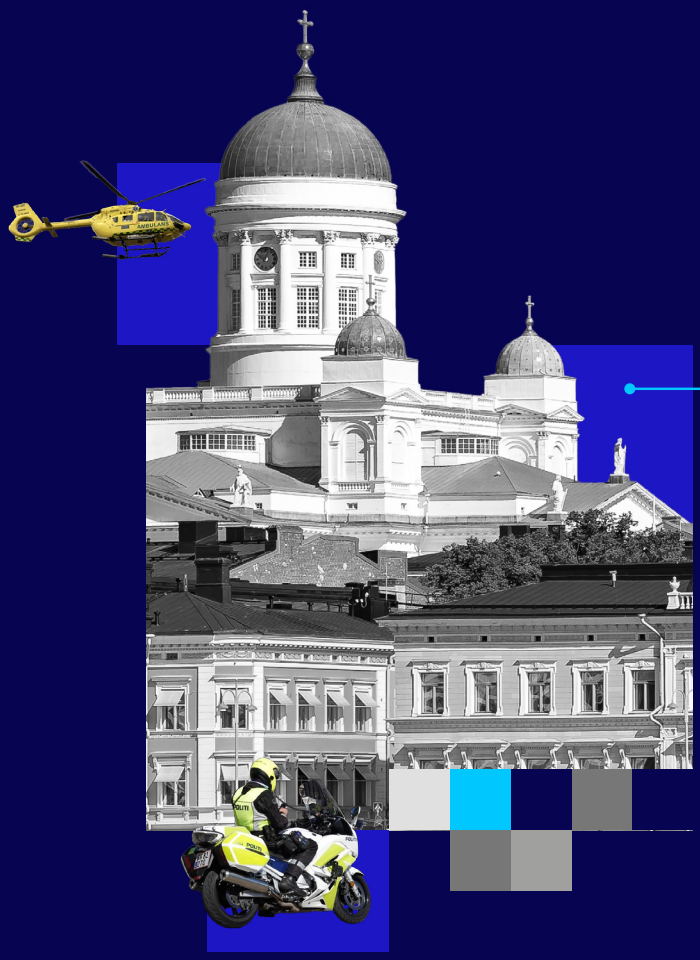
Building preparedness

Nordic Digital Security 2026

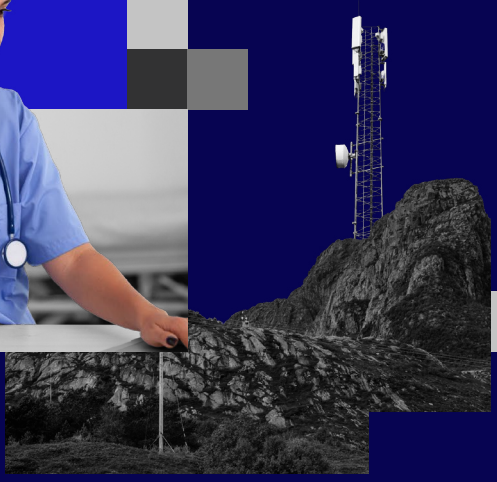














part of telenor DNA









Telenor Building preparedness

Building preparedness

When connectivity fails, the consequences can spread quickly. Businesses can lose access to critical systems, public services can be disrupted, and people may be left without vital information or the means to get help. Cyberattacks, sabotage, and severe weather make preparedness a shared concern for governments and businesses alike.

Last year, we called for closer Nordic cooperation on resilience. This year's report examines what that means in practice for businesses and public authorities. Which operations must continue during a serious disruption? What do they depend on? And have the plans to keep them running been tested with the people and suppliers involved?

Our survey across Denmark, Finland, Norway, and Sweden underlines the urgency. Only around half of respondents say their organisation is well prepared to maintain critical operations during a serious digital disruption. That is a finding we should take seriously. Organisations need to understand their dependencies, address weaknesses, and test whether their plans will work in a crisis.

For Telenor, preparedness starts with our responsibility to keep people and businesses connected. It also means working with customers, suppliers, and authorities to understand our shared dependencies and where disruption could have the greatest impact. This report offers practical guidance to help organisations identify weaknesses and strengthen their ability to maintain and restore critical operations.

Preparing together requires cooperation and clear agreements between governments, operators, and other essential service providers. Together, we must decide which services need to be maintained, at what minimum level, and how scarce resources will be shared. We must also agree who is responsible for exceptional preparedness measures and how they will be funded. Nordic cooperation should make it easier to share expertise and support one another across borders when needed.

Preparedness must also include communications. During a crisis, people need reliable information about what is happening and what they should do. We must be ready to communicate clearly even when facts are incomplete, false information spreads, or normal channels are unavailable.

The Nordics have strong institutions and a long tradition of trust and cooperation to build on. But resilience cannot rest on trust and good intentions alone. It requires joint exercises, a shared understanding of critical dependencies, and practical agreements for mutual assistance across borders. Above all, it means identifying and fixing the weaknesses before a crisis exposes them.

The time to prepare together is now.

Birgitte Engebretsen
CEO of Telenor Norway

Jonas Edén
CEO of Telenor Sweden

Jussi Tolvanen
CEO of DNA, Finland

Lars Thomsen
CEO of Telenor Denmark

Executive summary

Security is climbing the Nordic agenda, but readiness is lagging behind. A short overview of the threats, the survey findings and Telenor's recommendations for businesses and authorities.

→ Pp. 06 — 07

The Nordic threat picture

From state-backed espionage and sabotage to AI-enabled fraud and supply-chain risk, we map the actors and developments shaping the threats to Nordic businesses.

→ Pp. 08 — 14

How they attack

Most attacks still begin with a stolen login, an exposed service, or a deceived employee. What has changed is how quickly AI and ready-made attack services can exploit them.

→ Pp. 15 — 21

The Nordic resilience gap

Our survey of 2,427 Nordic business leaders shows security rising up the agenda, yet only half feel ready to keep critical operations running through a serious disruption.

→ Pp. 22 — 25

From backup to tested continuity

Backup power and spare routes are only the start. Telecom resilience is a system of layers that must be tested together before a crisis hits.

→ Pp. 26 — 27

Digital sovereignty gets real

Who controls the technology we depend on? How the Nordics can turn digital dependence into resilience through deliberate choices rather than self-sufficiency.

→ Pp. 28 — 35



Who's keeping your AI in check?

Telenor's Lead for Responsible AI, Zainab Hussain Siddiqui, shares six practical steps for building responsibility into how AI is developed, bought and used.

→ Pp. 36 — 41

Resilience has a cost

Continuity doesn't happen by accident. Play your way to tested continuity and see how investment, procurement, and clear ownership decide who climbs and who slides back.

→ Pp. 42 — 43

When trust becomes the target

When a network goes down, a second crisis starts online. Experts from Norwegian Defence Research Establishment (FFI) and Finland's Security Committee explain why trust has to be built before it's needed.

→ Pp. 44 — 49

Resilience checklist

A practical self-assessment to help businesses and public authorities find their most critical continuity gaps and decide what to fix first.

→ Pp. 50 — 53

What authorities should prepare for

Five priorities for Nordic governments, from clear resilience targets and funding to joint exercises across borders and trusted crisis communication.

→ Pp. 54 — 63

A note on the use of AI

This report was produced through a combination of human expertise and AI-assisted editorial work. The ideas, opinions, knowledge and analysis presented throughout the report originate from human sources, including interviews, research, survey data and subject-matter expertise. AI tools supported the editorial process for tasks such as structuring and outlining content, editing language and reducing text for clarity and length. All content has been reviewed and shaped by human editors, who retain responsibility for the final publication.

CHAPTER 1

Priority is running ahead of preparedness

Executive summary

50%

of Nordic organisations feel well prepared to keep critical operations running through a serious digital disruption.

Finland 56% · Norway 49% · Denmark 49% · Sweden 47%

Security and resilience are moving up the agenda across the Nordics. But our survey of 2,427 business leaders and decision-makers shows that recognising the risks is not the same as being ready for disruption. This year's report argues for practical resilience. That means knowing which services must keep running and what they depend on, and proving that backup arrangements work before they are needed.

Priority

71% see digital sovereignty growing in importance

58% put greater weight on security when buying

Preparedness

50% feel ready for serious disruption

36% expect higher security and resilience investment

12% feel fully prepared for AI-enabled threats

Recognising the need for resilience is one thing.

Building it is another.

Why it matters to decision-makers

Nordic security assessments highlight the growing risks associated with Russian hybrid activity, while cybercrime, power disruptions, and extreme weather also underline the need for stronger operational resilience. Service disruption is the threat Nordic leaders cite most (39%), and security is now shaping what they buy. Yet only around a third expect to invest more.

Telenor's call to action

- Resilience must be tested, not assumed. Backups only matter if they work under pressure, across power, networks, people, and suppliers.
- Sovereignty means control, not self-sufficiency. The aim is deliberate choices and fewer unacceptable dependencies, not building everything at home.
- Trust is built before the crisis. A serious disruption tests systems and trust at the same time, and the relationships needed to respond must already exist.

What Telenor asks of Nordic governments

Digital resilience cannot be built by asking each organisation to prepare in isolation. Telenor calls on Nordic governments and public authorities to:

1. Set clear resilience outcomes and fund what is required. Define essential functions, minimum service levels, and restoration priorities, and agree in advance who pays for exceptional preparedness.
2. Build trusted infrastructure while preserving openness and competition. Address unacceptable dependencies while preserving competition and access to trusted partners.
3. Coordinate preparedness across sectors and borders. Involve critical operators in crisis planning and enable cross-border backup and recovery.
4. Exercise together and close the gaps. Give every significant weakness an owner, funding, and a deadline, then test the correction.
5. Treat trusted communication as an operational capability. Agree and test how people will get timely crisis information, including when normal channels fail.

