertise used to build telecommunications networks, energy systems, or digital infrastructure could also support defence or security functions.

That distinction has become difficult to sustain. Modern infrastructure systems operate across commercial, regulatory, security, and preparedness functions simultaneously. An energy engineer may be managing grid stability, protecting systems against cyber intrusion, and supporting offshore, all while meeting the obligations of EU's critical entity resilience and cybersecurity frameworks — CER and NIS2. Telecommunications engineers maintaining commercial 5G networks are also working on infrastructure resilience, redundancy, and protection against electronic interference. AI systems developed for predictive maintenance may simultaneously support cybersecurity monitoring and infrastructure protection. The term omni-use captures this more accurately: the same engineering ecosystems, infrastructures, and technical competencies increasingly support multiple societal functions simultaneously, without any single domain being primary (Singer, Mueller and Kraus, 2025; Kremidas, 2025).

The policy implications are significant. Preparedness can no longer be treated as a separate security layer added onto civilian infrastructure systems after the fact. The engineering ecosystems underpinning the green and digital transitions are increasingly part of the region's operational resilience architecture itself. How Nordic engineering capability is developed, funded, and coordinated must reflect that reality.

Box 3.3: Lessons from Ukraine: Infrastructure Resilience Under Sustained Attack

Ukraine's experience since 2022 offers rare real-world evidence of what infrastructure resilience means under sustained attack. Distributed generation, mobile substations, flexible network configurations, and modular repair approaches helped sustain electricity and digital services even when major infrastructure assets were repeatedly damaged. Equally important was repair surge capacity: pre-positioned materials, trained technical teams, and cross-border equipment support enabled restoration under conditions far beyond those anticipated in peacetime planning.

For the Nordic-Baltic region, the central lesson is that preparedness depends not only on protecting infrastructure, but on maintaining the engineering workforce capacity, operational autonomy, and restoration capability required to recover systems repeatedly during prolonged disruption. That makes societal preparedness a human capital issue as much as a technical one.

Sources: Ringsmose and Rynning (2023); NATO (2023) Civil Preparedness; ENTSO-E (2024).

3.5 From Regulation to Preparedness Capability: The EU Framework

A dimension insufficiently recognised in Nordic preparedness discourse is the extent to which the EU has, since 2022, begun constructing a regulatory, industrial, and technological architecture that directly shapes how societal resilience and preparedness capability are organised. Two regulatory instruments are particularly significant.

The CER Directive (EU 2022/2557) establishes binding obligations across eleven critical sectors, requiring operators to conduct systematic risk assessments and implement technical and organisational measures that translate directly into engineering design and operational capability requirements (European Commission,

2022). NIS2 (EU 2022/2555) complements this by extending harmonised cybersecurity obligations across a much wider range of entities, mandating incident handling, business continuity, supply chain security, and the use of multi-factor authentication and encryption, capabilities that require engineering expertise to implement and maintain them at scale (European Commission, 2022).

Taken together, these frameworks function as capability frameworks for preparedness, generating demand for hybrid engineering profiles that span IT security, OT operations, cross-border coordination, and regulatory compliance simultaneously. The implementation challenge is therefore not primarily legal. It is fundamentally a workforce and engineering capability challenge.

Beyond regulation, the European Defence Industrial Strategy (EDIS), launched in March 2024, reflects a broader shift in European policy thinking away from viewing economic competitiveness, industrial capacity, technological sovereignty, and preparedness as separate policy domains, and towards recognising their growing interdependence (Bux, U. and Del Monte, 2024). For the Nordic-Baltic region, this creates both opportunity and pressure: the region possesses substantial engineering depth in many of the domains these frameworks prioritise, yet the pace at which demand for specialist engineering competence is growing now outstrips the capacity of existing education and workforce systems to respond.



Taken together, these frameworks function as capability frameworks for preparedness, generating demand for hybrid engineering profiles that span IT security, OT operations, cross-border coordination, and regulatory compliance simultaneously.

Box 3.4: CER, NIS2, and the Engineering Workforce: What Compliance requires

CER Articles 13 and 14 require critical entities to conduct regular risk assessments and implement technical and organisational resilience measures, increasing demand for engineering capabilities able to secure and restore critical infrastructure under conditions of disruption.

NIS2 Article 21 mandates cybersecurity risk-management measures including incident handling, business continuity, supply-chain security, multi-factor authentication, and encryption, while Article 23 establishes strict incident-reporting obligations and timelines. Together, these requirements increase demand for engineers capable of managing cyber incidents within operational technology and industrial control environments without disrupting live physical processes, a specialised competency area that remains in limited supply across Europe.

Both directives also strengthen requirements for cross-border cooperation and information sharing, creating demand for engineers able to operate within interoperable Nordic-Baltic and EU security frameworks.

Sources: European Parliament and Council of the European Union (2022) Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive), Articles 13–14. Official Journal of the European Union, L333, pp. 164–198.

European Parliament and Council of the European Union (2022) Directive (EU) 2022/2555 concerning measures for a high common level of cybersecurity across the Union (NIS2 Directive), Articles 21 and 23. Official Journal of the European Union, L333, pp. 80–152.

European Commission (2022) CER Directive Articles 13–14; European Commission (2022) NIS2 Directive Article 21, Article 23.

3.6 NATO Enlargement, and the Competence Imperative

Finland's accession to NATO in April 2023 and Sweden's in March 2024 constitute the most significant transformation of Nordic security architecture since the Cold War (NORDEFCO, 2023). Together, they close the strategic gap between NATO's northern flank and the Baltic states, create conditions for more integrated Nordic-Baltic planning, and generate new interoperability requirements that extend deep into civilian infrastructure and engineering domains.

The formal foundation of NATO's civil preparedness agenda is Article 3 of the Washington Treaty. Since 2016, NATO has operationalised this through its Baseline Requirements for National Resilience, covering continuity of government, energy, communications, transport, emergency response, food and water systems, and the management of mass casualties (NATO, 2016; Christie and Berzina, 2022; Dowd and Cook, 2022). In practice, these requirements are engineering and workforce challenges as much as policy commitments. Resilient energy supply depends on grid stability and black-start capability; communications resilience depends on hardened telecommunications infrastructure and network redundancy; and continuity across transport, water, and digital systems depends on engineers capable of sustaining and restoring interconnected infrastructure under degraded conditions.

NATO's DIANA programme, the Defence Innovation Accelerator for the North Atlantic, is also relevant to the omni-use capability agenda, particularly through its focus on AI, autonomous systems, quantum technologies, biotechnology, and space (NATO DIANA, 2024). The significance of these developments lies less in defence procurement itself than in the growing overlap between civilian technological capability, infrastructure resilience, and preparedness requirements across the Nordic-Baltic region. Recent NATO resilience scholarship emphasises that preparedness depends not only on military capability, but on resilient civilian systems, societal mobilisation capacity, and the ability of civilian institutions and infrastructure operators to function under conditions of prolonged hybrid pressure (Hoogensen Gjörv, Glebov and Holshek, 2025). This situates engineers at the forefront of preparedness.

3.7 Engineers at the front of preparedness

What distinguishes preparedness in the Nordic and Baltic context is that societal resilience now depends as much on civilian engineering capability as on conventional defence capacity. Modern crises rarely unfold through conventional military confrontation alone. Preparedness challenges arise when the interconnected systems that support everyday life are disrupted, including energy, telecommunications, transport, water, finance, and digital services. When these systems are disrupted, the ability to sustain societal functioning depends fundamentally on the availability of highly specialised engineering and technical expertise.

This interdependence makes preparedness a collective engineering challenge as much as a national one and shifts its centre of gravity from infrastructure design toward the human and institutional capability required to sustain systems under prolonged disruption. The strategic importance of this capability is growing while many Nordic and Baltic countries already face shortages across engineering, cybersecurity, digital infrastructure, and advanced technical occupations. These pressures are intensified by the evolving character of disruption itself. Cyber-attacks, supply-chain failures, infrastructure sabotage, disinformation, and extreme weather events interact across connected systems, producing cascading effects that are difficult to isolate or manage within traditional sector boundaries.

Preparedness, in other words, is not only about stronger infrastructure or more advanced technology. It is equally about maintaining the human, institutional, and industrial capacity to adapt, coordinate, repair, and recover while disruption is still unfolding.

Civil preparedness extends beyond critical infrastructure and the engineering professions themselves. It encompasses the capacity of society to continue functioning as close to normal as possible under conditions of crisis or war. Engineers play a central role in this effort, but they do so alongside firms, public institutions, and production systems whose continued operation underpins societal resilience.

Industrial adaptability forms an important part of this broader capability. Companies with significant civilian production capacity may be able to repurpose operations

to support emergency or wartime requirements, while innovation ecosystems can accelerate the development of new solutions. Ukraine's experience illustrates both dimensions. Small start-ups have driven important advances in areas such as drone technology, yet scaling these innovations has depended on established manufacturers, production capacity, supply chains, certification systems, and the mobilisation of civilian engineering talent (CSIS, 2026; Council on Foreign Relations, 2026). For the Nordic-Baltic region, this suggests that preparedness depends not only on specialised engineering expertise and critical infrastructure resilience, but also on the adaptability of the wider industrial ecosystem and its capacity to convert civilian capabilities into societal resilience when circumstances require.

Box 3.5 Preparedness Equals Resilience Plus Mobilisation

Resilience concerns whether systems can withstand disruption. It is primarily an infrastructure, organisational, and engineering challenge involving redundancy, modularity, adaptability, and fail-safe design.

Preparedness concerns whether societies can sustain, repair, adapt, and restore critical functions during prolonged disruption. It depends on engineering capability, operational decision-making capacity, industrial adaptability, institutional coordination, and the ability to mobilise resources rapidly across sectors and borders.

The key distinction is surge capacity: the ability to mobilise specialised expertise, production capability, and organisational resources quickly and at scale. A society may invest heavily in resilient infrastructure and still remain vulnerable if critical skills, industrial capacity, or institutional capabilities erode through workforce shortages, weak learning systems, fragmented coordination, or insufficient preparedness planning.

Sources: NATO (2016) *Baseline Requirements for National Resilience*; Tierney (2019).

3.8 The Capability Challenge

The analysis developed above leads to four interconnected conclusions.

1. First, the Nordic-Baltic region has moved from Europe's strategic periphery to a more central position within collective preparedness and defence planning. This shift is generating sustained and growing demand for engineering expertise across energy systems, telecommunications, transport infrastructure, logistics, cloud architecture, cybersecurity, and other critical civilian sectors.
2. Second, advanced engineering capability increasingly shapes resilience, deterrence, and societal continuity.
3. Third, the combined effect of the CER Directive, NIS2, NATO resilience requirements, and emerging European industrial security frameworks is transforming preparedness into a concrete workforce challenge.
4. Fourth, the traditional dual-use framework no longer adequately captures the structure of preparedness. The same infrastructures, engineering ecosystems, firms, technologies, and professional competencies increasingly support commercial activity, digital transformation, societal resilience, industrial strategy, and security functions simultaneously. This report therefore adopts the concept of omni-use to describe an environment in which economic, societal, and security functions increasingly depend on the same engineering capabilities and infrastructure systems.

Taken together, these developments point to a strategic constraint that extends beyond technology itself. The limiting factor increasingly lies in whether Nordic and Baltic societies can organise, sustain, renew, and mobilise the engineering expertise on which resilient infrastructure systems depend. Preparedness is therefore not only a question of defence investment or infrastructure protection. It is equally a question of workforce depth, institutional coordination, long-term competence renewal, and the capacity to maintain operational continuity across interconnected systems during prolonged disruption.

The chapters that follow build from this foundation. Chapter 4 examines the Nordic innovation ecosystem as the institutional and technological base on which both competitiveness and preparedness capability increasingly depend. Chapter 5 analyses how Nordic-Baltic cooperation must evolve from political coordination towards shared operational engineering capacity. The following sections examine how these engineering strengths intersect with growing workforce pressures, institutional fragmentation, and emerging preparedness requirements.



AI generated image

04. Engineering the Foundations of Nordic Preparedness

The analysis developed thus far has argued that preparedness in the Nordic-Baltic region increasingly depends on civilian engineering capability embedded across interconnected infrastructure systems. It also introduced the concept of omni-use to describe how the same engineering ecosystems now simultaneously support economic activity, societal resilience, preparedness, and security functions.

This chapter examines how these capabilities were developed, where the region's engineering depth is concentrated, and why these strengths now possess growing preparedness relevance. It analyses the institutional and industrial ecosystems underpinning Nordic and Baltic resilience across energy systems, telecommunications, digital infrastructure, industrial capability, and advanced technologies. At the same time, it argues that significant governance and workforce gaps continue to limit the region's ability to mobilise these capabilities fully under conditions of sustained disruption.

4.1 The Omni-Use Logic of Nordic Engineering Strength

The Nordic region exemplifies the omni-use logic to a greater degree than most regions of comparable economic scale. Its technological strengths emerged from the practical demands faced by small, open, highly digitalised economies operating in demanding geographic and climatic conditions. Managing offshore energy systems in Arctic environments, building advanced telecommunications networks across sparsely populated territories, and developing secure digital public services used daily by entire populations required deep engineering expertise long before preparedness became a central political concern.

These capabilities are strategically valuable because they were developed through the long-term operation of civilian infrastructure systems rather than primarily through defence procurement programmes. Engineers built expertise by operating energy grids, telecommunications networks, offshore systems, transport infrastructure, and digital public services continuously under demanding real-world conditions. This produced operational knowledge that is difficult to reproduce through preparedness exercises or short-term security initiatives alone. The preparedness value of the Nordic region therefore lies not only in technologies or infrastructure assets themselves, but in the accumulated engineering competence embedded across firms, public institutions, infrastructure operators, universities, and professional ecosystems.

The engineering strengths now central to preparedness were not originally developed for security purposes. They emerged because advanced telecommunications markets, offshore energy development, industrial automation,

and ambitious digital public administration required them. Their preparedness relevance reflects a broader systemic shift in which the civilian systems supporting everyday societal functioning increasingly overlap with the systems exposed to disruption, coercion, and hybrid pressure. As established in Chapter 2, this is the omni-use logic in practice: the Nordic region's strengths in energy systems.

Box 4.1 Norway's Offshore Wind Transition

Norway's offshore wind sector demonstrates how engineering capability developed for the green transition increasingly also supports preparedness and infrastructure resilience. Floating offshore wind projects such as Hywind Tampen have required advanced expertise in subsea engineering, offshore structures, digital monitoring systems, power electronics, marine logistics, remote operations, and grid integration under harsh North Sea conditions.

Many of these competencies were originally developed in offshore oil and gas and are now being transferred into offshore wind through targeted reskilling and workforce transition initiatives involving industry, universities, and vocational education providers. The result is an engineering ecosystem that simultaneously supports decarbonisation, digital infrastructure management, offshore resilience, and critical energy security.

Sources: Equinor (2024) Hywind Tampen; Norwegian Offshore Wind (2024) Offshore Wind Education in Norway; WindEurope (2025) Europe's Wind Energy Workforce Report; International Energy Agency (2024) Offshore Wind Outlook 2024.

4.2 Energy Systems Engineering: Depth, Transition, and Preparedness Relevance

Energy systems engineering constitutes the Nordic region's strongest and most strategically significant omni-use capability domain. The operation of geographically dispersed, weather-dependent renewable energy systems across tightly interconnected regional electricity markets has required sustained investment in

power electronics, digital grid management, offshore systems engineering, black-start capability, and advanced infrastructure coordination. These are precisely the types of competencies increasingly recognised by NATO, ENTSO-E, and European resilience frameworks as critical to maintaining energy continuity under conditions of disruption and crisis (NATO, 2023; ENTSO-E, 2024; Fingrid, 2023).

What gives the Nordic region particular depth in this domain is the combination of technological sophistication and sustained operational practice. Engineers working within Nordic transmission system operators, offshore energy firms, utilities, and infrastructure operators daily manage highly complex systems under conditions shaped by geographic dispersion, harsh climatic environments, fluctuating renewable generation, and cross-border interdependence. This produces forms of operational and systems expertise that are accumulated through practice and coordination over time, and which cannot easily be recreated through formal training alone.