CHAPTER 2

The Nordic threat picture 2026

Telenor's presence across Denmark, Sweden, Finland, and Norway gives us a broad perspective on the Nordic threat landscape. Drawing on insights from our security experts and national authorities, this article looks at the threats facing Nordic businesses and the particular importance of telecommunications. From espionage and destructive cyberattacks to cybercrime, AI-enabled fraud, and supply-chain vulnerabilities, it examines the actors and developments shaping today's risks, and how the consequences can spread across organisations and essential services.

2 The Nordic threat picture

Telecommunications and the customers who depend on us

Telecommunications support everyday business and essential services, from payments and healthcare to emergency response. An attack on a network can therefore affect organisations far beyond the operator itself. For Telenor, understanding the threats to our networks also means understanding how they could affect our customers and the services we provide.

Our networks are valuable both as infrastructure and as a source of information. A business may attract attention because of the data it holds, the customers it serves, or its role in a critical supply chain. We need to consider these connections when assessing our own exposure and that of our customers.

This requires us to connect individual incidents with the wider security picture. It also means distinguishing deliberate attacks from accidents and technical failures, as well as being clear about what the evidence tells us and where uncertainty remains.

The wider Nordic security picture

Russia's war against Ukraine continues to shape security across the region. Norway's Police Security Service (PST) expects increased Russian intelligence activity in 2026, including interest in military activity, support for Ukraine, and the High North. It identifies property and logistics infrastructure associated with support for Ukraine as the most likely targets of potential Russian sabotage, while warning that other civilian infrastructure may also be affected.[1]

The intended effects extend beyond the immediate damage. PST describes sabotage as a means of creating unrest and weakening the ability and willingness to support Ukraine. It also notes that sabotage and disruptive activity in Europe have often been carried out through intermediaries acting on behalf of others. For businesses, this means that their role in supplying goods, transport, or essential services can be relevant to their exposure to state threats.

Sweden's Security Service (Säpo) describes a Russia more willing to take risks and more offensive in its covert influence activities. It warns of sabotage intended to obstruct Western support for Ukraine and reports having observed Russian attempts at cyber sabotage.[2]

In June 2026, Denmark's Agency for Societal Security (SAMSIK) sharpened its warning about destructive cyber-

Photo: Norwegian Ministry of Defence



↳ Telenor's Nordic threat picture builds on the Nordic security services' assessments for 2026.

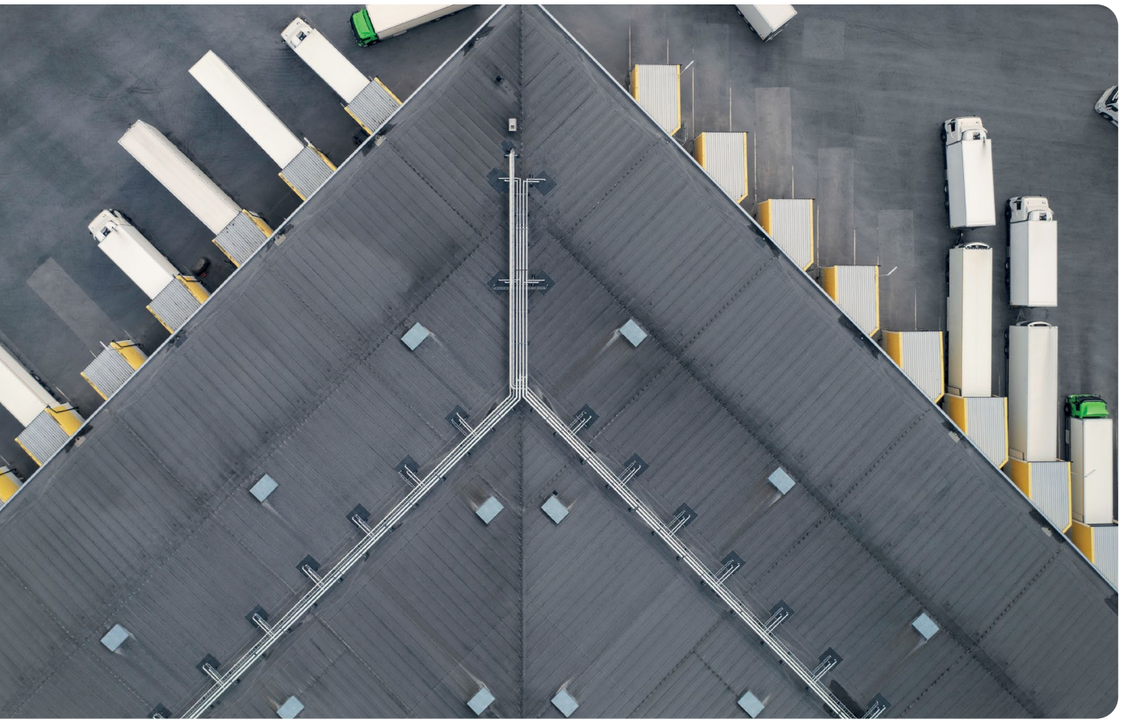


Photo: Telenor/Getty Images

attacks by Russian state hackers, highlighting the potential for more extensive harm to important societal functions. It stressed these actors' capacity to carry out coordinated, targeted attacks against critical infrastructure. The overall threat level for destructive cyberattacks remained medium.[3]

Finland's Security and Intelligence Service (Supo) assesses that an end to the fighting in Ukraine would not remove Russia's ambitions for great power status or its confrontational stance towards the West.[4] For businesses, the implication is that state threats are likely to remain a long-term security concern even if the fighting in Ukraine ends.

Military escalation cannot be ruled out while the war in Ukraine continues. In a September 2026 assessment, the Danish Defence Intelligence Service (FE) judged the risk of a limited Russian military attack against one or more NATO countries bordering Russia to be low but growing. Such an attack could seek to divide NATO over its collective response. The service nevertheless regarded an outright invasion as highly unlikely.[5]

↳ PST sees logistics infrastructure linked to support for Ukraine as the most likely target of potential Russian sabotage.

In this broader security environment, Nordic businesses face a mix of state, criminal, and supply-chain threats that can affect information, services, and trust. Taken together, national assessments indicate that Russia poses the most immediate and wide-ranging state threat across the region. Chinese intelligence activity remains a significant long-term concern, including cyber espionage and efforts to acquire technology and information about digital infrastructure.

Intelligence threats to networks and information

Access to customer data or network information can support intelligence gathering. Metadata, such as when and where communications take place, can be valuable even without access to the content of those communications. States can also use recruitment and physical reconnaissance, sometimes relying on intermediaries who obscure who is responsible.

Norwegian PST identifies cyber operations as the principal channel for the Chinese intelligence threat to Norway. Its 2026 assessment reports that Chinese cyber threat actor Salt Typhoon compromised vulnerable network devices in Norwegian organisations. It also notes that US authorities describe the actor as specialising in operations against telecommunications infrastructure.

These threats can take several forms. An attacker may remain inside a network to collect information over time, or establish access for a later operation, including disruption. An intrusion can therefore be harmful even when services continue to work normally. Discovering unauthorised access does not, by itself, establish that sabotage was the objective.

Information and access that need protection

1. Customer data and communications metadata that could support intelligence gathering.
2. Information about network vulnerabilities and how critical systems can be accessed.
3. Staff accounts and access rights that could be misused or obtained through deception.
4. Details of critical suppliers and the services on which operations depend.

Cybercrime and AI broaden business exposure

Financially motivated cybercrime remains a threat to Nordic businesses. Criminals seek opportunities to steal money, obtain valuable information, and extort organisations. The consequences can include interrupted operations, exposure of confidential information, and damage to customer relationships. Extortion does not always involve encrypting systems. Even after a business restores its operations from backups, criminals can still threaten to publish or misuse stolen information.

In its Threat Landscape 2025 report, the European Union Agency for Cybersecurity (ENISA) describes a professionalised criminal

ecosystem in which access brokers and ransomware services lower the barriers to entry. Businesses can therefore face attackers drawing on capabilities and access purchased from others.[6]

Advances in AI may further increase the scale and speed of these threats. AI can make impersonation more convincing and help attackers identify and exploit vulnerabilities, although current assessments generally indicate that it enhances existing methods rather than creating entirely new categories of attack. The UK's National Cyber Security Centre assesses that AI will make elements of cyber intrusion more efficient and effective, while reducing the time available to address vulnerabilities before they are exploited.[7] At the same time, AI also offers opportunities to strengthen defence.

Security depends on the supply chain

An organisation can be affected without being the intended target. A compromised software component or service provider can expose several customers. For Telenor and other businesses, assessing security therefore means looking beyond our own systems to the suppliers and subcontractors we depend on.

For each critical supplier, businesses should identify what information and systems the supplier can access, which services rely on the supplier, and how those services would continue if the supplier became unavailable. Dependencies may extend beyond direct suppliers to subcontractors and technology providers further down the chain.

Disruption can spread across services and undermine trust

Telecommunications depend on other services, including power and transport. A failure in one sector can interrupt operations in another, and those dependencies may extend across Nordic borders. Disruption to the systems controlling physical processes, such as energy or water supply, can also affect businesses that have not themselves been attacked.

Subsea cables illustrate the importance of infrastructure and the need for care in interpreting incidents. Supo's 2026 overview notes that cable damage in the Baltic Sea has occurred for decades. Repeated damage alone does not establish deliberate action or state involvement; each incident requires careful investigation.[8] We need to prepare for sabotage while retaining the ability to manage accidents and technical failures.

Disruption can also create an opportunity to spread misleading accounts of what has happened. Uncertainty about the cause, extent, or likely duration of an incident can be exploited to weaken confidence in a business or the authorities. Accurate, timely communication is therefore part of the response.



Photo: The Finnish Border Guard

↳ Each incident at sea requires careful investigation before conclusions are drawn.

Understanding exposure and sharing observations

Threat assessments should help businesses identify which actors may have an interest in them, what could be targeted, and where disruption would have the greatest consequences. Norway's National Security Authority highlights persistent weaknesses in preventive security and contingency planning, and calls for security management that brings digital, physical, and personnel security together.[9]

For businesses, this starts with knowing what normal activity looks like and making it easy for staff to report unusual events. Personnel security should address deliberate misuse, attempts to pressure or recruit staff, and the risk of people being deceived.

Businesses should share relevant observations with the appropriate authorities, as an incident that appears isolated may be part of a wider operation. Sharing this information can help establish what has happened and whether other organisations are at risk.

Warning signs worth examining

1. Unexpected requests for access to systems or sensitive information.
2. Unusual interest in a site, its infrastructure, or the people working there.
3. Unexplained system behaviour or activity outside normal patterns.
4. Attempts to pressure, recruit, or deceive employees.

Make sure staff know how to report a concern so it can be assessed.



Photo: Telenor

↳ Telenor's Security Operations Centre monitors and responds to threats around the clock.

1. Norwegian Police Security Service (PST) (2026). National Threat Assessment 2026, 6 February 2026.
2. Krisinformation.se (2026). The security situation in Sweden, updated 30 March 2026.
3. Danish Agency for Societal Security (2026). Heightened threat from destructive cyberattacks, 30 June 2026.
4. Finnish Security and Intelligence Service (Supo) (2026). The end of the war will not change the character of Russia, National Security Overview 2026.
5. Danish Defence Intelligence Service (2026). Assessment of the threat from Russia, 24 September 2026, pp. 2–3.
6. European Union Agency for Cybersecurity (ENISA) (2025). ENISA Threat Landscape 2025, October 2025, version 1.2, January 2026.
7. UK National Cyber Security Centre (NCSC) (2025). Impact of AI on cyber threat from now to 2027, 7 May 2025.
8. Finnish Security and Intelligence Service (Supo) (2026). Growing tensions in the Baltic Sea, National Security Overview 2026.
9. Norwegian National Security Authority (NSM) (2026). Risk 2026, 6 February 2026.

CHAPTER 3

How they attack: familiar routes, faster attacks

Cyberattacks in 2026 are not suddenly following an entirely new playbook. Most still start with familiar routes: a stolen account, an exposed service, a vulnerable supplier, or a person persuaded to do something that appears legitimate. What is changing is how quickly and at what scale those routes can be exploited. Attack services are easier to buy, software dependencies give attackers access to multiple organisations at once, and AI enables parts of an attack to be carried out faster than before.

The easiest route still wins

The wider threat picture tells us who may target Nordic organisations and why. This article focuses on something more practical: how attackers actually get in.

Attackers are usually pragmatic. If a stolen password, an exposed management interface, or a convincing email gives them access, there is little reason to start with a technically spectacular exploit. Even sophisticated threat actors may use simple methods to gain access.

Identity is one of the most attractive entry points. According to Telenor Cyberdefence's report for the second quarter of 2026, many serious incidents were linked to compromised user accounts.[1] Once an attacker can log in with a legitimate account, they may be able to bypass controls that are designed to detect a conventional break-in.

The same access can also be used for very different purposes. A compromised account may lead to fraud, data theft, extortion, espionage, or disruption. It can also be sold to someone else. The criminal group that gains the initial access is not necessarily the one that ultimately uses the access.

Access has become a service

Cybercrime has increasingly become a service economy. Attackers can buy phishing infrastructure, stolen credentials, malware, compromised accounts, and access to systems rather than building everything themselves. Specialist "initial access brokers" focus on obtaining access to organisations and selling it to other criminals. Gaining access and exploiting it have become separate activities within the cybercrime economy. Phishing-as-a-service packages can provide the pages, hosting, automation, and support needed to run a campaign.

This changes who can carry out an attack. An attacker does not need to master every stage of an intrusion. Different parts of the attack chain can be bought, automated, and combined. In practice, this often means the same attack methods can be used faster and against many more targets.

Software supply chains: one compromise, many victims

Software supply-chain attacks are not new. What has changed is the size and complexity of the dependency chain around modern software development. A single application may depend on many external libraries, packages, extensions, and build tools, each of which can introduce another route into the development process. Dependencies may themselves have dependencies, meaning an organisation can be several steps removed from the component that is compromised.

The risk is not limited to someone deliberately placing malicious code in an open-source package. Attackers can compromise a software developer account, hijack a release process, abuse build credentials, poison a dependency, or target the tools developers use every day. If they succeed upstream, the malicious component can then travel through normal development and deployment processes into organisations that were never individually targeted.

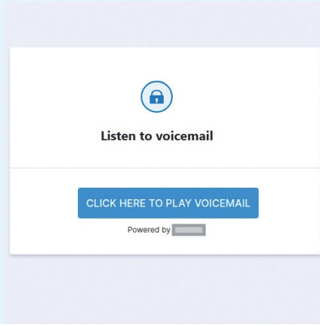
A 2026 campaign, known as "Mini Shai-Hulud", compromised widely used open-source software packages, allowing malicious code to spread through the software-development supply chain. Akamai reported that attackers hijacked a legitimate release workflow and used it to publish malicious package versions.[6] Google Threat Intelligence has also highlighted how attackers are increasingly targeting the intersection between open-source software, development pipelines, and AI-assisted coding.[7]

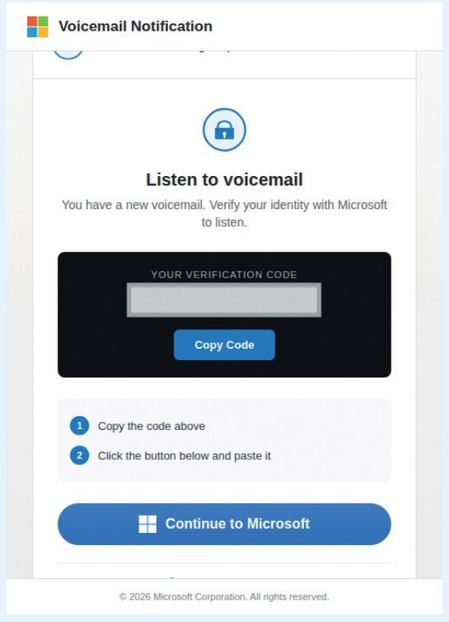
Device code phishing: a familiar weakness at a new scale

Device code authentication is a legitimate login method designed for devices or applications where entering a password directly is inconvenient: the user is given a short code and completes the login on another device. In a device code phishing attack, the attacker abuses this process by tricking the victim into authorising a login session that the attacker has already started. The victim may even complete the process on Microsoft's genuine login page, which makes the interaction look more convincing.

In 2026, Telenor has seen a marked increase in this type of attack in Norway,[2] while national cybersecurity authorities in Finland[3] and Sweden[4] have also warned about the technique and reported active campaigns using it. Microsoft has separately described a widespread campaign that combined dynamic device-code generation, automation, and AI-generated lures to compromise organisational accounts at scale.[5] The important shift is the industrialisation of the method: steps that once required an attacker to interact with a victim in real time can increasingly be handled automatically.

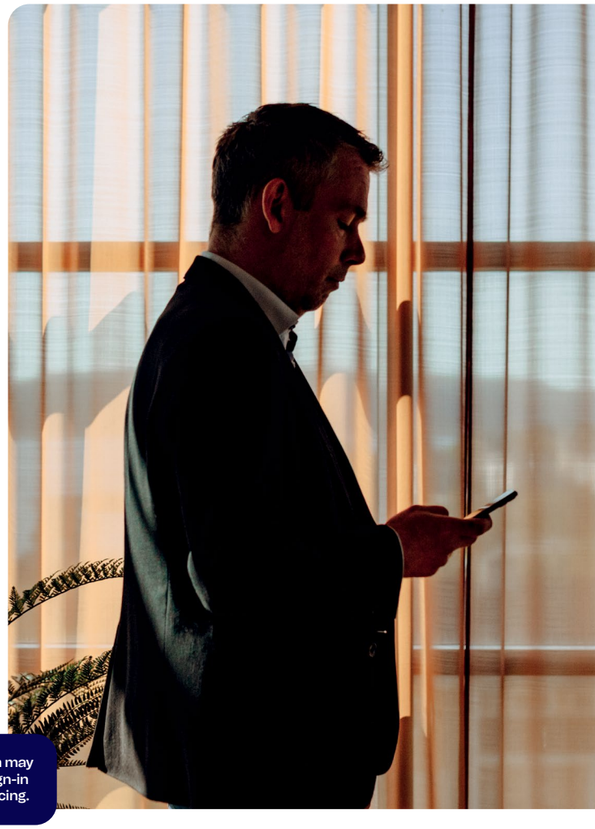
Once an account is compromised, the attacker may be able to read email, search documents, map colleagues and suppliers, create inbox rules, or use the trusted account to approach the next victim. This is why a small mistake can become the starting point for a much wider attack.