The energy transition has further expanded and strengthened this engineering base. The rapid development of offshore wind, particularly in Denmark and Norway, has driven advances in subsea cabling, offshore structural engineering, power conversion systems, digital monitoring technologies, and complex system integration. Many of these competencies are directly relevant to the growing preparedness challenge surrounding offshore infrastructure protection and restoration. WindEurope (2025) and the International Energy Agency (2024) both identify mounting shortages of specialised engineers and technicians across offshore wind, grid integration, and energy systems management as emerging risks to Europe's energy transition and infrastructure resilience objectives.

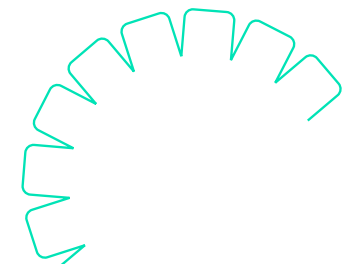
The implementation of the CER Directive increasingly translates these technological capabilities into concrete preparedness obligations. Critical infrastructure operators must now demonstrate capacity in resilience planning, infrastructure restoration, operational continuity, and systematic risk management under adverse conditions. This creates growing demand for engineers capable not only of designing advanced energy systems, but also of sustaining and restoring them during prolonged disruption. The Nordic ecosystem enters this period from a position of significant strength. However, maintaining that advantage will depend on workforce renewal, specialist training capacity, and the long-term sustainability of specialised engineering pipelines.

4.3 Secure Communications and Network Engineering

Nordic telecommunications engineering represents one of the region's most strategically significant omni-use assets. The commercial imperatives of building high-performance networks across sparsely populated geographies, harsh climatic environments, and complex maritime terrain have produced engineering depth in radio frequency design, network architecture, subsea cabling, and large-scale systems integration that few regions of comparable economic scale can match. Finland's Nokia and Sweden's Ericsson built the competence ecosystems that remain the core of Europe's remaining industrial capacity in mobile network infrastructure engineering. These capabilities have immediate relevance to communications systems that can continue operating under conditions of disruption and attack. (European Commission, 2024; ENISA, 2024).

Nordic network engineers have not only designed advanced systems but operated and maintained them continuously under real-world conditions. That operational continuity matters for preparedness: the knowledge of how networks fail, how they behave in degraded states, and how restoration is managed at scale is accumulated through practice rather than acquired through training alone (NATO, 2023).

The near-term risk to this competency base is workforce erosion through commercial restructuring at Nokia and Ericsson, the two firms around which much of Europe's mobile network engineering ecosystem is organised. What matters analytically is that competence in radio frequency design, network architecture, and complex network software management depends on long-cycle industrial ecosystems, specialised workforce pipelines, and accumulated systems integration knowledge that, once dispersed, cannot be reconstituted quickly (ENISA, 2024; European Commission, 2024; Adamson and Ålander, 2026).



Box 4.2: Finland: Engineering Capability in a Whole-of-Society Model

Finland's preparedness engineering base benefits from an institutional advantage beyond technical capability. Its comprehensive security model has maintained coordination between civilian infrastructure, industry, and national resilience planning since the Cold War, while several other Nordic countries reduced equivalent preparedness structures after the early 1990s.

This continuity has supported a comparatively integrated ecosystem linking VTT's applied research infrastructure, Aalto and Tampere University's strengths in telecommunications, cybersecurity, and systems engineering, and Patria's defence-industrial capability. Finland's National Emergency Supply Organisation further connects public authorities and critical infrastructure operators through a network involving approximately 1,500 companies and sectoral coordination pools.

The continuing challenge is ensuring that this institutional coordination capacity can be translated into sufficient engineering depth in areas such as operational technology security, resilient communications infrastructure, and critical systems engineering as CER and NIS2 requirements.

Sources:

Finnish National Emergency Supply Agency (NESA) (2025) The National Emergency Supply Agency.

European Commission (2022) Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive). Official Journal of the European Union.

Hyvönen, A.-E. and Juntunen, T. (2020) 'From "spiritual defence" to robust resilience in the Finnish comprehensive security model', in Larsson, S. and Rhinard, M. (eds.) Nordic Societal Security: Convergence and Divergence. London: Routledge.

4.4 Digital Public Infrastructure and Civic Systems Engineering

The Nordic region's investment in digital public infrastructure constitutes a third category of omni-use preparedness asset, one built through the practical demands of governing small, highly digitalised societies rather than through security-oriented design. Denmark's digital public sector, among the world's most advanced in scale and integration, has generated genuine institutional expertise in large-scale systems architecture, interoperability engineering, and secure identity infrastructure (European Commission, 2024). These competencies underpin government continuity under disruption — not as aspirational capabilities but as operational realities tested daily at population scale.

Estonia's trajectory is equally instructive. The country deliberately constructed a resilient, distributed digital state architecture encompassing X-Road interoperability infrastructure, digital identity systems, and data embassy arrangements, embedding a preparedness engineering logic from the outset. These are systems designed to function under adversarial conditions, including the loss of physical territory.

The engineering competence that built and maintains this architecture is a regional asset of growing strategic importance as other Nordic and Baltic governments face equivalent design challenges under CER and NIS2 obligations (European Commission, 2022).

Preparedness in digital infrastructure, however, also depends on the physical foundations that sustain connectivity, storage, and computational continuity under disruption. In this respect, Iceland occupies a distinctive position within the regional preparedness architecture.



These are systems designed to function under adversarial conditions, including the loss of physical territory.



Box 4.3: Iceland: Energy-Backed Digital Resilience

Iceland's contribution to Nordic digital infrastructure is distinctive and often underappreciated. Abundant geothermal and hydropower resources support some of the world's most energy-secure data centre and telecommunications infrastructure. In a threat environment where transatlantic data routing and cloud infrastructure are increasingly targets of hybrid pressure, Iceland's energy-backed digital resilience, combined with its North Atlantic geographic position, provides strategic depth that few other locations can match.

Iceland ranked first in a cross-country analysis of 38 OECD member states for supporting women in STEM roles, with approximately 45 per cent of STEM positions held by women (see also Box 8.4). This advantage in talent utilisation compounds the geographic and energy security advantages that make Iceland a strategically distinctive node in the regional preparedness architecture.

Sources: Organisation for Economic Co-operation and Development (OECD (2024); NordForsk (2025); European Commission (2024).

Norway and Sweden have developed complementary strengths in industrial systems integration, the engineering of large-scale process control environments across offshore energy, manufacturing, and utilities, which translate directly into the operational continuity requirements that preparedness frameworks now mandate (Norwegian Ministry of Defence, 2024; ENISA, 2024). These capabilities were developed commercially, through decades of managing complex physical infrastructure in demanding environments, and their preparedness relevance is a consequence of that civilian investment rather than a deliberate security outcome (ANE, 2025).

Across these national profiles, the common thread is the operational engineering depth of expertise: engineers who have built, operated, and restored complex systems at scale over long periods under real-world conditions. Rather than any specific technology, it is this deep expertise that constitute the genuine preparedness asset.

Chapters 5, 6 and 7 examine in greater detail how the Nordic-Baltic region's existing engineering depth intersects with the changing competency demands generated by preparedness, infrastructure interdependence, technological transformation, and prolonged societal disruption. Their focus is not only where specialised competencies already exist, but where workforce gaps, institutional fragmentation, and emerging operational requirements are creating growing pressures across preparedness-relevant engineering domains.

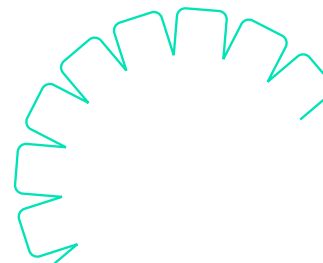
4.5 The Innovation Ecosystem as Preparedness Infrastructure

Taken together, the Nordic innovation system constitutes a preparedness asset of substantial depth. Its civilian engineering base in energy systems, secure communications, subsea operations, and digital infrastructure represents precisely the kind of omni-use capability on which preparedness increasingly depends (ANE, 2025). At the same time, four structural challenges emerge clearly from the analysis and shape the competency gaps examined in the following chapters.

1. First, the relationship between innovation and institutional anchoring. Nordic firms and research institutions are producing advanced capabilities across the engineering domains examined in this chapter, but whether the knowledge they generate remains embedded within Nordic institutional ecosystems over time, or gradually migrates through acquisition, restructuring, and global talent competition, has direct preparedness implications (Slåtmo et al., 2024; Nordic Innovation, 2026). The concern is not primarily frontier technologies. Rather, it concerns the established engineering competencies in energy systems, subsea infrastructure, and secure communications that already form the operational backbone of regional resilience. If the firms and institutions anchoring this knowledge are hollowed out or absorbed into external ecosystems, preparedness capacity may erode rapidly and prove difficult to rebuild.
2. A related preparedness challenge concerns technological sovereignty. For the Nordic-Baltic region, technological sovereignty should not be understood as self-sufficiency, but as the ability to maintain strategic control over critical technologies and infrastructures despite external dependencies. This includes retaining sufficient domestic and regional capability to understand, operate, secure, maintain, and restore systems that increasingly rely on globally concentrated suppliers of cloud services, semiconductors, artificial intelligence, telecommunications equipment, and cybersecurity solutions. Preparedness therefore depends not only on technological access, but also on preserving the engineering and institutional capabilities required to exercise independent judgement

and operational continuity under conditions of disruption or geopolitical pressure (Brookings Institution, 2025; European Commission, 2026; Baldoni and Di Luna, 2025).

3. Third, the growing disconnect between regulatory demand and engineering supply. CER and NIS2 create legal obligations that map directly onto engineering competency requirements, yet the institutional pathways connecting regulatory demand to education, training provision, and workforce planning remain weakly developed (European Commission, 2022). Operators increasingly face binding obligations to demonstrate resilience and restoration capacity, while the engineering programmes expected to supply these competencies have not been systematically redesigned to meet emerging demand (ENISA, 2024).
4. Fourth, the distinction between STEM talent in general and the specific engineering competencies that preparedness requires, a distinction critical to avoiding the policy mistake of treating aggregate graduate numbers as a proxy for preparedness capability (Finnish Ministry of Finance / TEK, 2024). The Nordic region produces substantial numbers of engineering graduates overall, but the specialist competencies most critical to infrastructure resilience, including power systems restoration, subsea operations, and hardened communications engineering, remain concentrated within a relatively small number of institutions, programmes, and firms.



4.6 The Nordic Model and the Preparedness Governance Gap

The engineering strengths described above are real. But possessing technical depth is not the same as being able to deploy it. Most of the infrastructure that needs to keep running, including power, communications, water, and transport, is owned and operated by private companies (Heinrich Böll Stiftung, 2023). What they do not routinely do is test how systems hold up under sustained pressure, plan restoration at speed, or coordinate response with counterparts in neighbouring countries. The interface between public authority and private operator is, in most Nordic countries, still mediated more by informal relationships than by structured coordination frameworks. That is a social asset, but not an adequate substitute for systematic governance (NORDEFCO, 2023).

At the regional level, no overarching framework exists for identifying shared engineering dependencies, coordinating investment, or benchmarking performance collectively. Each country continues to plan its engineering workforce primarily according to national priorities and institutional structures (NordForsk, 2025). Since Russia's full-scale invasion of Ukraine in 2022, Nordic and Baltic governments have reached broad agreement on the nature and seriousness of the preparedness challenges confronting the region (Ringsmose and Rynning, 2023).

This diagnosis is increasingly reflected in Nordic policy developments. In June 2026, the Nordic Ministers for Co-operation agreed to strengthen and better coordinate Nordic work on societal security and emergency preparedness, explicitly recognising that existing efforts remain fragmented across initiatives, sectors, and governance structures. The ministers called for the development of a more coherent and strategic Nordic framework capable of strengthening cross-sector coordination, knowledge sharing, and collective preparedness capacity across the region (Nordic Council of Ministers, 2026). This recognition reinforces the argument advanced in this report that the central preparedness challenge is increasingly one of integration, mobilisation, and coordination rather than awareness or strategic intent.

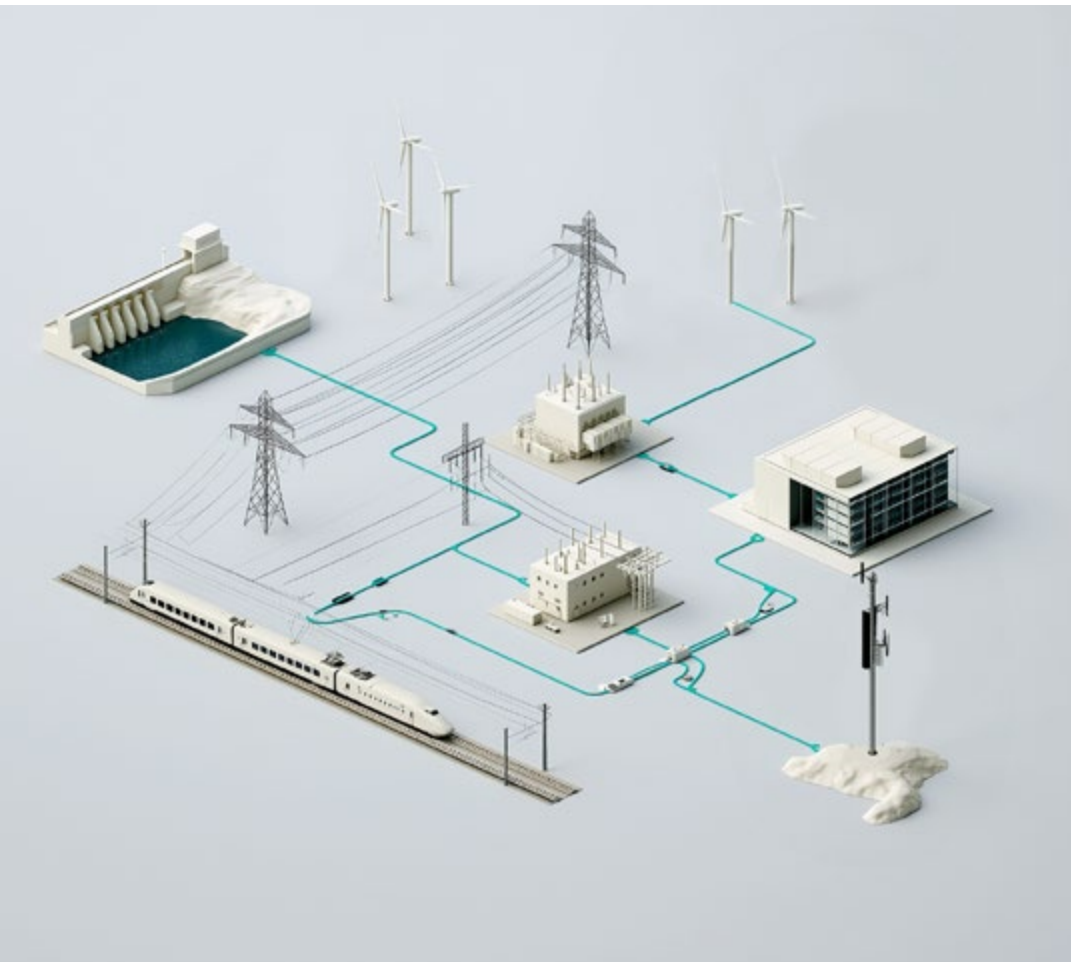
4.7 Beyond Capability: The Integration Challenge!

The analysis developed throughout this section points toward a broader conclusion. The Nordic-Baltic region possesses substantial engineering depth across many of the domains now central to preparedness, including energy systems, secure communications, digital public infrastructure, offshore operations, industrial automation, and advanced systems integration. These capabilities were developed primarily through civilian economic activity, yet they now form part of the operational infrastructure on which societal resilience increasingly depends.

The central challenge is therefore no longer simply whether these competencies exist. It is whether they can be coordinated, sustained, and mobilised rapidly under conditions of prolonged disruption and cross-border pressure. Preparedness depends not only on technological sophistication or innovation performance, but on the institutional capacity to translate fragmented engineering assets into operational capability at regional scale.