In device code phishing, the victim may complete the login on a genuine sign-in page. That is what makes it convincing.

Photo: Telenor



Open source is not inherently unsafe. The risk comes from the number of components and dependencies involved, and from the need to manage trust across the whole development chain. Organisations need to know what enters the development environment, protect developer accounts and build credentials, control how dependencies are introduced, and monitor the build and release process.

When an attack comes after hours

Partner perspective - WithSecure, DNA's partner in Finland

WithSecure, a Finnish cybersecurity company and DNA's partner in Finland, helps businesses prevent, detect, and respond to attacks. Drawing on its work across the Nordics, WithSecure describes an incident at a Danish company that illustrates why defences need to work outside normal business hours.

The Danish business had installed software to detect suspicious activity on its computers, monitored by a service partner and backed by an automated response. When a targeted attack struck in the middle of the night, no one from the internal IT team was watching a screen. WithSecure says the automated response stopped the attack before it could escalate. Its incident response specialists were then available afterwards to investigate and advise.

For WithSecure, the case illustrates the value of having a response ready before it is needed. Its wider advice is to address the weaknesses attackers can exploit, while ensuring detection and response remain effective when staff are unavailable.

AI changes the speed of the attack

AI is now part of real-world cyber operations, but its immediate effect is more practical than science fiction. Threat actors are using it to make existing activities faster and more efficient: reconnaissance, social engineering, vulnerability research, exploit development, malware development, and analysis of stolen information.

The most important change is speed. In September 2026, Google Threat Intelligence Group reported a case in which a threat actor compromised cloud infrastructure and then planned, built, and ran an agent-enabled mass credential-harvesting campaign in less than six hours.[8] The AI system helped manage scanning, troubleshoot problems, and switch between the IP addresses used to send attack traffic, requiring far less human intervention than a conventional operation. Agentic systems can also make an attack more adaptive, changing tactics when something fails and responding dynamically to the environment they encounter rather than simply following a predefined sequence.

Fully autonomous attacks are still unusual, and skilled people remain involved in advanced operations. But more of the repetitive work can now be handed over to machines.

For defenders, this matters because the window to react is getting shorter. If AI helps attackers move more quickly from disclosure of a vulnerability to actively exploiting it, organisations have less time to identify affected systems, test a fix, and deploy it. The same applies after an account is compromised: automated scanning and exploration of compromised systems can turn access into a wider incident very quickly. Defenders therefore also need to automate more of the detection and response cycle, so that vulnerability management, monitoring, and containment can keep pace with attacks that increasingly operate at machine speed.

People are still part of the attack chain

Social engineering remains effective because many security processes still depend on a person approving, resetting, installing, or paying something. A convincing email, a call from someone claiming to be the helpdesk, or a request from a compromised supplier account can all create the moment an attacker needs.

AI makes this deception easier to scale. Messages can be translated, personalised, and quickly adapted to imitate the tone, terminology, and context of a particular organisation, while synthetic voice and video make it harder to recognise the familiar signs of fraud. Compromised business accounts add another layer of credibility because the message may genuinely come from a colleague, customer, or supplier the recipient already knows.

3 How they attack

"The important change in 2026 is how quickly a familiar weakness can turn into a serious incident."

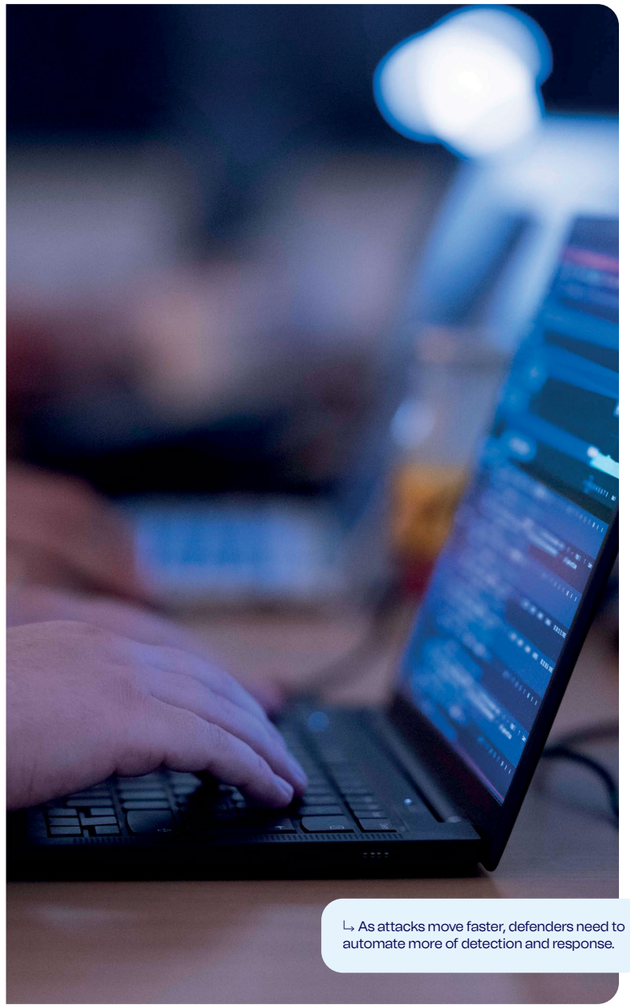


Photo: Telenor

↳ As attacks move faster, defenders need to automate more of detection and response.

Training is most useful when it helps employees recognise how attacks actually work, rather than relying on generic awareness messages. But awareness training cannot carry the entire burden. Even experienced users can be deceived. Security controls should assume that some attempts will succeed.

The aim is to make mistakes less likely and, just as importantly, less damaging: use phishing-resistant authentication where appropriate, limit standing privileges, verify unusual requests through a separate trusted channel, restrict risky authentication flows, and make abnormal access easier to detect.

The basics still matter, but they need to move faster

Many successful attacks still rely on familiar weaknesses: unsupported internet-facing devices, delayed security updates, poorly protected accounts, excessive privileges, weak separation between systems, or inadequate monitoring. These are often described as basic cyber hygiene. That can make the work sound simple. It is not.

Good security foundations will not stop an organisation from being targeted. They make it harder for an attacker to succeed and limit the consequences when something does go wrong.

In a complex organisation, keeping systems patched, identities protected, configurations secure, and monitoring effective is a continuous operational task. The challenge in 2026 is that organisations have less time to get it right. However, smaller organisations do not necessarily need to build all these capabilities themselves; monitoring, detection, and response can increasingly be obtained as managed services.

Attack techniques will keep changing, but the basic pattern is much the same. Attackers look for an easy way in, exploit trust, and use whatever access they can get. The important change in 2026 is how quickly a familiar weakness can turn into a serious incident.

Check where you stand

You do not have to start from scratch. Nordic authorities provide practical tools that can help organisations assess their current cybersecurity posture, identify gaps, and decide what to tackle first.

Norway, Cybersjekk:
NSM's Cybersjekk gives organisations a quick overview of their security posture and recommends measures based on their answers. It draws on NSM's basic principles for ICT security and can be repeated as security improves.

Cybersjekk.no

Denmark, Systemoverblikket:
The Danish authorities' Systemoverblikket helps businesses map important systems and data and provides prioritised recommendations for improving their protection. A separate IT risk assessment tool is available for organisations that want to go further.

Sikkerdigital.dk

Sweden, Cybersäkerhetskollen:
Cybersäkerhetskollen helps organisations assess how systematically they work with information and cyber security. It provides immediate feedback and suggested actions, with benchmarking available against other organisations.

Ncsc.se

Finland, Kybermittari / Cybermeter:
Developed by Finland's National Cyber Security Centre, Cybermeter provides a structured way for organisations and management teams to assess cyber-risk management and identify areas for improvement.

Kyberturvallisuuskeskus.fi

The tools differ, but the principle is the same: understand where you stand, identify the most important gaps, and improve systematically rather than trying to respond to every new threat individually.



Photo: Telenor

When attacks move faster, so must the response. Pictured: Telenor Norway's Network Operations Centre (NOC).

1. Telenor Cyberdefence (2026). Trusselbildet Q2 2026: Trusselaktørene blir raskere – virksomhetenes responstid blir avgjørende.
2. Telenor (2026). Telenors sikkerhetspuls Q1 2026.
3. Finnish National Cyber Security Centre (2026). Uusi aalto M365-tietojenkalastelussa – AI-avusteinen laitekoodin kalastelukampanja, 21 May 2026.
4. CERT-SE (2026). CERT-SE:s veckobrev v.22, 29 May 2026.
5. Microsoft Defender Security Research Team (2026). Inside an AI-enabled device code phishing campaign, Microsoft Security Blog, 6 April 2026.
6. Akamai Security Intelligence Group (2026). Mini Shai-Hulud: The Worm Returns and Goes Public, 15 May 2026.
7. Google Threat Intelligence Group (2026). GTIG AI Threat Tracker: From Prompting to Autonomy – The Evolution of Adversarial AI, 8 September 2026.
8. Google Threat Intelligence Group (2026). GTIG AI Threat Tracker: From Prompting to Autonomy – The Evolution of Adversarial AI, 8 September 2026.

CHAPTER 4

The Nordic resilience gap

Security and resilience are moving up the agenda across the Nordics. But confidence in the ability to keep critical operations running tells a different story. Our survey of 2,427 Nordic business leaders and decision-makers reveals a gap between recognising the risks and being ready for disruption.

Only half feel ready for serious disruption



Agree that their organisation is well prepared to maintain critical operations during a serious digital disruption.

What this means:
Resilience is tested when normal operations fail. The results point to a gap between recognising the importance of security and being confident that critical operations can continue through a serious disruption.

Disruption tops the threat list

44% Finland

40% Norway

39% Sweden

33% Denmark

Name service disruption among their top three digital threats.

What worries Nordic organisations most?

39% Service disruption

37% Data breaches

32% Fraud and impersonation

State-linked threats stand out in Denmark
18% cite state-linked cyber activity, compared with 8–12% elsewhere.

AI concerns in Finland
25% cite AI-enabled threats, the highest in the Nordics.

What this means:
Nordic decision-makers are most concerned about consequences close to the business: services going down, data being compromised, and fraud and impersonation. The findings put operational continuity at the heart of the threat picture.

Security is shaping buying decisions



Say that, over the past 12 months, security and resilience have become more important criteria when procuring connectivity or digital services.

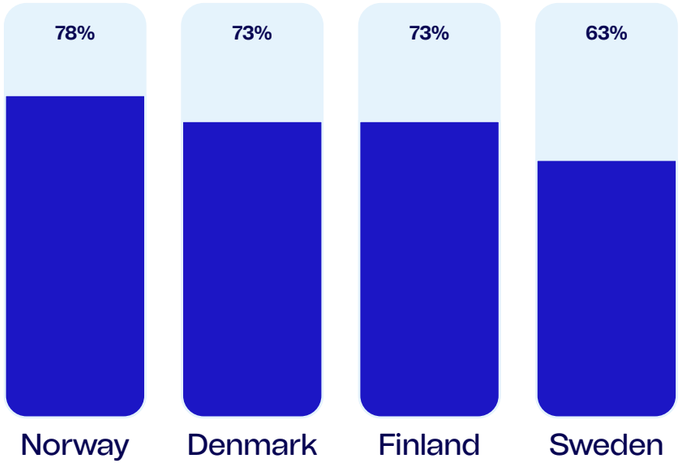
What this means:
The shift suggests resilience is moving upstream – from something organisations address after technology is chosen to something that increasingly influences the choice itself.

Control over data matters

Where
data is stored

Who
can access it

Which
jurisdiction applies

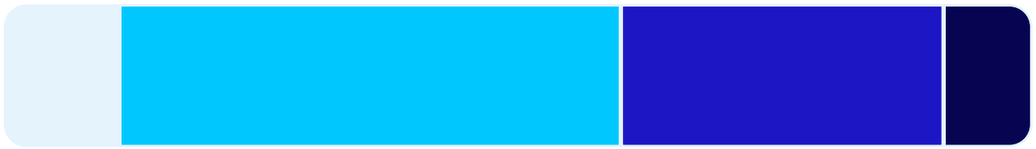


Agree that digital sovereignty will become increasingly important to their organisation.

What this means:
Digital sovereignty is emerging as a resilience issue. Knowing where critical data is stored, who can access it, and which jurisdiction applies is increasingly part of how Nordic organisations think about control over their digital dependencies.

Full AI preparedness remains uncommon

Self-assessed ability to detect and respond to AI-enabled cyber threats.



12% feel fully prepared

48% feel somewhat prepared

33% feel unprepared

7% do not know

Across the Nordics, priority is running ahead of preparedness

Priority

71% see digital sovereignty growing in importance

58% put greater weight on security when buying

Preparedness

50% feel ready for serious disruption

36% expect higher security and resilience investment

12% feel fully prepared for AI-enabled threats

Recognising the need for resilience is one thing.

Building it is another.

Four markets, different resilience signals

Norway

78% Highest focus on sovereignty

65% Highest reported AI preparedness

Sweden

36% Highest concern about fraud and impersonation

29% Highest concern about ransomware and malware

Denmark

61% Security and resilience rising in procurement

18% Highest concern about state-linked cyber activity

Finland

56% Highest reported operational readiness

44% Highest concern about service disruption

About the survey
The survey was conducted by Opinion on behalf of Telenor in August–September 2026. It is based on responses from 2,427 business leaders and decision-makers across Norway, Sweden, Denmark and Finland, with approximately 600 respondents in each market. The findings reflect respondents' assessments of their own organisations.

CHAPTER 5

From backup to tested continuity

Continuity means keeping essential services running at an agreed minimum level and restoring those that are interrupted. Networks, people, and suppliers must be able to work together during disruption.

Resilience depends on the whole system

Networks and power

Protected infrastructure
Sites, masts, fibre, and data centres protected against physical damage and unauthorised access.

Backup power
Batteries, generators, fuel deliveries, and arrangements for prolonged power cuts.

Alternative connections
Separate routes, spare capacity, and tested switching when a connection fails.

Systems and operations

Core systems and data
Systems that connect users and run services, with protected data backups and tested recovery.

Monitoring and cyber protection
Detect faults and attacks, protect systems, and contain incidents.

Response and recovery
Clear responsibilities, service restoration, and timely information for customers and authorities.

People and coordination

People and suppliers
Trained teams, supplier support, spare parts, and access to affected sites.

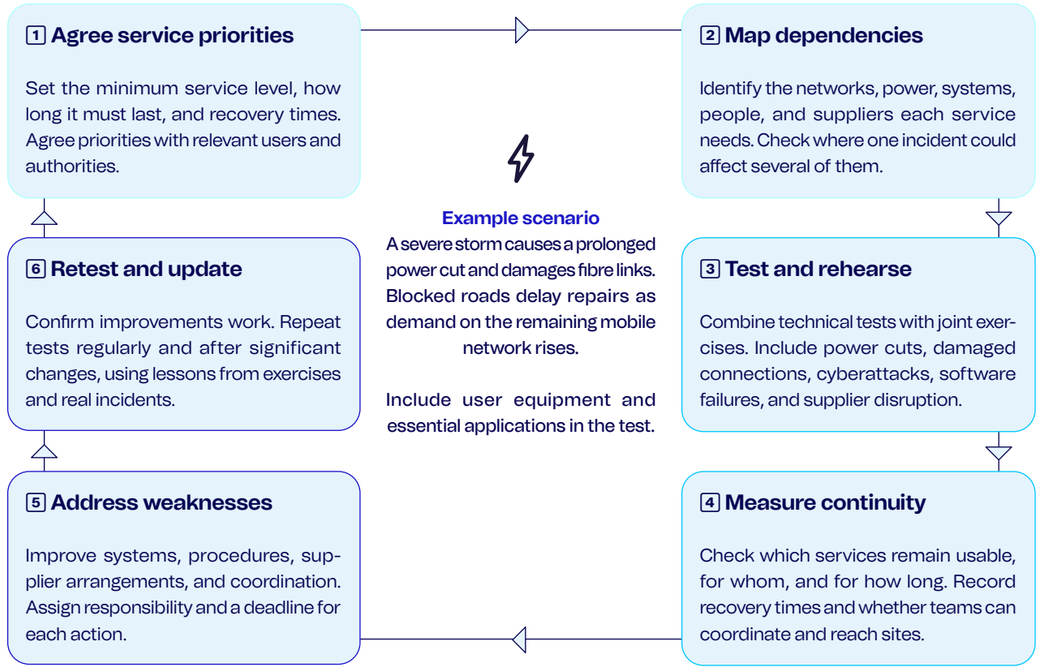
Cooperation across sectors
Joint plans and exercises with energy providers, transport operators, and public authorities.

Critical service needs
Agree the connectivity needs of emergency services, public services, and critical businesses.

Why this matters in the Nordics
Nordic societies depend heavily on digital services. Severe weather, long distances, and shared dependencies make coordination across sectors and borders essential.

Can essential services keep working?

The continuity test cycle
Test whether systems, people, and suppliers can maintain essential services and restore those that are interrupted.



Resilience depends on systems, people, suppliers, and authorities working together to maintain essential services and restore those that are interrupted.

The spreadsheet that made recovery possible

Partner perspective - Truesec, Telenor's partner in Denmark

Truesec is a cybersecurity specialist whose teams help organisations respond to attacks and restore operations. One of its cases involved a fully automated logistics business that was hit by ransomware.

The backups had been wiped and the inventory records lost. The company no longer had records of where goods were stored and how much stock it held. Truesec estimates that reconstructing that information from the physical warehouse would have taken around three weeks.

Fortunately, an employee had saved a spreadsheet containing warehouse locations and stock balances. That file enabled the company to recover quickly.

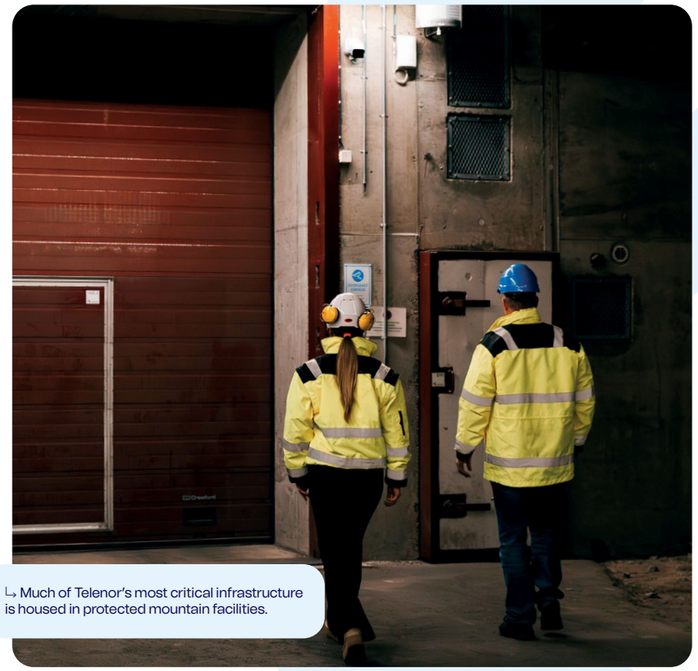
Truesec's advice is to make access to essential data like this part of a tested recovery plan. Organisations should agree which services must be restored first, keep backup copies protected even if an administrator's account is compromised, and practise restoring the systems and data those services need.