Several structural pressures emerge repeatedly across the analysis. Critical engineering knowledge and specialist competences are increasingly vulnerable to restructuring, acquisition, and global talent competition. At the same time, preparedness obligations under frameworks such as CER and NIS2 are expanding far faster than the workforce systems designed to supply the corresponding engineering capability.

Across the Nordic region, preparedness-relevant learning opportunities are distributed across universities, professional associations, technological institutes, infrastructure operators, defence-related programmes, vendor certifications, and private training providers. While many high-quality programmes exist, the overall landscape remains fragmented. Neither governments nor employers possess a comprehensive overview of preparedness-related learning provision across the Nordic-Baltic region, and engineers seeking to enter emerging preparedness



Ai generated image

domains often face unclear pathways. This lack of coherence is increasingly problematic because preparedness capability depends on hybrid competence profiles that combine engineering, cybersecurity, systems integration, operational resilience, data analytics, and regulatory understanding. Such profiles frequently cut across traditional disciplinary and institutional boundaries. Viewed through an omni-use lens, education systems, lifelong learning institutions, and skills intelligence infrastructures become part of preparedness infrastructure itself. The capacity to anticipate emerging capability requirements, translate demand signals into educational provision, and continuously renew specialised expertise increasingly constitutes a strategic resilience function. The same mismatch extends to governance. Highly interconnected infrastructure systems increasingly operate across national and sectoral boundaries, while workforce planning, professional recognition, and preparedness governance remain organised primarily through fragmented national structures.

Taken together, these pressures confirm the report's central argument: the Nordic-Baltic preparedness challenge is not primarily one of technological capability, but of operational integration. The region possesses substantial engineering strengths, yet preparedness ultimately depends on whether these capabilities can be organised, coordinated, and mobilised across institutional, sectoral, and national boundaries.

The next chapter examines the cooperative frameworks through which the Nordic and Baltic countries are seeking to achieve that integration.

05. From Strategic Alignment to Operational Preparedness

The Nordic-Baltic region possesses substantial strengths relevant to preparedness, including advanced infrastructure, strong engineering capabilities, digitally mature public sectors, and high levels of institutional trust. Yet these assets remain embedded within nationally organised systems designed primarily for peacetime coordination rather than sustained cross-border disruption.

This chapter examines the cooperative frameworks through which the Nordic and Baltic countries seek to overcome that fragmentation. It argues that although the region has achieved a historically high degree of political alignment and strategic convergence, the institutional arrangements needed to translate these strengths into shared operational engineering capacity remain underdeveloped.

5.1 The Cooperative Architecture: What Exists

What distinguishes the current phase of Nordic and Baltic cooperation from earlier periods is that preparedness is no longer organised primarily around territorial defence alone. Increasingly, it is structured around the continuity of civilian systems whose disruption would rapidly undermine both military and societal functioning simultaneously. This changes the meaning of regional cooperation itself. The challenge is no longer only interoperability between armed forces. It is interoperability between energy systems, telecommunications networks, logistics infrastructures, digital public services, industrial supply chains, and the engineering workforces capable of sustaining them under prolonged pressure.

This creates a qualitatively different coordination problem from earlier Nordic security cooperation. Traditional defence integration could be organised through ministries of defence, procurement structures, and military planning processes. Preparedness engineering, by contrast, cuts horizontally across ministries, regulators, infrastructure operators, universities, labour market institutions, and private firms. A grid restoration following a major blackout requires simultaneous coordination between transmission system operators, emergency services, OT security teams, equipment suppliers, and municipal authorities. The same applies to subsea cable repair, telecommunications continuity, cloud infrastructure resilience, and cross-border OT/ICS incident response. Many of these actors have historically operated with limited strategic coordination outside crisis management contexts (Boin and Lodge, 2016; European Commission, 2024a).

Recent policy developments suggest growing recognition of this challenge. In June 2026, the Nordic Ministers for Co-operation agreed to strengthen and better coordinate Nordic cooperation on societal security and emergency preparedness, explicitly acknowledging that existing efforts remain fragmented across initiatives, sectors, and governance arrangements. The ministers called for the development of

a more coherent and strategic Nordic framework capable of strengthening cross-sector coordination, knowledge sharing, and collective preparedness capacity across the region (Nordic Council of Ministers, 2026).

The significance of this development extends beyond preparedness policy itself. It reflects a broader shift in understanding. The central challenge facing the Nordic-Baltic region is increasingly not the absence of capability, technological sophistication, or strategic awareness. The region possesses world-class expertise in energy systems, telecommunications, cybersecurity, digital infrastructure, advanced manufacturing, and critical infrastructure operations. The challenge is whether these capabilities can be mobilised, integrated, and sustained across institutional, sectoral, and national boundaries when disruption occurs.

Box 5.1 The Baltic Cyber Defence Model: A Template for Regional Engineering Cooperation

The significance of the Cooperative Cyber Defence Centre of Excellence (CCDCOE) lies not only in cyber defence. It demonstrates how common competency frameworks, shared exercises, institutional coordination mechanisms, and cross-border professional networks can transform fragmented national capabilities into operational regional capacity. The challenge facing Nordic-Baltic preparedness is whether similar approaches can be developed across other preparedness-critical domains including energy systems, telecommunications, infrastructure restoration, logistics, and operational technology security.

A Nordic-Baltic preparedness engineering network modelled on this architecture, covering power systems resilience, critical communications, and OT/ICS security alongside cyber, would represent a qualitative step toward the shared operational capacity currently missing. It would also provide the career pathway visibility and professional recognition that currently makes preparedness-relevant engineering roles difficult to attract talent into.

Sources: NATO CCDCOE (2024) Locked Shields 2024; Comfort (2007).

The Nordic-Baltic region is arguably more strategically aligned than at any point since the Cold War, yet the governance architecture through which preparedness-relevant engineering capability is developed, coordinated, and mobilised remains fragmented across national systems designed primarily for peacetime sectoral administration. The challenge facing Nordic-Baltic cooperation is therefore not only one of resilience, but increasingly one of operational integration. Preparedness depends on whether the region can transform a collection of highly capable national systems into a more coherent preparedness ecosystem capable of sustaining continuity, adaptation, and recovery under conditions of prolonged systemic disruption.

5.2 The Gap Between Frameworks and Operational Capacity

The cooperative frameworks described above are real and valuable. Frameworks, however, are not capacity. Three structural reasons explain why existing mechanisms have not yet generated the operational engineering capability that preparedness demands.

The deeper issue is not the absence of cooperation. The Nordic and Baltic countries cooperate extensively. The problem is that cooperation remains disproportionately oriented toward consultation, alignment, and information exchange rather than toward the difficult institutional work of building shared operational capability. Preparedness engineering requires forms of coordination that are considerably more demanding than political alignment alone. Critically, it also requires the lifelong learning infrastructure to sustain these capabilities over time, encompassing the capacity to continuously identify emerging competence needs, develop relevant provision, and keep specialised expertise current across a workforce that spans sectors, institutions, and national systems.

Modern preparedness failures rarely emerge from a total absence of capacity. They emerge when individually capable systems prove unable to coordinate rapidly enough once cascading disruption begins (Perrow, 1999; Tierney, 2019). The Iberian blackout of April 2025 illustrated this precisely: no single actor lacked capability, but the interaction between voltage control failures, reactive power gaps, and cascading generation disconnections across multiple operators

produced a result none had modelled or planned for (ENTSO-E Expert Panel, 2026). Infrastructures fail relationally rather than independently. The same applies to preparedness governance.

The Nordic-Baltic region therefore faces a challenge that is fundamentally institutional as much as technological: whether societies that remain organised primarily through nationally bounded administrative systems can generate the degree of operational integration that highly interconnected infrastructure systems now require.

5.3 Preparedness as a Shared Engineering Capability

The growing interdependence of Nordic and Baltic infrastructure systems increasingly makes preparedness a regional rather than purely national engineering challenge. Energy systems, telecommunications networks, subsea infrastructure, logistics corridors, digital services, and satellite-dependent systems operate across borders in ways that make disruption difficult to contain within any single country. The capacity to sustain and restore these systems therefore depends not only on national preparedness arrangements, but also on the ability to coordinate engineering expertise across the region.

This creates a strong rationale for closer cooperation in preparedness-relevant STEM domains. Several of the engineering fields most critical to infrastructure resilience, including operational technology security, advanced power systems management, secure communications, offshore infrastructure engineering, and systems integration, rely on highly specialised expertise that is already scarce across Europe. Smaller national labour markets may struggle to sustain sufficient depth independently across all of these domains over time.

The separation between economic policy and security policy becomes progressively harder to sustain in practice. The engineering domains underpinning infrastructure resilience such as AI-enabled monitoring, advanced telecommunications, quantum-secure communications, autonomous systems, satellite situational awareness, resilient energy systems, are simultaneously growth sectors and preparedness capabilities (ANE, 2024; Mazzucato, 2021).

The challenge is not simply one of producing more engineers. It increasingly concerns how specialist expertise can be shared, coordinated, and mobilised across interconnected infrastructure systems during periods of disruption. This has important implications for how engineering capability itself is understood. The preparedness challenge is often framed as a problem of emergency capacity or reserve mobilisation. In practice, preparedness increasingly depends on maintaining deep civilian competence ecosystems during peacetime across universities, firms, infrastructure operators, and professional communities. Engineering capability accumulates slowly through operational experience, institutional continuity, and sustained investment in specialist education and applied research (Nelson, 1993). The workforce pipelines, institutional networks, and applied research environments that generate it take decades to build and are not easily reassembled once they have dispersed. The Nordic-Baltic region possesses important advantages in this respect. High institutional trust, advanced public sectors, strong engineering traditions, and relatively dense cooperation between universities, industry, and infrastructure operators provide foundations that many other European regions lack. Yet these same systems were largely designed around national labour markets and nationally bounded policy frameworks. The strategic environment is now demanding a scale of cross-border engineering coordination for which existing governance arrangements were not originally constructed.

This places greater importance on cross-border professional mobility, cooperation between universities and infrastructure operators, shared training environments, and stronger alignment between preparedness planning and long-term workforce development.

Professional engineering associations, universities, infrastructure operators, and regional cooperation frameworks could potentially play a larger role in strengthening this capability base collectively. More systematic regional cooperation around specialist training, mutual recognition of qualifications, and workforce intelligence could help reduce fragmentation while strengthening regional preparedness capacity over time.

5.4 From Cooperation to Operational Capacity: Three Preconditions

For Nordic-Baltic cooperation to function as a genuinely shared preparedness system, closer coordination around engineering capability will increasingly be necessary. One important step would be a clearer regional overview of where preparedness-relevant engineering strengths and workforce gaps exist across the Nordic and Baltic countries, particularly in sectors such as energy systems, telecommunications, digital infrastructure, logistics, and operational technology.

A second priority concerns practical interoperability. In a prolonged disruption affecting multiple countries simultaneously, engineers and technical specialists may need to work across borders far more rapidly than current systems easily allow. This raises questions concerning qualifications recognition, security clearances, operational coordination, and the ability to mobilise specialised expertise quickly when infrastructure systems are under pressure.

Finally, preparedness planning itself may need to integrate workforce capability more directly into regional cooperation frameworks. Discussions within NORDEFECO and NATO increasingly address infrastructure resilience and operational continuity, but engineering workforce development still tends to remain fragmented across national education systems, sectoral policies, and infrastructure operators. A more coordinated regional approach could help strengthen long-term preparedness capacity across the Nordic-Baltic region as a whole.

What ultimately distinguishes operational preparedness from political preparedness is the capacity to act under conditions where coordination mechanisms themselves are under pressure. Crisis situations compress decision time, overload communication systems, generate uncertainty, and frequently blur institutional mandates. Under such conditions, preparedness depends less on abstract plans than on whether trusted operational relationships, interoperable professional cultures, and pre-existing coordination routines already exist across organisations and borders (Comfort, 2007).

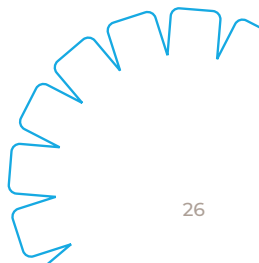
This places engineering professions in a strategically unusual position. Engineers increasingly function not only as technical specialists but also as institutional integrators operating across infrastructures, organisations, and jurisdictions

simultaneously. The preparedness challenge is therefore not reducible to technical education alone. It concerns whether societies can sustain professional ecosystems capable of operating effectively across technological complexity, institutional fragmentation, and geopolitical instability as a single operational reality.

From this perspective, preparedness is inseparable from questions of institutional design. The issue is not simply how to protect infrastructure. It is whether the governance arrangements connecting states, markets, universities, and professional institutions can generate the long-term coordination that highly interconnected infrastructure systems require.



The challenge is not simply one of producing more engineers. It increasingly concerns how specialist expertise can be shared, coordinated, and mobilised across interconnected infrastructure systems.



06. Preparedness engineering domains

Chapters 1 to 5 argued that preparedness in the Nordic-Baltic region increasingly depends on civilian engineering capability embedded across interconnected infrastructure systems. They also showed that although the region possesses substantial engineering depth, the institutional systems needed to coordinate and sustain that capability under prolonged disruption remain fragmented.

The focus now shifts from preparedness as a strategic concept to preparedness as an operational engineering challenge. Its focus is the competencies required to sustain, protect, restore, and adapt critical infrastructure systems under conditions of disruption, hybrid pressure, and technological change.

Modern preparedness failures rarely occur because infrastructure does not exist. They occur because systems become too interconnected, too complex, or too dependent on scarce expertise to be restored rapidly once disruption begins. The limiting factor is therefore increasingly not infrastructure itself, but the availability of engineers capable of operating across interconnected physical, digital, and organisational systems under pressure.

Three broad categories of preparedness engineering are in focus. The first concerns systems continuity engineering: the competencies required to maintain and restore critical infrastructure during disruption. The second concerns threat-adaptive engineering: the competencies required to detect and respond to hostile interference in real time. The third concerns frontier capability engineering: emerging domains such as AI-enabled monitoring, autonomous systems, quantum-secure communications, advanced materials, and space-enabled situational awareness, where preparedness requirements are evolving faster than workforce systems can adapt.

Across all three categories, a common pattern emerges. Preparedness increasingly depends on hybrid engineering profiles combining infrastructure expertise, digital systems capability, cybersecurity, operational coordination, and the ability to make decisions under degraded and uncertain conditions.

6.1 Systems Continuity Engineering

The Nordic region's deepest preparedness engineering competence lies in power systems. Managing geographically dispersed, weather-dependent generation across tightly interconnected grids has produced strong capability in power electronics, grid management, substation protection, and large-scale offshore wind integration (NATO, 2023; ENTSO-E, 2024). Black-start engineering — the restoration of a grid after a total blackout without an external power source — represents the most demanding expression of this domain. Expertise remains concentrated within the

technical teams of transmission system operators such as Energinet, Fingrid, Statnett, and Svenska kraftnät.

Two structural weaknesses stand out. First, black-start expertise is concentrated within a relatively small number of engineers and specialist contractors whose tacit operational knowledge is not routinely documented or transferred systematically (ENTSO-E Expert Panel, 2026). Second, utility management systems increasingly depend on engineers who can combine power systems expertise with understanding of cybersecurity risks embedded in digital control architectures. Existing educational pathways do not yet produce this hybrid profile at sufficient scale (ENISA, 2024).

Box 6.1: Engineers in the Dark: The Black-Start Challenge

The 28 April 2025 Iberian blackout, the most severe power system collapse in Europe in more than two decades, demonstrated the growing complexity of restoring highly interconnected electricity systems under crisis conditions. ENTSO-E's final report concluded that the blackout resulted from interacting factors including oscillations, voltage-control weaknesses, and cascading generation disconnections that existing operational arrangements were not designed to manage effectively.

The incident also highlighted the strategic importance of highly specialised grid restoration and black-start expertise. Large-scale restoration depends on a relatively small pool of engineers capable of coordinating transmission operations, voltage control, and cross-border recovery under extreme conditions. As European electricity systems become more tightly coupled and technically complex, preserving and transferring this operational expertise is becoming an increasingly important preparedness challenge.

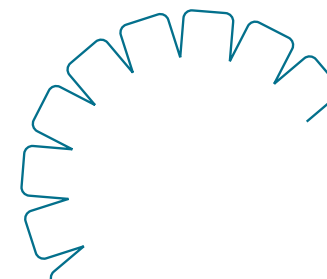
Sources: European Network of Transmission System Operators for Electricity (ENTSO-E) (2026) *Final Report on the Grid Incident in Spain and Portugal on 28 April 2025*.

6.2 Operational Technology and Industrial Control Systems Security

Operational technology and industrial control systems security illustrates a widening mismatch between infrastructure exposure and defensive capability. As industrial systems become increasingly connected to cloud and IT environments, critical infrastructure in energy, water, transport, and manufacturing is exposed to cyber threats capable of generating physical disruption.

The workforce shortage is substantial. ENISA's NIS Investments 2024 report found that more than three-quarters of organisations struggle to recruit cybersecurity professionals, with OT-specific expertise among the scarcest capability areas (ENISA, 2024). The problem is not only quantitative but also technical. Much critical infrastructure still relies on legacy control systems designed before networked integration became standard. Securing these systems requires engineers who understand both industrial processes and cybersecurity, a combination few educational programmes currently produce systematically.

A further weakness concerns incident response. NIS2 reporting requirements assume operators possess engineering teams capable of diagnosing attacks, isolating faults, and restoring operations while physical systems remain live. In practice, many organisations lack this depth of operational expertise. (European Commission, 2022).



Box 6.2 Estonia's CCDCOE: A Model for Regional Capability Development

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn demonstrates that a small national engineering workforce can achieve disproportionate regional influence through deliberate institutional investment in a specialist domain. Its Locked Shields exercises explicitly test the integrated engineering and operational competency that operational technology security demands, combining legal, technical, and operational dimensions in ways that reflect the cross-disciplinary profile preparedness engineering increasingly requires (NATO CCDCOE, 2024).

The CCDCOE model is directly relevant to the governance gap identified in previous parts of the report. It shows that shared operational capacity can be built incrementally through exercise infrastructure, competency standardisation, and institutionalised knowledge sharing, without requiring the prior establishment of a unified regional authority.

Sources: NATO CCDCOE (2024) *Locked Shields 2024*.

6.3 Telecommunications, Subsea Infrastructure, and Satellite Engineering

Finland's Nokia and Sweden's Ericsson remain central to Europe's mobile network infrastructure capability. The engineering ecosystems built around these firms constitute a preparedness asset of strategic importance. Commercial restructuring therefore carries implications extending beyond employment alone. Nokia reduced its workforce from approximately 103,000 employees in 2018 to around 74,100 by end-2025, while Ericsson eliminated close to 17,000 positions after 2022 (Nokia, 2025; Ericsson, 2026). Competence in radio-frequency engineering, network architecture, telecommunications software systems, and large-scale network integration cannot easily be replaced within short timeframes.

The preparedness significance of these capabilities extends beyond telecommunications markets themselves. Secure communications, satellite connectivity, subsea cables, cloud infrastructure, and digital public services

increasingly depend on engineers capable of maintaining operational continuity under adversarial conditions. As infrastructure systems become more interconnected, telecommunications engineering also becomes more operationally integrated with cybersecurity, space-based services, and critical infrastructure restoration.

A further vulnerability concerns repair and restoration capability. Subsea cable systems and communications interconnectors depend on highly specialised engineering crews, limited repair vessels, and complex cross-border coordination arrangements. The bottleneck is often not technical feasibility, but the availability of restoration capacity at sufficient scale during prolonged disruption.

Box 6.3: Ukraine's Infrastructure Engineers: Operational Lessons

Ukraine's experience since 2022 demonstrates that telecommunications resilience depends not only on technical architecture, but also on engineering workforce capability under crisis conditions. Ukrainian engineers maintained digital government services and communications continuity through distributed network architectures, rapid rerouting, emergency satellite connectivity, and continuous infrastructure repair under active attack conditions.

For the Nordic-Baltic region, the lesson is that telecommunications resilience under adversarial conditions requires not only the technical architecture that makes distributed operation possible, but a workforce culture that enables engineers to act with operational authority and speed. Building that workforce culture in peacetime, through exercises and structured response protocols, is a preparedness investment of the same order as procuring hardware or upgrading infrastructures.

Sources: NATO (2023) *Civil Preparedness*; ENISA (2024) *NIS Investments 2024*.

6.4 Civil and Structural Resilience Engineering

During the Cold War, Finland and Sweden embedded preparedness considerations directly into civil engineering standards for public infrastructure and buildings. Much of this capability weakened after 1989. Sweden's Defence Commission concluded in 2023 that the country's civil defence system was not designed to manage armed attack, reflecting decades of institutional dismantlement (Försvarsdepartementet, 2023). Finland remains the principal regional exception, having maintained significant continuity in shelter engineering and civil defence planning.

A second weakness concerns assessment and retrofitting capacity for existing infrastructure. Much critical infrastructure was designed for a different threat environment. CER obligations increasingly require engineers capable of evaluating infrastructure resilience under contemporary hybrid and military risk conditions, yet professional standards and training systems have not fully adapted.

Civil and structural engineering therefore functions as a foundational preparedness capability. Restoring power systems or communications networks is of limited value if the physical infrastructure supporting those systems cannot withstand disruption.

6.5 Logistics and Supply-Chain Continuity Engineering

The Nordic region possesses substantial logistics capability developed through different national pathways: Norway's offshore supply-chain management, Denmark's globally integrated logistics ecosystems around Maersk and DSV, and Finland's Total Defence model linking commercial logistics to preparedness planning.

The difficulty lies in translating commercial logistics optimisation into preparedness capability. Commercial supply chains prioritise efficiency under normal operating conditions. Preparedness logistics requires maintaining operational continuity under disruption, rapidly rerouting supply flows, and sustaining minimum viable function in degraded environments.

In many areas, the underlying engineering expertise exists somewhere within the Nordic ecosystem, but it was developed primarily for commercial rather than adversarial operating conditions.

6.6 Threat-Adaptive Engineering

The competency domains examined in Section 5.1 focused primarily on continuity: maintaining infrastructure and essential services during disruption. The domains examined here involve a different challenge. They concern systems that must detect, interpret, and respond to hostile interference while it is happening.

This distinction matters because modern infrastructure is no longer exposed only to accidental failure or natural disruption. Energy systems, telecommunications networks, industrial control systems, and transport infrastructure increasingly operate in environments where cyber intrusion, data manipulation, sabotage, and coordinated hybrid attacks are persistent risks rather than exceptional events. Preparedness therefore requires engineering systems that can adapt dynamically under adversarial conditions rather than simply continue operating during stress.

6.7 AI-Enabled Infrastructure Monitoring

Critical infrastructure has become an increasingly important target in hybrid conflict. Many operational environments rely on supervisory control and data acquisition systems that remotely manage electricity grids, transport systems, industrial production, and communications infrastructure. Manipulation of these systems can generate cascading failures across multiple sectors simultaneously.

AI-enabled monitoring changes how infrastructure is protected. Traditional monitoring systems rely heavily on predefined thresholds and rule-based alarms. Machine learning systems can instead analyse large volumes of operational data continuously and identify anomalous patterns before failures escalate.

This creates demand for hybrid engineering profiles combining signal processing, embedded systems engineering, cybersecurity, machine learning operations, and detailed understanding of physical infrastructure systems.

Box 6.4: Finland: Fingrid and AI-Augmented Grid Security

Fingrid operates Finland's national transmission grid, which has acquired growing strategic importance following Russia's full-scale invasion of Ukraine and Finland's NATO accession. Across the Finnish energy sector, investments in cybersecurity, digital resilience, and operational technology monitoring have accelerated, including growing interest in AI-assisted anomaly detection for critical infrastructure systems. The competency profile required increasingly combines power systems engineering, data analytics, and operational technology cybersecurity expertise — a combination widely recognised as difficult to recruit across Europe's critical infrastructure sectors. Finnish universities, including Aalto University, have correspondingly expanded provision in cybersecurity, resilient energy systems, and secure digital infrastructure. The Finnish case illustrates how preparedness increasingly depends on closer coordination between infrastructure operators, governments, and universities in developing hybrid engineering competencies for resilient infrastructure operation under conditions of heightened geopolitical risk.

Sources: Finnish Government (2024) *Finland's Cyber Security Strategy 2024–2035*. Helsinki: Prime Minister's Office. Fingrid — *The Finnish Transmission System*; Aalto University Cybersecurity Programmes; Finland increases cybersecurity spending in response to AI-enabled threats (C4ISRNET, 2024).

6.8 Autonomous Systems and Counter-Drone Technologies

Autonomous systems and counter-drone technologies represent one of the fastest-moving preparedness capability domains. Ukraine's rapid expansion of drone production demonstrated that relatively low-cost autonomous platforms can now perform reconnaissance, electronic warfare, and precision operations at large scale. Drone incursions across Nordic airspace in 2025 further reinforced the urgency of European counter-UAS capability development (counter-unmanned aerial systems, commonly known as drone defence).

The required engineering competencies fall into two interconnected areas. The first concerns autonomous systems themselves: control systems, sensor fusion, computer vision, swarm coordination, and resilient operation under jamming conditions. The second concerns counter-drone capability: radar engineering, radio-frequency management, electronic warfare, and directed-energy systems.

The central difficulty is that threat evolution now moves faster than conventional curriculum development cycles.

Box 6.5: Sweden and Estonia: Two Models of Counter-Drone and Autonomous Systems Development

Sweden's Loke counter-UAS system illustrates rapid defence capability development in response to evolving drone threats. Developed by Saab using modular integration of radar, electronic warfare, and remote weapon technologies, the system received a procurement order from the Swedish Defence Materiel Administration in 2026, with deliveries planned for 2027–2028.

Estonia represents a different model. Milrem Robotics has become one of Europe's leading developers of unmanned ground systems, demonstrating how small states can build preparedness-relevant capability through specialised robotics and autonomy firms with strong international linkages.

Together, the two cases illustrate a broader workforce challenge: autonomous systems and counter-drone technologies evolve faster than traditional curriculum cycles. Preparedness therefore increasingly depends on rapid technical education models and stronger links between civilian engineering ecosystems and defence capability development.

Sources: Saab (2025) 'The "Loke" counter-drone concept debuts in NATO mission', Saab Newsroom, 29 September. Saab (2026) 'Saab receives order for counter-unmanned aerial system from Sweden', Saab Newsroom, 2 April. Milrem Robotics (2024) 'About us'.

Estonian Embassy in Kyiv (2024) 'Estonian company Milrem Robotics partners with the Ukrainian Defence Industry to forge next-generation robotic systems', 7 February.

07. Frontier Preparedness Engineering and Emerging Competency Needs

The domains examined in this section operate at the leading edge of the preparedness engineering frontier.

They share three structural features: the underlying technologies are developing faster than educational and institutional systems can track; the competency profiles they require are genuinely novel and not yet defined within established engineering disciplines; and the commercial demand for the same talent is intense, creating recruitment and retention challenges that public and defence sector employers are poorly positioned to meet.

7.1 Quantum-Secure Communications

Quantum-secure communications may become one of the most demanding preparedness capability challenges of the coming decade because it requires replacing encryption systems embedded across critical infrastructure while the supply of specialised expertise remains extremely limited.

Quantum computing could eventually weaken the encryption systems currently protecting government communications, financial transactions, telecommunications infrastructure, and energy systems. As a result, governments and infrastructure operators increasingly face the task of transitioning toward quantum-resistant encryption architectures and quantum-based secure communications technologies.

This is not a conventional software transition. It affects highly interconnected infrastructure ecosystems across multiple sectors simultaneously and requires expertise spanning cybersecurity, telecommunications engineering, photonics, embedded systems, and quantum physics.

The workforce pipeline remains narrow. Quantum information science programmes exist across the Nordic region, but graduate output remains limited relative to projected demand.

(NordForsk, 2025).

Box 7.1: Sweden and Denmark: Complementary Quantum Strategies

Sweden's Wallenberg Centre for Quantum Technology (WACQT), coordinated by Chalmers University of Technology, is among Europe's largest national quantum initiatives and includes the development of superconducting quantum hardware within Sweden itself (WACQT, 2024).

Denmark has pursued a complementary strategy focused on ecosystem development and capital mobilisation. In October 2025, the Copenhagen based 55 North quantum fund announced a €300 million fund backed by EIFO and Novo Holdings, signalling a major long-term commitment to quantum commercialisation and scaling (Novo Holdings, 2025).

Together, the Swedish and Danish approaches illustrate complementary models of quantum capability development. The longer-term challenge is whether these investments can be translated into a sufficiently deep Nordic workforce pipeline in quantum engineering and systems integration.

Sources: Wallenberg Centre for Quantum Technology (WACQT) (2024) WACQT: Wallenberg Centre for Quantum Technology. Gothenburg: Chalmers University of Technology. Available at: WACQT official site; Novo Holdings (2025) Novo Holdings acts as cornerstone investor in 55 North, the world's largest dedicated quantum fund. Copenhagen: Novo Holdings, 2 October.

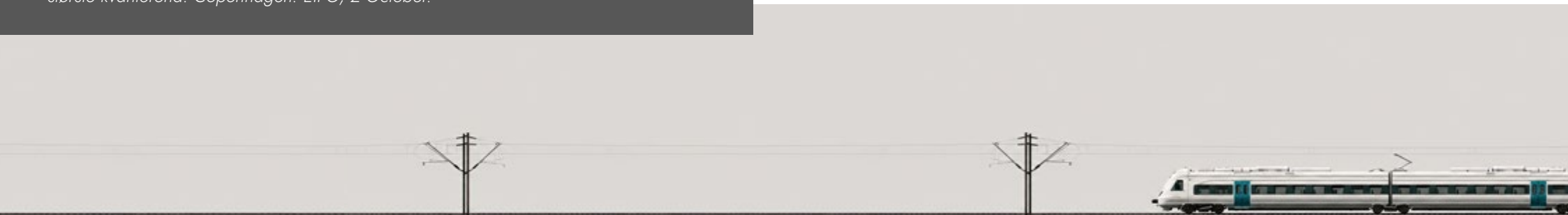
Export and Investment Fund of Denmark (EIFO) (2025) Danmark lancerer verdens største kvantefond. Copenhagen: EIFO, 2 October.

7.2 Advanced Materials and Rapid Infrastructure Repair

Preparedness increasingly depends not only on protecting infrastructure, but also on restoring it rapidly after damage. This creates growing strategic importance for advanced materials and repair engineering.

This domain integrates materials science, additive manufacturing, and structural engineering. Advanced materials relevant to preparedness include ultra-high-performance concrete for hardened shelters, self-healing polymers and composites for infrastructure components, and thermally stable electronic encapsulants for sensitive field-deployed components. Field-deployable metal 3D printers capable of producing replacement mechanical components have been piloted in Nordic defence logistics contexts, substantially reducing lead times for critical spares. Relevant capabilities include hardened construction materials, self-healing composites, additive manufacturing, and field-deployable repair technologies capable of reducing restoration time during infrastructure disruption. In highly interconnected infrastructure systems, prolonged outages can generate cascading effects across energy, transport, communications, and industrial operations. The speed with which damaged systems can be stabilised and returned to minimum functional capacity therefore becomes a critical operational factor.

Advanced materials and repair engineering remain comparatively underdeveloped within preparedness planning despite their growing importance for infrastructure continuity under prolonged disruption.



Box 7.2: Norway: SINTEF and Research in Materials Resilience

Norway's SINTEF has developed substantial capability in materials resilience, structural integrity monitoring, and infrastructure repair technologies through sustained engagement with offshore energy systems in remote and harsh environments (SINTEF, 2024). Its 5G COMPAD project explores how civilian 5G technologies can be adopted in defence and peacekeeping operations, a direct expression of the omni-use logic.

Norway's April 2024 Long-Term Defence Plan commits an additional NOK 600 billion over twelve years, creating sustained procurement demand for the materials and repair capabilities in which SINTEF specialises (Norwegian Ministry of Defence, 2024). The challenge is translating that procurement demand into a workforce pipeline: advanced materials engineering is a small-scale discipline in all Nordic countries, and current graduate output is insufficient to meet the demand that defence procurement investment will generate.