CHAPTER 6

Digital sovereignty gets real

What happens when an essential service depends on software, updates, or supplier support that suddenly become unavailable? Digital sovereignty is about the choices and capabilities needed to keep that service running. That starts with understanding where dependencies become vulnerabilities and what it takes to preserve credible alternatives.

Photo: Telenor



↳ Much of Telenor's most critical infrastructure is housed in protected mountain facilities.

6 Digital sovereignty gets real

When dependence becomes a security question

Digital sovereignty is not a new concept, but the geopolitical context has changed the urgency and scope of the conversation around it. Vendor dependence, jurisdiction, software control, data protection, and critical infrastructure resilience have been discussed for years. What is changing is that these issues are increasingly being brought together as part of a broader security and preparedness agenda.

Russia's war against Ukraine, sabotage and hybrid threats in Europe, cyber operations by state-linked actors, supply-chain insecurity, and uncertainty in global technology policy have changed how digital dependencies are assessed. Cloud, software, AI, and digital infrastructure are no longer only questions of efficiency, innovation and cost. They are also part of Europe's strategic resilience.

The challenge is to ensure that critical digital services remain trusted, available, and controllable under stress. For public authorities, hospitals, emergency services, transport systems, telecom networks, energy systems and financial infrastructure, resilience depends not only on cybersecurity, but also on who operates key systems, which jurisdiction applies, how software is maintained, whether alternatives exist, and how services can continue during a crisis.

A practical sovereignty test starts with three questions.

1. Who controls the data?
2. Who can keep the service operating?
3. How dependent are we on technology that cannot readily be maintained, replaced, or moved?

Europe puts sovereignty into policy

The proposed EU Cloud and AI Development Act (CADA) is best understood as part of this wider shift. Cloud and AI infrastructure are not just commercial services, they are strategic resources for economic security, competitiveness, and resilience.

CADA at a glance

The Cloud and AI Development Act, CADA, is the European Commission's proposed framework for strengthening Europe's cloud and AI ecosystem. It is now being considered by the European Parliament and the Council and may change before adoption.

The proposal focuses on three main areas. First, it supports research, development and innovation in next-generation cloud and AI technologies. Second, it aims to expand European computing capacity by accelerating sustainable data-centre deployment. Third, it seeks to strengthen autonomy through a common EU-wide framework for assessing cloud and AI sovereignty and mechanisms supporting adoption in the public sector and critical sectors.

CADA reflects a wider rebalancing in European digital policy, where openness to global technology is increasingly combined with stronger safeguards for critical dependencies, public-sector resilience, and operational control in sensitive use cases.

Three dimensions of digital sovereignty

With CADA, sovereignty must be defined in more practical terms. It is not enough to declare that a service is "sovereign"; authorities and critical sectors need to understand what kind of control is required, for which workloads, and under which circumstances.

A useful way to think about sovereignty is across three dimensions: data sovereignty, operational sovereignty, and technology sovereignty.

Photo: European Union



↳ The proposed Cloud and AI Development Act now goes to the European Parliament and the Council. The final text may still change.

Data	Operations	Technology
Where data is held, who can access it, and which laws apply	Who can operate, support, and, restore a service including during disruption	Whether underlying software, platforms, and components can be maintained, replaced, or adapted
Who controls our data?	**Can we keep services running and recover?**	**Can we manage our technology dependencies?**

Taken together, these dimensions show that digital sovereignty cannot be reduced to data residency. For critical systems, a key question is whether organisations retain the control and capabilities needed to operate, support and restore services under adverse geopolitical conditions, including when access to essential technology or supplier support is restricted.

However, the level of control required depends on the criticality of the service. A practical approach to digital sovereignty should be risk-based. A municipality's website, a school collaboration tool, a public-health analytics platform, and classified emergency communications should not all be treated in the same way. Over-classification increases cost, reduces flexibility, and slows innovation. Under-classification leaves critical functions exposed. The task is to define which workloads require which level of control, prioritise the dependencies that matter most, and sequence changes in a way that is technically and economically realistic.

"Digital sovereignty cannot be reduced to data residency."

Four countries, four approaches

Across the Nordics, digital sovereignty has also become a practical policy question. The debate is not only about cloud infrastructure, but also about software choice, public procurement, vendor dependence and concentration risk, security classification, and the ability of public authorities to maintain control over critical digital services. Even when organisations use different service suppliers, they may share dependencies on the same underlying cloud or AI model providers.

Denmark is focusing on reducing vendor dependence and widening technology choice, backed by DKK 80 million for a 2026–2029 action plan for digital sovereignty.[1] Finland is approaching digital sovereignty through security and preparedness, including updated cloud-security criteria and greater scrutiny of dependence on infrastructure outside national control.[2,3] Norway is emphasising national control over critical digital infrastructure, including access to data-centre capacity under Norwegian technical and legal control in peace, crisis and war.[4] Sweden is combining public-sector cloud policy, shared digital infrastructure and AI capability with a stronger focus on security, efficiency and technological choice.[5,6]



Photo: Telenor

Distributed telecom infrastructure – local exchanges, fibre backbones and mobile sites – can form part of the foundation for sovereign edge cloud.

6 Digital sovereignty gets real

"Telecom operators already operate critical national infrastructure under national regulation."

These developments in the Nordics suggest that digital sovereignty is developing as a question of choice, preparedness, and control. Public authorities need access to global technology, but they also need the ability to assess dependencies, choose alternatives, avoid lock-in, and apply stricter requirements where public order, national security or essential services are at stake.

A similar logic applies to cloud. Sovereignty cannot mean simply rejecting global technology. In many areas, global hyperscalers provide world-leading capabilities in scalability, automation, cyber defence and AI tooling. The challenge is to combine these capabilities with appropriate legal and operational control for sensitive workloads. Some use cases may be served by public cloud with strong contractual safeguards. Others may require an EU sovereign model. The most sensitive national functions may require national sovereign cloud with local operational control, cleared personnel and exclusive national jurisdiction.

The common thread is that sovereignty should expand the range of credible choices available to governments and critical sectors. It should help them decide when global platforms are appropriate, when European or Nordic alternatives are needed, and when national control is indispensable.

Where telecom operators fit

Telecom operators have a particular role in this agenda. They already operate critical national infrastructure under national regulation, security obligations and public expectations. They manage distributed infrastructure, national fibre backbones, mobile networks, local exchanges, data centres, security operations, and customer-facing services. This means telecom operators can play an important role in sovereign digital ecosystems. Their potential contribution lies not simply in hosting data, but in combining connectivity, distributed infrastructure, security operations and local operational capability under established regulatory and security frameworks.

Sovereign edge cloud is especially relevant for use cases requiring low latency, high availability, local processing or jurisdictional assurance. Healthcare, public safety, energy, transport, industrial automation and emergency services may all require digital infrastructure close to users and devices, while remaining under trusted operational control. In the Nordics, distributed telecom infrastructure can form part of that foundation.

This does not mean telecom operators should build everything themselves. A credible model will rely on partnerships with technology vendors, cloud providers, system integrators, and cybersecurity providers. But the operating model matters. For sensitive workloads, the relevant issue is whether a local or European actor retains operational responsibility, customer control, update control, jurisdictional assurance, and service-continuity capability.

Telecom operators also face a specific complexity: networks themselves are becoming increasingly cloudified. Core networks, operations support systems, analytics, automation, customer channels, network telemetry and AI-enabled operations may all rely on cloud infrastructure somewhere in the stack. A simplistic approach to cloud sovereignty could therefore have unintended consequences for network architecture, innovation, and resilience.