Sources: SINTEF (2024); Norwegian Ministry of Defence (2024) Long-Term Defence Plan.

7.3 Space-Enabled Situational Awareness and Positioning Resilience

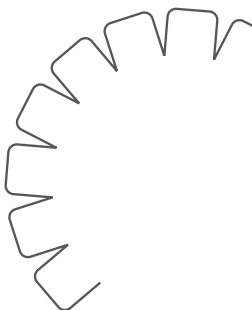
Space-based assets have become foundational infrastructure for both civilian and defence operations across the Nordic-Baltic region. The region has become a primary documented zone of GNSS disruption: Finnish, Estonian, and Lithuanian aviation authorities have issued repeated warnings since 2022, and the International Civil Aviation Organisation has registered the Baltic and Barents regions among the most GPS-degraded environments globally (ICAO, 2024).

An additional layer of engineering capability is now required: space domain awareness, meaning the ability to monitor, understand, and respond to threats and disruptions in space-based systems. The Nordic commercial space ecosystem, led by Finland's ICEYE (which operates the world's largest commercial synthetic aperture radar satellite constellation) alongside Kongsberg Satellite Services and OHB Sweden, provides strategically significant engineering and operational expertise (ICEYE, 2024; Kongsberg Satellite Services, 2024; OHB Sweden, 2024).

7.4 System-of-Systems Modelling and Resilience Analytics

The competency domains examined in Sections 6.1 to 6.3 share a structural feature: none operates in isolation. Understanding how their interdependencies behave under stress, and designing institutions and systems that maintain essential functions when components fail, requires a distinct meta-competency: system-of-systems modelling and resilience analytics. Engineers working in this domain require hybrid competencies combining quantitative modelling, cyber-physical systems understanding, infrastructure operations, and the ability to translate technical risk into decision-relevant insights for policymakers, operators, and crisis-management authorities. Elements of this capability already exist across Nordic engineering education and research in fields such as energy systems modelling, Arctic infrastructure engineering, cyber-physical systems, and risk analysis. However, these competencies remain fragmented across disciplines and institutional environments and are rarely organised as a dedicated preparedness-oriented engineering specialisation.

This gap has important operational implications. System-of-systems modelling makes it possible to identify which dependencies, competencies, and infrastructure functions become the critical bottlenecks under crisis conditions. Without that capability, preparedness planning risks overlooking the interconnections most likely to determine whether disruption can be contained, coordinated, and recovered from effectively.



Box 7.3: Modelling Infrastructure Interdependence Under Crisis

Research environments at the Technical University of Denmark examine how failures cascade across interconnected infrastructure systems, bringing together expertise from electrical engineering, computer science, economics, and security studies to model recovery dynamics under conditions of disruption. Broader European infrastructure resilience analyses similarly show that failures in energy, communications, transport, and digital systems rarely remain isolated, but instead propagate through tightly coupled dependencies that complicate restoration efforts.

The key implication for workforce planning is that recovery capacity depends not only on physical assets or financial resources, but on the availability of engineers capable of coordinating multiple interdependent repair processes simultaneously. In this context, system-of-systems modelling is not simply an academic exercise. It provides a practical basis for identifying which engineering competencies are most likely to become operational bottlenecks during crisis response and recovery.

Sources: Technical University of Denmark research centres on cyber-physical energy systems and infrastructure resilience. ; ENTSO-E Expert Panel (2026).

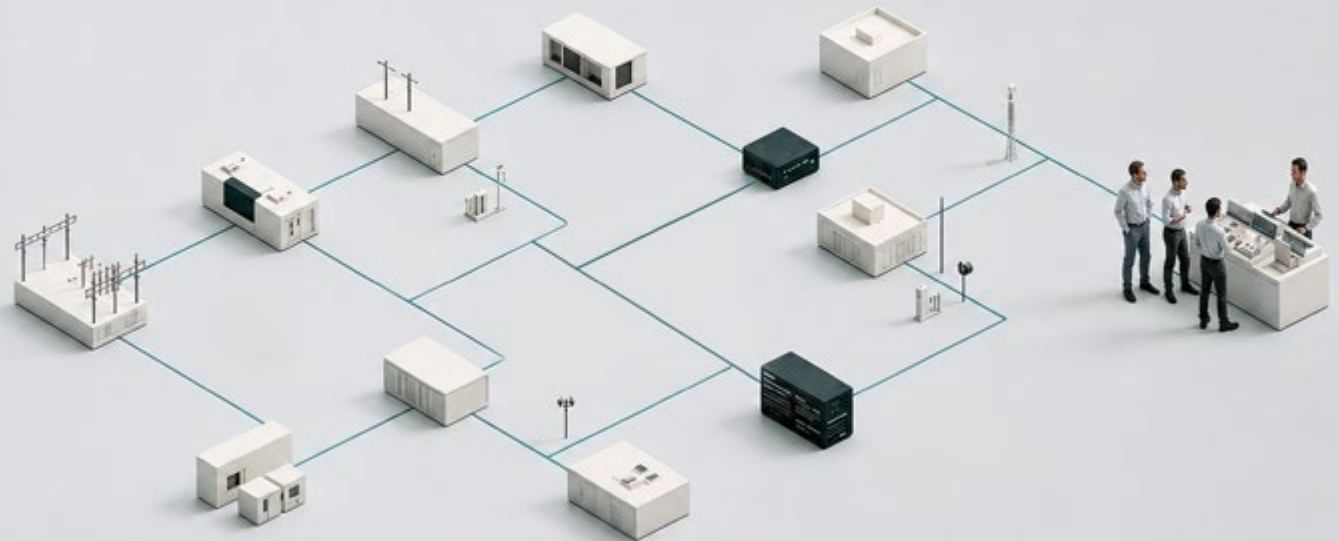


Table 7.1: Cross-Domain Preparedness Engineering Profiles

Preparedness Engineering Profile	Core Engineering Domains	Cross-Domain Competencies	Why they are Critical for Preparedness	Key Workforce Challenge
OT/ICS Security Engineer	- Industrial control systems - SCADA - Operational technology - Automation engineering	- Cybersecurity - Incident response - Risk management - NIS2/CER compliance	Protects and restores critical infrastructure where cyber incidents cause physical disruption	Shortage of engineers combining industrial systems expertise with cybersecurity capability
Black-Start and Grid Restoration Specialist	- Power systems engineering - Transmission operations - Grid control - Power electronics	- Crisis decision-making - Systems coordination - Infrastructure restoration - Emergency operations	Enables recovery of electricity systems following major outages and cascading failures	Expertise concentrated among a small and ageing cohort with significant tacit knowledge at risk
Resilience-Capable Civil and Structural Engineer	- Structural engineering - Transportation infrastructure - Water systems - Construction engineering	- Risk assessment - Resilience design - Critical infrastructure protection - Adaptation planning	Designs and upgrades infrastructure to withstand disruption, sabotage, and extreme events	Preparedness-oriented resilience competencies remain weakly institutionalised in engineering education
Crisis Logistics and Infrastructure Continuity Engineer	- Supply-chain engineering - Transport systems - Logistics networks - Infrastructure operations	- Scenario planning - Continuity management - Emergency logistics - Cross-sector coordination	Maintains critical flows of energy, equipment, materials and services during sustained disruption	Commercial logistics optimisation does not automatically translate into preparedness capability
AI-Enabled Infrastructure Systems Engineer	- Data engineering - Infrastructure operations - Automation - Systems engineering	- Machine learning - Anomaly detection - Cybersecurity - OT integration	Supports predictive monitoring, early warning, and adaptive infrastructure management under stress	Hybrid AI-infrastructure profiles are emerging faster than education and training systems can supply
Quantum-Secure Communications Engineer	- Telecommunications - Networking - Cryptography - Embedded systems	- Quantum technologies - Cybersecurity - Systems integration - Secure communications	Supports transition towards quantum-resistant infrastructure and secure communications architectures	Extremely limited talent pipeline with strong competition from commercial technology sectors

7.5 The Hybrid Competence Challenge: What Cuts Across All Domains

Across all competency domains examined in this chapter, a structural feature recurs: preparedness engineering demands deep domain knowledge combined with one or more adjacent fields that standard engineering education does not produce systematically. Cybersecurity, systems engineering, operational logistics, and scenario analysis each appear repeatedly as essential complements to domain expertise. Six cross-domain profiles stand out as particularly critical and scarce.

- The OT/ICS security engineer who bridges industrial control systems and cybersecurity.
- The black-start and grid restoration specialist who combines power systems expertise with operational authority under pressure.
- The resilience-capable civil and structural engineer who designs in accordance with contemporary threat standards.
- The crisis logistics engineer who sustains minimum viable supply chains under degraded conditions.
- The AI-infrastructure integration specialist who deploys machine learning within operational constraints.
- The quantum-secure communications engineer who manages the transition from current encryption architectures.

These profiles do not map cleanly onto a single existing discipline, and each is in critically short supply relative to CER and NIS2 compliance requirements (European Commission, 2022; ENISA, 2024).

The preparedness domains and profiles identified in this report should be understood as indicators of emerging capability needs rather than blueprints for initial engineering education. These capabilities may be embodied in highly specialised individuals or distributed across multidisciplinary teams. What matters is the ability to combine specialist expertise, systems understanding, and operational coordination effectively under conditions of disruption.

A further dimension cuts across all profiles: tacit knowledge. Black-start engineering, hardened civil design, and subsea cable repair are embedded primarily in practitioner experience rather than in documented standards alone, and in several sub-domains the majority of experienced engineers are within ten to fifteen years of retirement (ENTSO-E Expert Panel, 2026).

The technologies, infrastructures, and regulatory frameworks shaping preparedness are evolving rapidly, while the growing convergence of digital, physical, and security domains makes future competency requirements increasingly difficult to anticipate. Initial engineering education must therefore provide strong scientific, technical, and systems foundations that enable engineers to adapt and build new expertise throughout their working lives.

At the same time, preparedness increasingly depends on responsive lifelong learning systems capable of evolving alongside changing technologies and capability needs. Microcredentials can form a critical component of such systems by creating greater coherence between structured education and work-based learning, while offering flexible pathways through which engineers can acquire highly specialised competencies as requirements evolve. They can also help make acquired skills more visible, portable, and responsive to emerging labour market demand.



What matters is the ability to combine specialist expertise, systems understanding, and operational coordination effectively under conditions of disruption.

Box 7.4: What the Region Has Built: Education and Training for Preparedness Engineering

Dedicated provision for preparedness engineering exists across the Nordic region, but the picture is uneven. The most developed offer concentrates heavily on cybersecurity: Aalborg University's 120 ECTS MSc in Cyber Security, Aalto University's Secure Systems track, and Finland's JAMK/JYVSECTEC applied OT security laboratory constitute a meaningful regional base (Aalborg University, 2024; Aalto University, 2024). Estonia's CCDCOE and its Locked Shields exercises extend that base into live operational practice.

Provision for several other preparedness-critical engineering profiles nevertheless remains comparatively limited and fragmented across Nordic higher education. Institutions such as Norwegian University of Science and Technology, Aalto University, and University of Oulu do provide relevant teaching and research in areas including power-system operation and restoration, resilient energy systems, transport and infrastructure resilience, and supply-chain continuity. However, dedicated educational pathways explicitly focused on black-start and grid restoration engineering, hardened civil infrastructure for crisis conditions, or integrated crisis logistics engineering remain relatively thin and dispersed across courses, laboratories, and research groups rather than institutionalised as major standalone competency tracks. This is particularly significant because these domains depend heavily on operational expertise that is ageing rapidly and often insufficiently codified within formal education systems.

Sources: University web pages; ENISA (2024).

08. Engineering Workforce Constraints and Preparedness Capacity

Chapter 6 and Chapter 7 mapped the current operational and emerging frontier engineering competencies on which preparedness increasingly depends, spanning systems continuity, threat-adaptive capability, and emerging domains such as AI-enabled infrastructure monitoring, autonomous systems, quantum-secure communications, and resilience analytics.

It also showed that these competencies are not being produced, coordinated, or renewed at sufficient scale through existing educational, workforce, and institutional systems. This chapter examines the workforce constraints underlying that gap. Its central argument is that the preparedness challenge facing the Nordic-Baltic region is no longer primarily one of technological awareness or strategic recognition, but of engineering workforce depth, institutional coordination, and long-term upskilling and reskilling strategies.

8.1 The Structural Workforce Constraint

The workforce gap facing the Nordic-Baltic region is not a single problem. It is the compound effect of three structural constraints operating simultaneously. The first is demographic: the engineering workforce most relevant to preparedness is ageing faster than successor cohorts are being formed. The second is distributional: specialised competencies are concentrated in a small number of institutions, firms, and national contexts, a challenge that aggregate workforce statistics obscure. The third is competitive: sectors and employers best positioned to attract preparedness-relevant engineers are systematically outbid by commercial technology and energy employers on compensation, career progression, and working conditions.

These constraints are examined in turn in the following sections.

8.2 The Demographic Constraint: Retirement, Succession, and Tacit Knowledge Loss

The Nordic countries share a demographic profile combining ageing working-age populations with high but insufficient rates of engineering education (Finnish Ministry of Finance / TEK, 2024). Power grid operators, telecommunications network engineers, water system managers, and defence procurement specialists recruited in the 1990s are approaching retirement over the 2025 to 2035 period. In several preparedness-critical sub-domains, including black-start engineering, quantum hardware integration, and subsea cable repair, the practitioner generation is within ten to fifteen years of retirement and no adequate successor cohort is yet in formation (ENTSO-E Expert Panel, 2026; NordForsk, 2025).

The quantitative dimension is substantial. TEK's labour market surveys indicate that 78 per cent of Finnish companies reported a shortage of skilled workers in 2023 (Finnish Ministry of Finance / TEK, 2024). Grid Dynamics estimates a deficit of approximately 10,000 engineers in technology-intensive fields in Norway, including a projected shortfall of over 4,000 cyber security experts (Grid Dynamics, 2025). The Scalers projects a shortage of tens of thousands of software and systems engineers in Sweden within this decade (Scalers, 2024). The Baltic states face additional demographic pressure through net emigration of skilled workers since EU accession. ENISA's NIS Investments 2024 report estimates an EU-wide cybersecurity workforce shortage of approximately 300,000 professionals in 2024 (ENISA, 2024); ISC2's 2024 Cybersecurity Workforce Study estimates the European gap at approximately 424,000 (ISC2, 2024). Net Group's 2026 analysis finds that Estonia alone must expand its cybersecurity workforce by approximately 86 per cent within five years (Net Group, 2026).

The qualitative dimension is equally significant. Several preparedness-critical domains depend on highly specialised expertise concentrated within relatively small professional communities. As experienced engineers retire, the challenge is not simply replacement but ensuring continuity in capabilities that require years of operational practice to develop.



Ai generated image

Box 8.1: Finland's Engineering Workforce Pressures: Key Indicators

TEK's 2024 labour market survey found that the technology sector is characterised by acute shortages in specialised sub-fields (Finnish Ministry of Finance / TEK, 2024). Only 3 per cent of international technology workers in Finland reported they always or almost always felt equal to native Finnish job applicants in recruitment, while 14 % pointed to mostly feeling equals. For foreign tech professionals employed in Finnish companies 16% always or almost felt equal, while 36% reported they mostly felt equal.

These figures point to structural integration challenges with direct implications for workforce adequacy. This is particularly significant in the Finnish context, where demographic constraints and a relatively small domestic labour pool increase dependence on attracting and retaining international engineering talent. Finland's comprehensive security model and the coordination architecture of the National Emergency Supply Agency provide important institutional resilience mechanisms, but they do not resolve the underlying engineering supply challenge if barriers to international recruitment and retention persist.

Sources: Finnish Ministry of Finance / TEK (2025) *International Technology Experts*. P 14. Figure 7.

8.3 The Distributional Constraint: Concentration, Fragility, and the Illusion of Aggregate Adequacy

Aggregate workforce statistics consistently overstate preparedness-relevant engineering capacity because they obscure the distributional concentration of critical competencies. The Nordic-Baltic region produces substantial numbers of engineering graduates each year, but the sub-specialisations most critical to preparedness are produced in much smaller numbers and are concentrated in a limited number of institutions, firms, and national contexts (Finnish Ministry of Finance / TEK, 2024; ENISA, 2024).

Three capacity constraints stand out:

1. First, institutional concentration: the engineering competencies most relevant to preparedness are housed in a small number of firms and public institutions whose restructuring, acquisition, or budget reduction can eliminate regional capability rapidly and without policy visibility. The Nokia and Ericsson workforce reductions previously discussed illustrate this risk: these are not simply commercial employment adjustments but structural reductions in a regional preparedness asset (Nokia, 2025; Ericsson, 2026).
2. Second, Finland's whole-of-society model, Estonia's cyber defence ecosystem, and Norway's offshore engineering base each constitute highly concentrated national capability clusters that are strategically significant for the wider region yet remain only partially embedded within cross-border mechanisms for capability sharing, redundancy, and operational continuity.
3. Third, generational concentration: much of the region's most operationally experienced expertise is concentrated within a single retiring generation, creating succession pressures in domains where replacement capacity is developing more slowly than workforce demand. Preparedness planning requires disaggregated competency mapping at the level of specific roles and sub-specialisations, not sector-level headcount projections.

The sectors competing for Nordic engineering talent are growing rapidly and offering conditions that preparedness-relevant public and defence employers find difficult to match. Major technology companies, including cloud providers, AI research laboratories, and semiconductor firms, have expanded substantially in the Nordic region, recruiting from precisely the talent pool that preparedness planners depend on (Saab AB, 2024). The renewable energy transition represents a second major demand driver: Nordic offshore wind investment will exceed 18 billion euros between 2024 and 2030, requiring large numbers of electrical, mechanical, and systems engineers whose skills overlap substantially with those needed for critical infrastructure protection.

This creates a structural labour market imbalance. The same engineers needed for preparedness-critical infrastructure are also heavily demanded by commercial technology sectors, particularly in AI, cybersecurity, digital infrastructure, and advanced energy systems, where compensation levels are often substantially higher.

Box 8.2: Sweden's Saab and the Defence-Commercial Talent Competition

Saab recruited 2,913 new employees in 2024, representing a 13 per cent year-on-year increase, and employed approximately 25,000 people globally by the end of the year. The company has attempted to strengthen recruitment and retention through a combination of mission-oriented organisational culture, hybrid working arrangements, and long-term incentive programmes that incorporate sustainability and diversity objectives, including targets related to gender balance. The case illustrates a broader structural challenge facing the Nordic defence and preparedness sector: competition for advanced engineering talent increasingly occurs within a labour market shaped by global technology firms with substantially greater compensation capacity. Non-monetary factors can partially offset this imbalance, but they are unlikely to resolve it fully without wider policy interventions, including defence engineering scholarships, public sector compensation reform, and structured public-private talent mobility arrangements.

Source: Saab AB (2025) Annual and Sustainability Report 2024. Stockholm: Saab AB, pp. 66–68.

Public sector and defence employers can partly offset lower compensation through mission-driven work, job security, and flexible working arrangements, as the Saab case above illustrates.

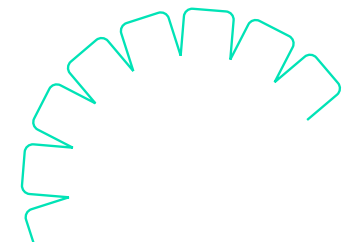
A further challenge concerns the growing overlap between preparedness and green transition workforce demands. The engineers needed for offshore wind, grid modernisation, and energy storage are often the same engineers required for preparedness-critical infrastructure, particularly in power systems, digital infrastructure, and systems integration. Treating these as competing demands for a fixed talent pool is therefore both analytically misleading and strategically counterproductive. The omni-use framing developed in Chapter 2 points instead toward integrated workforce strategies. This includes curriculum reform and engineering education investments designed to produce competency profiles that support both climate transition and preparedness objectives simultaneously, as institutions such as the Technical University of Denmark and Norwegian University of Science and Technology have begun to explore.

Box 8.3: Engineering the Energy Transition and Preparedness Simultaneously

The Technical University of Denmark and the Norwegian University of Science and Technology have both expanded research and educational activities in areas such as resilient energy systems, smart grids, digital infrastructure, systems integration, and energy security. While these initiatives are primarily linked to the green and digital transition, they also contribute to competency profiles relevant for preparedness and critical infrastructure resilience.

Sources: DTU Wind and Energy Systems ; DTU Power and Energy Systems.

NTNU Energy Transition Initiative; NTNU Resilient and Integrated Energy Systems.



8.4 The Preparedness Conversion Challenge

Technological strength does not convert automatically into preparedness capacity. The Nordic region's engineering base in energy systems, telecommunications, digital infrastructure, advanced manufacturing, and AI-enabled industrial systems is substantial — but the competencies embedded in that base were developed primarily for commercial operating conditions, and the institutions that govern them are not designed to mobilise them under disruption.

Three structural misalignments account for this gap. Engineering expertise is concentrated in globally oriented firms whose investment priorities and workforce allocation models follow commercial rather than resilience logic. Specialised talent flows toward sectors offering higher compensation and faster innovation cycles, even where preparedness systems depend on identical competencies. At the same time, preparedness-related demand signals generated through CER, NIS2, NATO resilience requirements, and national preparedness strategies rarely translate into sufficiently granular intelligence for education and training providers. Universities, vocational institutions, and continuing professional education systems therefore struggle to anticipate emerging competence requirements. Finally, the actors on whom preparedness depends, including public authorities, infrastructure operators, defence institutions, technology firms, and universities, operate on different funding cycles, time horizons, and incentive structures, with no systematic mechanism to align them around shared resilience objectives.

A further dimension of the preparedness conversion challenge concerns the distinction between access to technology and the capability to deploy it effectively. The Nordic-Baltic region generally enjoys access to advanced technologies through global markets and international partnerships. Yet preparedness depends equally on whether organisations possess sufficient engineering depth, operational expertise, and institutional capacity to adapt, integrate, repair, and scale these technologies under crisis conditions. In this sense, technological sovereignty is fundamentally a capability challenge rather than an ownership challenge.

This issue is reinforced by decades of specialisation and outsourcing. Where critical knowledge of infrastructure architecture, industrial control systems, telecommunications networks, cloud environments, or cybersecurity operations resides primarily with external providers, the ability to mobilise and repurpose

capability during prolonged disruption may be constrained. Preparedness therefore requires not only technological investment but also the retention of strategic competencies, institutional memory, and engineering judgement within the organisations and ecosystems responsible for societal resilience.

The consequence is that preparedness gaps can open silently within otherwise sophisticated engineering economies. Closing them requires deliberate institutional investment: structured pathways connecting commercial competence to preparedness functions that are currently, across most Nordic and Baltic countries, informal, underfunded, and dependent on individual initiative rather than design (Heinrich Böll Stiftung, 2023; NORDEFCO, 2023). CER and NIS2 compliance frameworks seem to assume that investment exists; in most cases it does not.

8.5 Gender, Diversity, and the Effective Talent Pool

The workforce constraints documented in Sections 8.1 to 8.4 are compounded by a persistent and under-addressed supply-side failure: the systematic exclusion of large portions of the available talent pool from preparedness-relevant engineering careers. This is not primarily an equity question, though it is that too. It is a quantitative workforce supply question with direct implications for preparedness planning. Women comprise between 20 and 32 per cent of engineering graduates across the Nordic-Baltic region; in sub-fields such as radio frequency engineering, radar, and electronic warfare, representation falls below 15 per cent (Norwegian Ministry of Defence, 2024). A sector that draws talent from only part of the population will struggle to meet growing workforce demand. Gender balance, diversity, and inclusion are therefore not optional social objectives, but structural requirements for long-term workforce capacity.

The barriers to entry are well documented: engineering education cultures favouring individual technical problem solving; security clearance processes designed around traditional career patterns; limited flexible working arrangements in preparedness relevant operational roles; and weak institutional pathways linking civilian infrastructure, preparedness, and defence related careers (OECD, 2024).

In the Baltic states, Russian-speaking minority populations represent a technically educated community whose participation in preparedness roles is constrained by security concerns, language barriers, and trust deficits. Across Sweden and Norway, immigrant professionals with engineering backgrounds face credential recognition barriers and network disadvantages that constitute a straightforward capacity loss in already-scarce labour markets.

Security requirements introduce an additional constraint on the effective talent pool that is rarely considered in preparedness planning. In Sweden, the number of Swedish engineering doctoral students fell by 36 % between 2010 and 2023, while international students increased to 55 per cent of all engineering doctoral students (Sveriges Ingenjörer, 2025, p. 3). In 2023, around 29 per cent of international engineering doctoral students originated from China, Iran, or Russia (ibid). At the same time, security protection requirements are being extended across defence, critical infrastructure, energy, telecommunications, and other security-sensitive sectors under the Swedish Security Protection Act (SFS 2018:585). While security clearance decisions are made individually, the expansion of security-classified positions means that doctoral graduation figures may overstate the pool of talent immediately available for strategically sensitive functions. As a result, workforce availability itself is emerging as a preparedness challenge, particularly in domains already characterised by shortages of highly specialised engineering expertise.

Box 8.4: Iceland and Norway: Contrasting Approaches to Gender Balance in Engineering

Iceland consistently ranks among the leading OECD countries on measures of gender equality and female labour market participation, including participation in science and technology-related occupations. Comparative international analyses have identified Iceland as one of the countries with the highest shares of women employed in STEM-related roles, reflecting sustained investment in gender-inclusive education pathways, childcare provision, and workplace equality measures. Norway has similarly expanded efforts to strengthen gender balance in engineering, technology, and defence-related sectors through targeted recruitment initiatives, gender-equality legislation, and increased focus on diversity within national preparedness and defence planning.

The broader Nordic lesson is that gender equity should not be treated solely as a social policy objective, but as an operational workforce strategy linked to preparedness capacity. Expanding women's participation in engineering and technology enlarges the available talent pool at a time when demand for preparedness-critical competencies is accelerating across energy, cybersecurity, infrastructure, and defence-related sectors.

Sources: CloudZero (2023) *The Leading Countries Breaking Barriers for Women in STEM*.

World Economic Forum (2024) *Global Gender Gap Report 2024*.

Norwegian Ministry of Defence (2024) *Defence Commission Report*.



Gender equity should not be treated solely as a social policy objective, but as an operational workforce strategy linked to preparedness capacity.

8.6 Implications for Preparedness Planning

Three findings emerge clearly from the analysis. First, the engineering competencies on which Nordic-Baltic preparedness depends are not absent. They exist, distributed across transmission operators, telecommunications firms, defence contractors, research universities, and national cyber agencies. The problem is structural: they are fragmented across institutions with different mandates, concentrated in firms whose investment priorities are shaped primarily by commercial conditions, and held disproportionately by a cohort approaching retirement without adequate succession in place. The workforce reductions at Nokia and Ericsson illustrate how quickly regionally significant capability can contract when commercial pressures and preparedness interests are not aligned through any shared institutional mechanism.

Second, the failures most likely to materialise are not catastrophic collapses of capability but coordination failures under pressure. These are moments when individually competent systems cannot act together quickly enough because the institutional connections between them were never built. The Iberian blackout and Ukraine's telecommunications experience each illustrate a version of this dynamic.

Third, the governance frameworks now being implemented, including CER, NIS2, and national resilience strategies across the region, assume a degree of workforce depth, institutional coordination, and cross-sector alignment that does not yet exist at the scale they require. The gap is not one of strategic awareness or political will. It concerns the formal and informal rules, funding mechanisms, and coordination arrangements that determine whether engineering capability developed in one sector can be sustained, shared, and mobilised across others when conditions require it. CER and NIS2 compliance deadlines are advancing while the workforce development, cross-sector coordination mechanisms, and funding arrangements needed to meet them remain largely unchanged. Whether the gap between framework requirements and institutional capacity is narrowing or widening cannot be determined with confidence, because no Nordic or Baltic country currently conducts systematic monitoring of preparedness-relevant engineering workforce capacity at the level of sub-specialisation that would make such an assessment possible. That absence of measurement is itself part of the problem.

09. Engineering Capacity and the Future of Preparedness

This final chapter draws together the report's central argument: that preparedness in the Nordic-Baltic region increasingly depends on the capacity to sustain and coordinate complex civilian engineering systems under conditions of prolonged disruption.

The challenge is no longer simply one of infrastructure investment, technological sophistication, or strategic awareness. It concerns whether the institutional systems responsible for developing, renewing, and mobilising specialised engineering capability can adapt to a more unstable and interconnected operating environment. The chapter therefore moves beyond competency mapping to examine the broader governance and workforce implications of preparedness. It argues that preparedness and economic competitiveness, long treated as separate policy domains, are converging around a shared set of omni-use technologies and the engineering talent ecosystems that sustain them.

9.1 Reframing Preparedness

The analysis presented throughout this report leads to a conclusion that is both uncomfortable and actionable. The Nordic-Baltic region cannot meet its future preparedness requirements through existing workforce development systems operating at their current scale, speed, and configuration. The competency demands are real, legally binding, and growing. The workforce constraints are structural and cumulative. Without deliberate intervention, the gap between preparedness requirements and available engineering capacity will widen.

Yet preparedness is no longer simply a workforce challenge. It is increasingly a challenge of how societies organise innovation, technological development, industrial capability, and talent ecosystems.

For much of the post-Cold War period, economic competitiveness and national preparedness were treated as separate policy domains. Innovation policy focused on productivity, growth, research excellence, and global competitiveness. Preparedness and defence policy focused on resilience, contingency planning, and military capability. These domains developed distinct institutions, funding mechanisms, and workforce strategies.

The emerging security environment increasingly challenges this separation. The technologies shaping future economic competitiveness are simultaneously becoming the technologies upon which societal resilience, critical infrastructure protection, and national security depend. Artificial intelligence, cybersecurity, advanced telecommunications, cloud and edge computing, autonomous systems, advanced

sensing technologies, quantum technologies, semiconductors, batteries, advanced energy systems, and space-based infrastructure now underpin economic growth, preparedness capability, and defence effectiveness.

This reality suggests that the traditional concept of dual-use technology may no longer be sufficient. Dual-use implies a transfer between civilian and military applications. Increasingly, however, the technologies most critical to preparedness operate across multiple domains at once. They create economic value, enable public services, strengthen infrastructure resilience, support crisis management, and contribute to defence capability at the same time. Emerging empirical research reaches a similar verdict from the innovation side, finding that the rigid civilian-military classification hinders technology transfer, complicates public-private partnerships, and deters investment in versatile technologies that span sectors with minimal adaptation (Singer, Mueller and Kraus, 2025). The concept of omni-use technologies, introduced earlier in this report, better captures this emerging reality.

Omni-use technologies derive their strategic importance not simply from their technical characteristics but from the ecosystems that surround them. Their value emerges through interconnected networks of firms, universities, research institutes, infrastructure operators, supply chains, regulatory frameworks, and highly specialised talent pools. Preparedness therefore becomes inseparable from the health and dynamism of broader innovation ecosystems.

This insight has profound implications for engineering workforce development. The engineers, data scientists, cybersecurity specialists, AI experts, telecommunications professionals, systems architects, infrastructure specialists, and energy engineers required to sustain economic competitiveness are increasingly the same professionals required to sustain preparedness and defence. The preparedness challenge is therefore not merely about creating new specialist roles. It is about ensuring that the broader engineering ecosystem possesses sufficient scale, diversity, adaptability, and mobilisation capacity to perform under conditions of disruption.

Preparedness can no longer be understood as a separate sector operating alongside the economy. It increasingly depends on the ability to convert civilian technological capability into resilience capability when circumstances demand it. Throughout this report, this has been described as the preparedness conversion

challenge. The central question is not whether technological capability exists, but whether it can be coordinated, mobilised, and sustained under conditions of crisis.

For the Nordic-Baltic region, this presents a significant strategic opportunity. The region already possesses internationally competitive strengths in advanced energy systems, telecommunications, digital infrastructure, maritime technologies, industrial automation, cybersecurity, defence technologies, and artificial intelligence. Investments in these areas can strengthen productivity, innovation, export competitiveness, strategic autonomy, resilience, and preparedness alike.