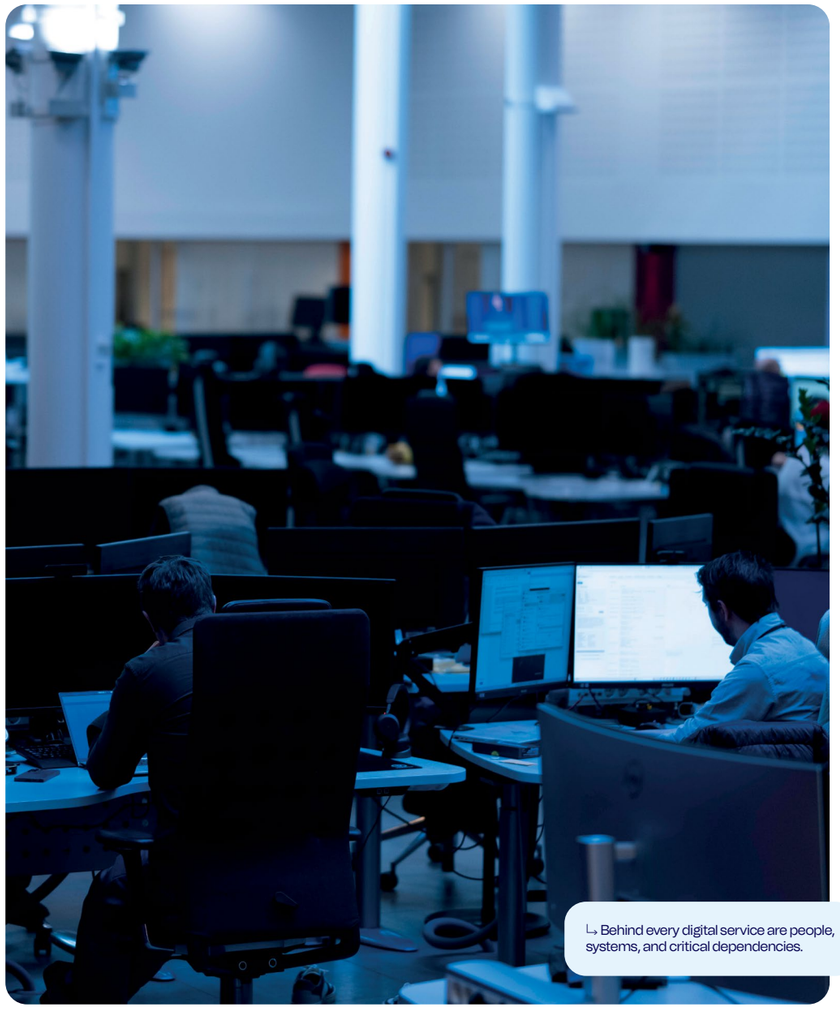


Photo: Telenor

↳ Behind every digital service are people, systems, and critical dependencies.

Put sovereignty to the test

The next phase of digital sovereignty will be practical. Authorities and critical sectors need workload classification: which functions are genuinely critical, which require national control, which can be served by EU-level sovereign services, and which can safely remain in standard public cloud. Procurement must also evolve. Public procurement should assess resilience, exit options, interoperability, jurisdictional exposure, operational control, supply-chain transparency, energy efficiency and long-term maintainability, not only price and standard functionality.

Sovereignty risks should also be tested against plausible scenarios. What happens if a critical cloud service becomes unavailable, remote support is interrupted, a software component can no longer be updated or a key supplier cannot deliver? Scenario testing turns an abstract dependency into an operational question: can the organisation continue, isolate the affected function, move the workload or recover through an alternative arrangement?

This cannot sit with the IT or security function alone. Procurement, enterprise architecture, legal, data governance, business continuity and operational teams all hold part of the sovereignty picture and need a shared understanding of which dependencies are acceptable.

Nordic cooperation should also be strengthened, but in a practical and targeted way. The key question is how society can make better use of the capacity, infrastructure, and expertise that already exist across the business sector. Telecom operators, cloud providers, industrial companies, transport actors and other critical sectors all hold capabilities that may be essential in a crisis. A Nordic approach could help make this capacity more usable across borders by aligning expectations on critical workloads, trusted suppliers, secure operations and incident response, while preserving national control where security requires it. The objective should be more preparedness and operational choice, not fragmented national solutions or an unrealistic attempt to build everything domestically.

Digital sovereignty should not be understood as digital self-sufficiency. That would be unrealistic and undesirable. It should be understood as the ability to make deliberate choices, maintain control over critical functions, reduce unacceptable dependencies, and preserve credible alternatives. These capabilities strengthen resilience by helping organisations withstand and recover from disruption, adapt to geopolitical change and continue delivering the services on which society depends.

1. Agency for Digital Government, Denmark (2026). Digital sovereignty.
2. Finnish Government (2026). Security criteria for cloud services to be updated with launch of new national criteria library.
3. Finnish Security and Intelligence Service (Supo) (2026). Cloud adoption obscures the digital independence of states.
4. Norwegian Ministry of Digitalisation and Public Governance (2025). Tydeliggjør krav til sikkerhet og setter mål for en bærekraftig og samfunnsnyttig datasenternæring, 27 June 2025.
5. Government Offices of Sweden (2026). Sweden's AI Strategy in five minutes. February 2026.
6. Government Offices of Sweden (2026). A cloud policy for Sweden – for increased security, efficiency and innovation in public administration. June 2026.



Photo: GSMA

↳ Zainab Hussain Siddiqui, Vice President Sustainability & Lead Responsible AI, Telenor.

CHAPTER 7

Who’s keeping your AI in check?

Responsible AI is becoming a business requirement. Existing governance for privacy, security, human rights and procurement remains essential, but the speed, scale and evolving capabilities of AI require organisations to adapt how those systems work.

Zainab Hussain Siddiqui, Vice President Sustainability & Lead Responsible AI at Telenor, shares what Telenor has learned about building responsibility into how AI is developed, bought, and used.

7 Who’s keeping your AI in check?

The reality check

362

362 AI incidents documented in 2025, up from 233 the previous year.

11%

11% of surveyed businesses reported having no responsible-AI policies in place in 2025, down from 24% in 2024.

59%

59% cite lack of knowledge as an obstacle to implementing responsible AI.

Source: Stanford HAI, AI Index Report 2026

Your responsible AI to-do list

01 Know where your AI is

You cannot govern what you cannot see.

Start by establishing and maintaining an inventory of where AI is being developed, procured, deployed and used across the organisation. That includes formally approved systems, AI embedded in existing software, and tools being used independently by employees.

For large organisations, even finding it can be difficult. Zainab Hussain Siddiqui says the first task is to "cast a net" across the organisation and understand where AI is happening.

ASK: What AI are we developing, buying or already using?

02 Set the guardrails

Don't begin with a 100-page AI policy. Establish the principles that should apply whenever AI is developed or deployed.

Think beyond cybersecurity and privacy. Responsible AI can encompass security, privacy, fairness and bias, human rights, data governance, transparency, explainability and human oversight and control. It can also include wider considerations such as inclusion and environmental impact.

"The guardrails, the guardrails, the guardrails. It is just so, so important."

– Zainab Hussain Siddiqui

ASK: What must our AI systems always do, and what must they never do?

03 Put responsibility where the AI is

Governance cannot operate at arm's length from the people building and deploying AI.

Telenor's experience points to involving those teams directly in responsible AI, while retaining clear accountability through project, contract or platform ownership.

The ambition is to build responsible practices into the process rather than an additional approval at the end.

ASK: Who owns the risk, and who understands the technology?

04 Make responsible use the default

The end goal is not for employees to remember a governance manual every time they use AI.

Build requirements into workflows, platforms and development processes wherever possible. Automate documentation and assessments where appropriate, while keeping human expertise and oversight where the risk requires it.

"The ideal scenario is that responsible AI is hardcoded into the steps we take to develop and deploy AI, while at the same time building the behaviours and culture that make responsible AI part of how people work."

– Zainab Hussain Siddiqui

ASK: Which safeguards can we embed in the process, and where is human judgement still required?

05 Ask harder questions before you buy

Buying AI transfers technology into your organisation, not responsibility out of it.

Before procuring an AI product, ask:

- What data was the model trained on and where did it come from?
- Has it been assessed for bias?
- Where will our data be processed?
- What can we change or control?
- What testing has been performed?
- Where is human oversight required?
- What happens if the model's behaviour changes over time?
- What responsibilities do we assume when we deploy or modify it?

ASK: Do we understand the AI well enough to trust it with our customers, people and data?

06 Match governance to the risk

Not every AI use case needs the same controls.

Summarising a public document is fundamentally different from using AI to make or support decisions about people. Increase testing, oversight, documentation and accountability as potential impact increases. Risk assessment is not a one-off exercise. Monitor performance and incidents after deployment, and reassess the use case when the model, data, operating context or intended purpose changes. Under the EU AI Act, deployers of high-risk AI systems have specific obligations, including assigning human oversight to people with necessary competence, training and authority.

ASK: What happens if this AI gets it wrong and who is affected, and how will we know?

It's about

Know the standard

ISO/IEC 42001
Think of ISO/IEC 42001 as a structured way to ask:
Have we properly thought through our AI risk?

The world's first AI management-system standard establishes requirements for creating, implementing, maintaining and continually improving an AI management system.

For Telenor's Zainab Hussain Siddiqui, its value is straightforward: it forces organisations to consider AI-specific risks, mitigations, accountability and human oversight systematically.

And the standard is gaining traction: 36% of organisations surveyed for Stanford's 2026 AI Index said ISO/IEC 42001 influenced their responsible-AI practices.

The end goal

A well-governed organisation isn't one with the longest AI policy.

It is one where people understand what responsible AI means for their role, safeguards are embedded in how AI is developed and deployed, accountability is clear, and responsible use becomes the default.

Because ultimately, responsible AI is about something bigger than compliance.

It's about trust.

trust.

Know what your AI can access

Partner perspective - Truesec, Telenor's partner in Denmark

Truesec's cybersecurity work includes helping organisations control access to their systems. It warns that accounts used by software can receive less oversight than employee accounts. AI agents, which can carry out tasks on a user's behalf, extend that concern.