Omni-use technologies allow preparedness to be understood not as a cost imposed on economic development but as a source of productivity-enhancing investment. Investments in resilient energy systems strengthen both industrial competitiveness and energy security. Investments in cybersecurity strengthen both export industries and national resilience. Investments in artificial intelligence support both innovation and operational decision-making in crisis and defence environments.

Preparedness therefore becomes not only a defence policy objective but also an industrial policy, innovation policy, education policy, and workforce development objective.

9.2 Looking Ahead: Preparedness as a Competitiveness and Innovation Strategy

The Nordic-Baltic region enters this new security era with significant strengths. It benefits from comparatively high levels of institutional trust, advanced infrastructure systems, strong research capabilities, sophisticated innovation ecosystems, and internationally competitive engineering sectors. These constitute important strategic assets in an increasingly uncertain world.

Yet being well positioned is not the same as being prepared.

The central question facing the region is no longer whether critical infrastructures exist. Rather, it is whether the engineering ecosystems, talent pipelines, research capabilities, industrial capacities, and institutional arrangements required to sustain, adapt, and restore those infrastructures can be renewed, coordinated, and mobilised under conditions of prolonged disruption. Preparedness is not a

temporary mobilisation effort. It is a continuous societal capability embedded across education systems, labour markets, industrial policy, infrastructure governance, and professional formation. It depreciates if not maintained and cannot be substituted through procurement decisions or emergency measures at the moment it is most needed.

This is ultimately less a technical challenge than an institutional and political one. Systems designed for an era of relative stability must now adapt to an environment characterised by infrastructural interdependence, persistent strategic competition, cyber disruption, climate-related shocks, and growing uncertainty. The challenge is whether governance systems, workforce strategies, and coordination frameworks can evolve rapidly enough to meet these conditions. It is also a question of anticipatory governance: whether policymakers can move beyond treating competitiveness, resilience, preparedness, and defence as separate policy agendas.

The most important lesson emerging from this report is that the future of preparedness depends less on building isolated preparedness systems than on ensuring that the innovation systems, industrial capabilities, and STEM talent ecosystems that underpin them are recognised and governed as strategic preparedness assets.

For the Nordic-Baltic region, this points towards a distinctive path forward. The region has an opportunity to become an international leader in an omni-use model of innovation, in which technological development, economic competitiveness, societal resilience, preparedness, and defence capability are understood as mutually reinforcing objectives rather than competing priorities. Many of the technologies, infrastructures, and engineering capabilities that drive economic growth increasingly serve simultaneously as foundations for resilience and security.

The strategic opportunity for the coming decade is therefore not simply to strengthen preparedness institutions, but to align the broader systems that generate knowledge, technology, talent, and innovation with the demands of a more contested and disruption-prone environment. A region that succeeds in this alignment will not only enhance its preparedness capacity but also strengthen its long-term competitiveness, adaptability, and its strategic technological sovereignty.

10. Glossary of Key Terms and Abbreviations

10.1 Key Concepts

Black-Start Capability

The ability to restore an electricity grid following a complete blackout without relying on external power sources. Black-start operations depend on highly specialised engineering expertise and coordination between generation, transmission, and distribution operators.

Civil and Societal Preparedness

The capacity of society to sustain, adapt, coordinate, and restore essential functions during crises, disruptions, or prolonged periods of pressure. Civil and societal preparedness extends beyond military capability to include critical infrastructure, public institutions, businesses, and workforce systems.

Competence Ecosystem

The interconnected network of educational institutions, employers, professional associations, research organisations, and workforce development systems that collectively develop and sustain specialised expertise.

Critical Infrastructure

Assets, systems, and networks whose disruption would significantly affect societal functioning, economic activity, public safety, or national security. This includes energy systems, telecommunications, financial services, transport, water, health services, and communication and digital infrastructure.

Engineering Workforce Depth

The availability, diversity, and sustainability of engineering expertise within a given domain. Workforce depth includes both the number of professionals and the institutional capacity to reproduce and renew specialised competencies over time.

Hybrid Threats

Actions that combine military, cyber, economic, informational, technological, and political means to create disruption below the threshold of conventional warfare.

Infrastructure Interdependence

The condition in which different infrastructure systems depend on one another for their operation. Failures in one system may trigger cascading disruptions in others.

Omni-Use Engineering

A concept developed in this report describing engineering capabilities, infrastructures, technologies, and professional competencies that simultaneously support economic activity, digital transformation, societal resilience, preparedness, and security functions. Unlike traditional dual-use concepts, omni-use recognises that these functions increasingly operate through the same interconnected systems and cannot be easily separated.

Operational Integration

The ability to coordinate infrastructure systems, organisations, professional communities, and workforce capabilities effectively during periods of disruption or crisis.

Preparedness Engineering

Engineering activities and competencies focused on sustaining, protecting, restoring, and adapting critical infrastructure and societal functions under conditions of disruption, crisis, or sustained pressure.

Resilience

The capacity of systems to absorb disruption while maintaining essential functions and recovering from shocks.

System-of-Systems Modelling

The analysis of interactions and dependencies between multiple interconnected infrastructure, organisational, and technological systems to understand how failures propagate and how resilience can be strengthened.

Tacit Knowledge

Operational expertise and practical know-how acquired through experience that is difficult to codify in manuals, procedures, or formal education.

Workforce Renewal

The process through which specialist competencies are transferred, renewed, and reproduced through education, training, mentoring, and professional development.

10.2 Organisations, Frameworks and Initiatives

ANÆ

Association of Nordic Engineers.

CCDCOE

Cooperative Cyber Defence Centre of Excellence. NATO-accredited cyber defence centre located in Tallinn, Estonia.

CER Directive

Critical Entities Resilience Directive (EU 2022/2557). European Union legislation requiring critical infrastructure operators to strengthen resilience and continuity capabilities.

DIANA

Defence Innovation Accelerator for the North Atlantic. NATO initiative supporting development of emerging and dual-use technologies.

EDIS

European Defence Industrial Strategy.

ENISA

European Union Agency for Cybersecurity.

ENTSO-E

European Network of Transmission System Operators for Electricity.

NB8

Nordic-Baltic Eight. Regional cooperation format involving Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway, and Sweden.

NATO

North Atlantic Treaty Organization.

NIS2 Directive

Directive (EU) 2022/2555 concerning measures for a high common level of cybersecurity across the European Union.

NORDEFCO

Nordic Defence Cooperation. Framework for defence cooperation between Denmark, Finland, Iceland, Norway, and Sweden.

OECD

Organisation for Economic Co-operation and Development

10.3 Technical Terms**AI**

Artificial Intelligence.

GNSS

Global Navigation Satellite System. Satellite-based positioning systems such as GPS, Galileo, and GLONASS.

ICS

Industrial Control Systems. Technologies used to monitor and control industrial processes and infrastructure.

OT

Operational Technology. Hardware and software used to control physical systems such as power plants, water treatment facilities, and transport systems.

OT/ICS Security

Protection of operational technology and industrial control systems against cyber and physical threats.

PLC

Programmable Logic Controller. Industrial computer used to automate and control machinery and infrastructure processes.

SAR

Synthetic Aperture Radar. Satellite-based radar technology capable of imaging the Earth's surface regardless of weather or light conditions.

SCADA

Supervisory Control and Data Acquisition. Systems used to monitor and control critical infrastructure operations remotely.

STEM

Science, Technology, Engineering and Mathematics.

UAS

Unmanned Aircraft System.

Counter-UAS

Technologies and systems used to detect, track, disrupt, or neutralise drones and other unmanned aerial systems.

10.4 Preparedness Engineering Profiles**OT/ICS Security Engineer**

Engineer combining industrial systems expertise with cybersecurity capability.

Black-Start and Grid Restoration Specialist

Engineer responsible for restoring electricity systems following major outages.

Resilience-Capable Civil and Structural Engineer

Engineer specialising in infrastructure resilience, protection, and recovery under adverse conditions.

Crisis Logistics and Infrastructure Continuity Engineer

Engineer responsible for maintaining critical supply chains and infrastructure services during disruption.

AI-Enabled Infrastructure Systems Engineer

Engineer applying AI and machine learning to infrastructure monitoring, resilience, and operational decision support.

Quantum-Secure Communications Engineer

Engineer specialising in quantum-resistant communications and secure digital infrastructure.

11.

Bibliography

Academic literature

Boin, A. and Lodge, M. (2016) 'Designing resilient institutions for transboundary crisis management: a time for public administration', *Public Administration*, 94(2), pp. 289–298. Available at: <https://doi.org/10.1111/padm.12264>.

Comfort, L.K. (2007) 'Crisis management in hindsight: Cognition, communication, coordination, and control', *Public Administration Review*, 67(s1), pp. 189–197. Available at: <https://doi.org/10.1111/j.1540-6210.2007.00827.x>.

Farrell, H. and Newman, A.L. (2019) 'Weaponized interdependence: How global economic networks shape state coercion', *International Security*, 44(1), pp. 42–79. Available at: https://doi.org/10.1162/isec_a_00351.

Hyvönen, A.-E. and Juntunen, T. (2020) 'From "spiritual defence" to robust resilience in the Finnish comprehensive security model', in Larsson, S. and Rhinard, M. (eds.) *Nordic Societal Security: Convergence and Divergence*. London: Routledge, pp. 154–178. Available at: <https://doi.org/10.4324/9781003045533-11>.

Larsson, S. and Rhinard, M. (eds.) (2020) *Nordic Societal Security: Convergence and Divergence*. London: Routledge.

Mazzucato, M. (2021) *Mission Economy: A Moonshot Guide to Changing Capitalism*. London: Allen Lane. Available at: <https://marianamazzucato.com/books/mission-economy> (Accessed: 28 May 2026).

Perrow, Charles (1999) *Normal Accidents: Living with High-Risk Technologies*. Updated edn. Princeton, NJ: Princeton University Press. Available at: <https://press.princeton.edu/books/paperback/9780691004129/normal-accidents> (Accessed: 28 May 2026).

Singer, J.R., Mueller, E.F. and Kraus, R. (2025) 'Dual-use or omni-use? Rethinking technology in a borderless world'. SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5185227 (Accessed: September 2026).

Tierney, Kathleen. (2019) *Disasters: A Sociological Approach*. Cambridge: Polity Press. Available at: https://www.politybooks.com/bookdetail?book_slug=disasters-a-sociological-approach-9780745671017 (Accessed: 28 May 2026).

Policy reports and official documents

Association of Nordic Engineers (ANE) (2025) Reclaiming Europe's Edge: Competitiveness through STEM Talent. Copenhagen: Association of Nordic Engineers. Available at: <https://nordicengineers.org/reclaiming-europes-edge-competitiveness-through-stem-talent/> (Accessed: September 2026).

Baldoni, R. and Di Luna, G. (2025) 'Sovereignty in the digital era: The quest for continuous access to dependable technological capabilities', IEEE Security & Privacy, 23(1), pp. 91–96. Available at: <https://ieeexplore.ieee.org/document/10871167> (Accessed: September 2026).

Center for Strategic and International Studies (CSIS) (2026) How and Why Ukraine's Military Is Going Digital. Washington, DC: Center for Strategic and International Studies. Available at: <https://www.csis.org/analysis/how-and-why-ukraines-military-going-digital> (Accessed: 12 June 2026).

Christie, E.H. and Berzina, K. (2022) NATO and Societal Resilience: All Hands on Deck in an Age of War. Washington, DC: German Marshall Fund of the United States. Available at: <https://www.gmfus.org/sites/default/files/2022-07/NATO%20and%20Societal%20Resilience%20All%20Hands%20on%20Deck%20in%20an%20Age%20of%20War.pdf> (Accessed: 28 May 2026).

Clapp, Sebastian. (2024) European Defence Industrial Strategy. European Parliamentary Research Service Briefing. Brussels: European Parliament. PE 762.402 – September 2024 Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762402/EPRS_BRI\(2024\)762402_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762402/EPRS_BRI(2024)762402_EN.pdf) (Accessed: 28 May 2026).

Council on Foreign Relations (2026) Securing Ukraine's Future in Europe: Ukraine's Defense Industrial Base, An Anchor for Economic Renewal and European Security. New York: Council on Foreign Relations. Available at: <https://www.cfr.org/articles/securing-ukraines-future-in-europe-ukraines-defense-industrial-base-an-anchor-for-economic-renewal-and-european-security> (Accessed: 12 June 2026).

Crespi, F., Cerra, R. and Zezza, F. (2025) 'Coopetitive Technological Sovereignty: A Strategy to Reconcile International Collaboration with Knowledge and Economic Security', Intereconomics: Review of European Economic Policy, 60(2), pp. 73–80. Available at: <https://doi.org/10.2478/ie-2025-0016> (Accessed: September 2026).

Department of National Defence (2024) Our North, Strong and Free: A Renewed Vision for Canada's Defence. Ottawa: Government of Canada, Department of National Defence. Available at: <https://www.canada.ca/en/department-national-defence/corporate/policies-standards/our-north-strong-free-renewed-vision-canada-defence.html> (Accessed: 12 June 2026).

Dowd, A.M. and Cook, C.R. (2022) Bolstering Collective Resilience in Europe. CSIS Briefs. Washington, DC: Center for Strategic and International Studies. Available at: <https://www.csis.org/analysis/bolstering-collective-resilience-europe> (Accessed: 28 May 2026).

Draghi, M. (2024) The Future of European Competitiveness: A Competitiveness Strategy for Europe. Brussels: European Commission. Available at: https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en (Accessed: 28 May 2026).

European Commission (2024) EDIS: Our common defence industrial strategy. Directorate-General for Defence Industry and Space. Available at: https://defence-industry-space.ec.europa.eu/eu-defence-industry/edis-our-common-defence-industrial-strategy_en.

European Commission (2024) A New European Defence Industrial Strategy: Achieving EU Readiness through a Responsive and Resilient European Defence Industry. JOIN(2024) 10 final. Brussels: European Commission and High Representative of the Union for Foreign Affairs and Security Policy. Available at: https://defence-industry-space.ec.europa.eu/eu-defence-industry/edis-our-common-defence-industrial-strategy_en (Accessed: 28 May 2026).

European Commission (2026) Strengthening Europe's Tech Sovereignty. Brussels: European Commission, Directorate-General for Communications Networks, Content and Technology. Available at: <https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty> (Accessed: September 2026).

European Parliament and Council of the European Union (2022a) Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L333, pp. 80–152. Available at: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng> (Accessed: 28 May 2026).

European Parliament and Council of the European Union (2022b) Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities (CER Directive). Official Journal of the European Union, L333, pp. 164–198. Available at: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng> (Accessed: 28 May 2026).

European Union Agency for Cybersecurity (ENISA) (2024a) NIS Investments 2024 ENISA. Available at: <https://www.enisa.europa.eu/publications/nis-investments-2024> (Accessed: 28 May 2026).

European Union Agency for Cybersecurity (ENISA) (2024b) Foresight Cybersecurity Threats for 2030: Update 2024. Athens/Heraklion: ENISA. Available at: <https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024> (Accessed: 28 May 2026).

European Commission, Joint Research Centre (Jungwirth, R., Smith, H., Willkomm, E., Savolainen, J., Alonso Villota, M. et al.) (2023) Hybrid Threats: A Comprehensive Resilience Ecosystem. Luxembourg: Publications Office of the European Union. Available at: <https://doi.org/10.2760/37899> (Accessed: September 2026).

European Network of Transmission System Operators for Electricity (ENTSO-E) (2024) Winter Outlook and Security of Supply Report 2024. Brussels: ENTSO-E. Available at: <https://www.entsoe.eu/outlooks/seasonal> (Accessed: 28 May 2026).

European Network of Transmission System Operators for Electricity (ENTSO-E) Expert Panel (2026) Final Report on the Grid Incident in Spain and Portugal on 28 April 2025. Brussels: ENTSO-E. Available at: <https://www.entsoe.eu/news/2026/03/20/entso-e-publishes-expert-panel-final-report-on-28-april-2025-blackout-in-spain-and-portugal/> (Accessed: 28 May 2026).

Finnish Government (2024) Finland's Cyber Security Strategy 2024–2035. Helsinki: Prime Minister's Office. Available at: <https://julkaisut.valtioneuvosto.fi/bitstreams/e5575ec3-1ce2-4f0a-aaff-50154789cb6d/download> (Accessed: 28 May 2026).

Försvarsdepartementet (2023) Kraftsamling: Inriktningen av totalförsvaret och utformningen av det civila försvaret. Ds 2023:34. Stockholm: Försvarsdepartementet, Regeringskansliet. Available at: <https://www.regeringen.se/rattsliga-dokument/departementsserien-och-promemorior/2023/12/ds-202334-kraftsamling/> (Accessed: 28 May 2026).

Government of Denmark (2022) Danish Security and Defence towards 2035. Copenhagen: Government of Denmark. Available at: https://um.dk/media/trhdwwdl/regeringens_security-policy-report_uk_web_09-final-a.pdf (Accessed: 12 June 2026).

Government Offices of Sweden (2026) Total Defence. Stockholm: Government Offices of Sweden. Available at: <https://www.government.se/government-policy/total-defence/> (Accessed: 12 June 2026).

Hoogensen Gjørsv, G., Glebov, S. and Holshek, C. (eds.) (2025) The Eighth Baseline Requirement: Resilient Civilians in Hybrid Threats and Warfare. NATO Science for Peace and Security Series E: Human and Societal Dynamics, Vol. 158. Amsterdam: IOS Press. Available at: <https://www.iospress.com/catalog/books/the-eighth-baseline-requirement-resilient-civilians-in-hybrid-threats-and-warfare> (Accessed: 28 May 2026). ISBN 978-1-64368-612-7.

International Energy Agency (IEA) (2024) World Energy Outlook 2024. Paris: IEA. Available at: <https://www.iea.org/reports/world-energy-outlook-2024> (Accessed: 28 May 2026).

Ministry of Defence Singapore (2026) Total Defence. Singapore: Ministry of Defence. Available at: <https://www.totaldefence.gov.sg/> (Accessed: 12 June 2026).

National Preparedness Commission (2026) Connecting for Continuity in a Crisis: Joining Forces to Strengthen UK Resilience. London: National Preparedness Commission. Prepared by PricewaterhouseCoopers (PwC).

NATO (2024) Resilience, Civil Preparedness and Article 3. Brussels: North Atlantic Treaty Organization. Available at: <https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3> (Accessed: 28 May 2026).

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2024) Locked Shields 2024 Demonstrated the Real Power of Cooperative Defence. Tallinn: NATO CCDCOE. Available at: <https://ccdcocoe.org/news/2024/locked-shields-2024-demonstrated-the-real-power-of-cooperative-defence/> (Accessed: 28 May 2026).

NATO DIANA (2024) Defence Innovation Accelerator for the North Atlantic. Brussels: NATO. Available at: <https://www.nato.int/en/about-us/organization/nato-structure/defence-innovation-accelerator-for-the-north-atlantic-diana> (Accessed: 28 May 2026).

Niinistö, S. (2024) Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness. Report to the European Commission. Brussels: European Commission. Available at: https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en (Accessed: 12 June 2026).

NordForsk (2025) NordForsk Impact Report 2025. Oslo: NordForsk/Nordic Council of Ministers. Available at: <https://www.norden.org/en/publication/nordforsk-impact-report-2025> (Accessed: 28 May 2026).

Nordic Council of Ministers (2025) Stronger Together: A New Era for Nordic Security and Preparedness. Background material for Nordic Council Theme Session 2025, Helsinki, 31 March–1 April. Copenhagen: Nordic Council. Available at: https://www.norden.org/sites/default/files/2025-03/NR%20Temasession_Baggrundsmateriale_EN_Version%201.pdf (Accessed: 28 May 2026).

Nordic Council of Ministers (2026) Nordic Countries Strengthen Their Cooperation on Preparedness. Copenhagen: Nordic Council of Ministers, 16 June 2026. Available at: <https://www.norden.org/en/news/nordic-countries-strengthen-their-cooperation-preparedness> (Accessed: September 2026).

Nordic Innovation (2026) Nordic Innovation Ecosystem Mobilisation. Oslo: Nordic Innovation. Available at: <https://www.nordicinnovation.org/programs/nordic-innovation-ecosystem-mobilisation> (Accessed: 28 May 2026).

NORDEFECO (2023) NORDEFECO Annual Report 2023. Stockholm/Helsinki: Nordic Defence Cooperation. Available at: <https://www.government.se/reports/2024/06/nordefco-annual-report-2023/> (Accessed: 28 May 2026).

Nordic Prime Ministers and Heads of Government (2025) Joint Statement on Cooperation for Enhanced Crisis Preparedness and Resilience: The Nordics, United and Strong. Helsinki: Finnish Government.

Norwegian Ministry of Defence (2024) The Norwegian Defence Pledge: Long-Term Defence Plan 2025–2036. Oslo: Norwegian Ministry of Defence. Available at: <https://www.regjeringen.no/en/dokumenter/the-norwegian-defence-pledge/id3032809/> (Accessed: 28 May 2026).

OECD (2024) Education at a Glance 2024: OECD Indicators. Paris: OECD Publishing. <https://doi.org/10.1787/c00cad36-en> (Accessed: September 2026).

Royal Academy of Engineering (2020) Critical capabilities: strengthening UK resilience. London: Royal Academy of Engineering. Available at: <https://raeng.org.uk/media/bm2e4chu/critical-capabilities-sp.pdf> (Accessed: 12 June 2026).

Royal Academy of Engineering (2022) Building Resilience: Reimagining Risk Assessment for a More Resilient Future. London: Royal Academy of Engineering. Available at: <https://raeng.org.uk/media/g31bttwt/raeng-building-resilience.pdf> (Accessed: 12 June 2026).

SFS (2018) Säkerhetsskyddslag (2018:585). Stockholm: Justitiedepartementet. Available at: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddslag-2018585_sfs-2018-585/ (Accessed: 12 June 2026).

Slätmo, E., Berlina, A., Bogason, Á., Halldórsdóttir, T.K., Itänen, M., Tomren, L. and Kačkus Tybjerg, J. (2024) Stabil civil beredskap i Norden: En studie av hur nordisk regionalpolitik kan bidra till civil beredskap. Policy Brief 2024:8. Stockholm: Nordregio. Available at: <https://pub.nordregio.org/pb-2024-8-stabil-civil-beredskap-i-norden/> (Accessed: September 2026).

Sveriges Ingenjörer (2025) Doktorandkrisen: Antalet svenska doktorander minskar kraftigt. Stockholm: Sveriges Ingenjörer, p. 3. Available at: <https://www.sverigesingenjorer.se/globalassets/25-03-doktorandkrisen-ett-hot-mot-svenskt-valstand.pdf> (Accessed: 12 June 2026).

Tanner, B., Kerry, C.F., Wyckoff, A.W., Kyosovska, N., Renda, A. and Tabassi, E. (2026) Is AI sovereignty possible? Balancing autonomy and interdependence. Washington, DC: Brookings Institution and Centre for European Policy Studies (CEPS). Available at: <https://www.brookings.edu/articles/is-ai-sovereignty-possible-balancing-autonomy-and-interdependence/> (Accessed: September 2026).

Tonurist Iret, Hanon Angela (2020) Anticipatory Innovation Governance Shaping the future through proactive policy making. OECD Working Papers on Public Governance No. 44. Available at: https://www.oecd.org/en/publications/anticipatory-innovation-governance_cce14d80-en.html.

Helsinki Commission (2024) Towards a total Defence of Europe- from Apathy to Action? Available at: <https://helsinkisecurityforum.fi/publications/> (Accessed 2 september 2026).

WindEurope (2023) Wind Energy in Europe: 2023 Statistics and the Outlook for 2024–2030. Brussels: WindEurope. Available at: <https://windeurope.org/intelligence-platform/product/wind-energy-in-europe-2023-statistics-and-the-outlook-for-2024-2030/> (Accessed: 28 May 2026).

WindEurope (2025) Europe's Wind Energy Workforce Report. Brussels: WindEurope. Available at: <https://windeurope.org/data/products/europes-wind-energy-workforce-report> (Accessed 2 September).

World Economic Forum (2024) Global Gender Gap Report 2024. Geneva: World Economic Forum. Available at: <https://www.weforum.org/publications/global-gender-gap-report-2024/> (Accessed: 28 May 2026).

Research institutions, universities and technical organisations

Aalborg University (2024) MSc in Cyber Security: Programme Description. Aalborg: Aalborg University. Available at: <https://www.aau.dk/uddannelser/kandidat/cyber-security> (Accessed: 28 May 2026).

Aalto University (2024) Secure Systems: Master's Programme in Automation and Electrical Engineering, curriculum 2024–2026. Espoo: Aalto University. Available at: <https://www.aalto.fi/en/programmes/masters-programme-in-automation-and-electrical-engineering/curriculum-2024-2026> (Accessed: 28 May 2026).

Fingrid (2023) Annual Review 2023. Helsinki: Fingrid Oyj. Available at: <https://www.fingrid.fi/en/investors/financial-reports-and-presentations/> (Accessed: 28 May 2026).

Finnish National Emergency Supply Agency (NESA) (2025) The National Emergency Supply Agency. Helsinki: NESA. Available at: <https://www.huoltovarmuuskus.fi/en/organisation/the-national-emergency-supply-agency> (Accessed: 28 May 2026).

ISC2 (2024) ISC2 Cybersecurity Workforce Study 2024. Alexandria, VA: ISC2. Available at: <https://www.isc2.org/research> (Accessed: 28 May 2026).

REWIRE Project (2025) Cybersecurity Skills Alliance: Workforce Gap Analysis. Brussels: REWIRE Consortium. Available at: <https://akmi-international.com/projects/rewire/> (Accessed 2 September 2026).

Wallenberg Centre for Quantum Technology (WACQT) (2024) WACQT: Wallenberg Centre for Quantum Technology. Gothenburg: Chalmers University of Technology. Available at: <https://www.chalmers.se/en/centres/wacqt/> (Accessed: 28 May 2026).

Corporate and industry sources

55 North (2025) 55 North Quantum Fund. Copenhagen: 55 North. Available at: <https://www.55n.vc/> (Accessed: 28 May 2026).

EIFO (2025) Danmark lancerer verdens største kvantefond. Copenhagen: Export and Investment Fund of Denmark. Available at: <https://eifo.dk/en/> (Accessed: 28 May 2026).

Ericsson (2026a) Ericsson Announces Proposed Headcount Reduction in Sweden. Stockholm: Ericsson. Available at: <https://www.ericsson.com/sv/press-releases/2026/1/ericsson-announces-proposed-headcount-reduction-in-sweden> (Accessed: 28 May 2026).

Ericsson (2026b) Full Year and Fourth Quarter Report 2025. Stockholm: Telefonaktiebolaget LM Ericsson. Available at: <https://www.ericsson.com/en/investors/financial-reports> (Accessed: 28 May 2026).

Equinor (2024) Hywind Tampen. Stavanger: Equinor. Available at: <https://www.equinor.com/energy/hywind-tampen> (Accessed: 28 May 2026).

Grid Dynamics (2025) IT Talent Shortage in the Nordics. San Ramon, CA: Grid Dynamics. Available at: <https://www.griddynamics.com/blog/nordics-tech-talent-shortage> (Accessed: 28 May 2026).

ICEYE (2024) Synthetic Aperture Radar Satellite Operations. Espoo: ICEYE. Available at: <https://www.iceye.com/> (Accessed: 28 May 2026).

Kongsberg Satellite Services (KSAT) (2024) Annual Report 2024. Tromsø: KSAT. Available at: <https://www.ksat.no/> (Accessed: 28 May 2026).

Milrem Robotics (2024) About Us. Tallinn: Milrem Robotics. Available at: <https://milremrobotics.com/company/> (Accessed: 28 May 2026).

Net Group (2026) Cybersecurity Skill Shortage. Tallinn: Net Group. Available at: <https://netgroup.com/blog/cybersecurity-skill-shortage/> (Accessed: 28 May 2026).

Nokia (2025) Annual Report 2024. Espoo: Nokia Corporation. Available at: <https://www.nokia.com/about-us/investors/results-reports/> (Accessed: 28 May 2026).

Novo Holdings (2025) Novo Holdings Acts as Cornerstone Investor in 55 North, the World's Largest Dedicated Quantum Fund. Copenhagen: Novo Holdings, 2 October. Available at: <https://novoholdings.dk/> (Accessed: 28 May 2026).

OHB Sweden (2024) Space Systems Capability Overview. Stockholm: OHB Sweden. Available at: <https://www.ohb-sweden.se/> (Accessed: 28 May 2026).

Patria Group (2024) Annual Report 2024. Helsinki: Patria Group. Available at: <https://www.patriagroup.com/> (Accessed: 28 May 2026).

Saab AB (2024) Annual Report 2024. Linköping: Saab AB. Available at: <https://www.saab.com/investors/reports-and-presentations> (Accessed: 28 May 2026).

Saab (2025) 'From concept to impact: Saab and the Swedish Air Force deploy "Loke"', Saab Newsroom, March. Available at: <https://www.saab.com/newsroom/stories/2025/march/from-concept-to-impact-saab-and-the-swedish-air-force-deploy-loke> (Accessed: 28 May 2026).

Saab (2026) 'Saab receives order for counter-unmanned aerial system from Sweden', Saab Newsroom, 2 April. Available at: <https://www.saab.com/newsroom/press-releases/2026/saab-receives-order-for-counter-unmanned-aerial-system-from-sweden> (Accessed: 28 May 2026).

Scalers (2023) Solving Scandinavia's Talent Gap. Available at: <https://thescalers.com/the-scandinavian-it-dilemma/> (Accessed 2 September 2026).

SINTEF (2024) Annual Report 2024. Trondheim: SINTEF. Available at: <https://www.sintef.no/en/sintef-group/annual-reports-and-brochures/integrated-annual-report-2024/> (Accessed: 28 May 2026).

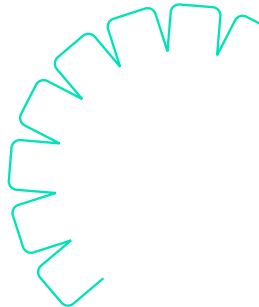
Other web sources

Adamson, E. and Ålander, M. (2026) 'Nordic-Baltic Total Defence: Easier Said Than Done', Heinrich Böll Stiftung, 13 January. Available at: <https://www.boell.de/en/2026/01/13/nordic-baltic-total-defence-easier-said-done> (Accessed: 28 May 2026).

CloudZero (2023) The Leading Countries Breaking Barriers for Women in STEM. Available at: <https://www.cloudzero.com/blog/women-in-stem/> (Accessed: 28 May 2026).

Kremidas-Courtney, C. (2026) 'From dual-use to omni-use: securing Europe's future', European Policy Centre Commentary, 1 October. Available at: <https://www.epc.eu/publication/from-dual-use-to-omni-use-securing-europes-future/> (Accessed: 28 May 2026).

Nordic Prime Ministers and Heads of Government (2025) Joint Statement on Cooperation for Enhanced Crisis Preparedness and Resilience: The Nordics, United and Strong. Helsinki: Finnish Government. Available at: <https://valtioneuvosto.fi/en/-/joint-statement-by-the-nordic-prime-ministers-and-heads-of-government-on-cooperation-for-enhanced-crisis-preparedness-and-resilience-the-nordics-united-and-strong> (Accessed: 28 May 2026).



The Association of Nordic Engineers, ANE, consists of engineering trade union associations from the Nordic countries:

The Swedish Association of Graduate Engineers (Sveriges Ingenjörer)

The Danish Society of Engineers (IDA)

The Norwegian Society of Engineers and Technologists (NITO)

The Association of Chartered Engineers in Iceland (VFÍ)

Engineers Finland representing the Finnish organisations:

the Academic Engineers and Architects in Finland (TEK), the Technical Association in Finland (TFiF), the Union of Professional Engineers in Finland (ILRY) and the Engineers in Finland (DIFF)



[Association of Nordic Engineers](#)



nordicengineers@ida.dk