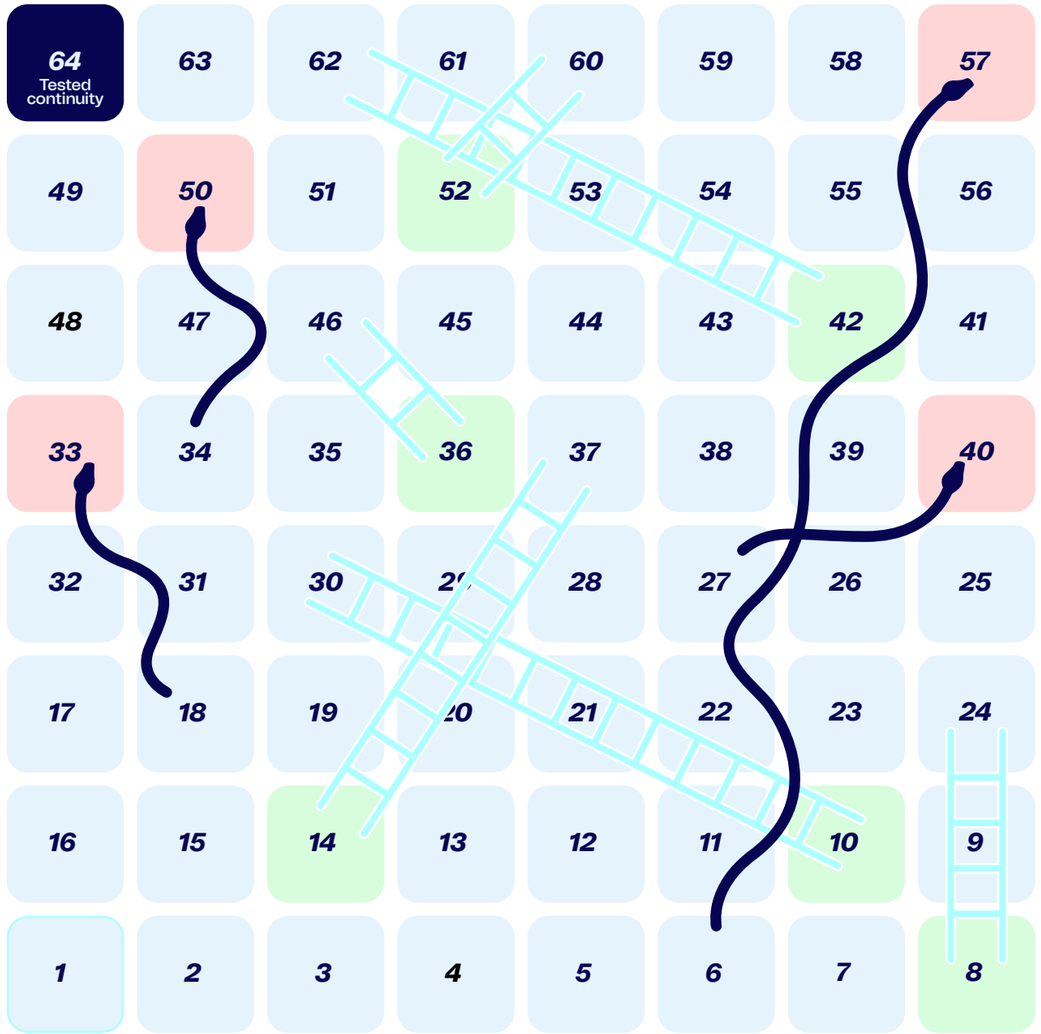
These tools use accounts or other digital credentials to access business systems. Truesec highlights the risk of giving them broad permissions without sufficient oversight. As agents act across systems at speed, poorly controlled access can have consequences beyond the task they were introduced to perform.

The governance task therefore starts when an agent is introduced. Organisations need a named person responsible for its access and clear limits on what it can do. Those permissions should be reviewed as its role changes, and access that is no longer needed should be removed.

CHAPTER 8

Resilience has a cost

Stronger digital and telecom resilience does not happen by accident. It requires investment, procurement models that value quality, and clear responsibility for who pays. Play it out below — each snake or ladder illustrates a choice or weakness that affects resilience.



Cut along the dashed circles
One token to each player. Grab any six-sided die to start playing – a coin/button works fine as a token too.



How to play

1 2–4 players. Everyone starts on square 1 – where resilience has not yet been assessed.

2 Take turns rolling a six-sided die and move your token that many squares.

3 Land on a ladder's foot (green) – climb to the top of the ladder.

4 Land on a snake's head (red) – slide straight down to its tail.

5 You must land on square 64 with an exact roll to finish – overshoot and you stay put.

6 First to reach square 64 – tested continuity – ***WINS.***

Ladders build resilience

8 **Redundancy and backup power**
Independent routes and tested backup power help maintain priority services during disruption.

10 **Procurement that values reliability**
Procurement rewards demonstrated resilience, maintenance and recovery capability.

14 **Monitoring, testing and exercises**
Monitoring detects problems; tests and exercises expose weaknesses that are then addressed.

36 **Clear funding and responsibility**
Named owners and committed funding turn resilience plans into implemented measures.

42 **Incident response & restoration capability**
Recovery is faster with practised teams, usable recovery plans and available spares.

52 **Supplier diversity and contingency planning**
Tested supplier alternatives and contingency arrangements reduce dependence on any one source.

Snakes erode it

33 **Underfunded maintenance**
Ageing batteries, equipment and neglected maintenance increase the risk of failure.

40 **Price-only purchasing**
Price-only purchasing leaves insufficient provision for backup capacity, maintenance and recovery.

50 **Unclear ownership of risks**
No one owns a critical dependency, so a known weakness remains unresolved.

57 **Critical incident exposes that you are not ready**
A shared failure point takes out both primary and backup connections, causing a prolonged outage.

i The policy point

Resilience requires upfront and ongoing investment. Public and private buyers must reward quality, not only lowest price. Critical resilience measures need clear funding and ownership. If society expects continuity in crisis, it must be willing to pay for it.

CHAPTER 9

When trust becomes the target

A major disruption creates an urgent technical problem. It can also create something harder to contain: a battle over what happened, who is responsible, and whom to trust.

One incident. Two crises.

The network goes down.

Engineers are trying to establish why. Authorities are assessing whether the cause is accidental failure, cyberattack, or physical sabotage. Customers want answers. Journalists are calling.

There is not yet enough verified information to give them. But the information crisis has already started.

Speculation spreads. Different explanations emerge. Old images or claims acquire new relevance. Someone points the finger. An apparently authoritative account offers an explanation. Some of it may be wrong. Some may be deliberately misleading. And some may simply be people trying to make sense of an uncertain situation.

While the organisation works to establish what happened, a second contest has already begun: defining what the incident means.

Operational crises
What happened?
What is affected?
How do we restore services?

Information crises
Who caused it?
What are we being told?
Whose version should we believe?

The facts are only part of the fight

Paul M. H. Buvarp, a senior scientist at the Norwegian Defence Research Establishment (FFI) studies disinformation and informational threats. He argues that one of the biggest mistakes organisations can make is to think of manipulation primarily as a contest between facts and falsehoods.



Photo: FFI

Paul M. H. Buvarp, Senior scientist at the Norwegian Defence Research Establishment (FFI).

"It's about feelings, it's about identity, and it's about trust."

Consider the competing explanations that followed the poisoning of former Russian intelligence officer Sergei Skripal or the shooting down of Malaysia Airlines flight MH17. Buvarp points out that many of the narratives promoted by Kremlin-linked or Kremlin-supportive sources did not form a single coherent alternative explanation.

And they did not have to.

The effect, he says, can be "much more about poisoning the well", meaning introducing enough competing explanations to make any coherent account, including the true one, harder to believe.

The objective may not be to persuade an entire population that one particular story is true. Confusion in itself has value. If people lose confidence in institutions, information sources, or each other, reaching agreement and acting decisively becomes much harder.

The vacuum fills fast

A serious disruption creates almost ideal conditions for this.

The organisation at the centre of an incident typically needs time to investigate and verify information. Different teams and authorities may need to coordinate, and decisions are often made with an incomplete picture.

Online, people aren't waiting for the full picture.

“This isn’t 1990 anymore”

Buvarp points to the 2024 Southport stabbing in the UK. As police, security institutions, and journalists worked to establish the identity and motive of the attacker, conspiracy theories and false narratives were already spreading online.

The initial false claim did not have to come from a foreign actor. “Yes, the threat actors in Russia are a problem,” Buvarp says. “But I think the bigger problem is everyone else.”

A rumour can emerge organically. Activists or political groups may connect it to an existing grievance. People share it because it fits what they already believe. Only then does a malign actor need to identify a useful narrative and amplify it.

That distinction matters. Organisations are not necessarily defending themselves against a neatly orchestrated disinformation campaign with an obvious beginning. They are operating in an information environment where speculation, misinformation, political agendas, and deliberate manipulation can rapidly become intertwined.

That also makes restraint important. Not every inaccurate claim, hostile comment, or legitimate criticism is part of an influence operation. Treating ordinary disagreement as deliberate manipulation can itself damage trust.

That changes what crisis communication needs to do.

The traditional instinct is understandable: establish the facts, coordinate internally, clear the response with legal teams, and communicate once the organisation is confident that what it says is correct.

Buvarp argues that waiting too long carries its own risk.

“This isn’t 1990 anymore.”

If an organisation stays silent for 24 or 48 hours while it works towards a verified account, other people will continue telling the story without it.

That does not mean speculating or communicating unverified information. Instead, Buvarp points to what some intelligence organisations and newsrooms call “showing the work”: explaining what is known, what is not yet known, what is being investigated, and how conclusions are being reached.

He cites the US intelligence community’s approach in the months before Russia’s full-scale invasion of Ukraine. Rather than keeping its assessment entirely behind closed doors, it disclosed unusually detailed information about what it was seeing and why.

An organisation may not yet be able to tell people exactly what happened, but it can still help them understand what it is doing to find out.

Trust is built before you need it

Preparing for the information crisis starts long before the outage, attack, or suspected act of sabotage.

Buvarp argues that organisations should treat trust among customers, communities, partners, and other stakeholders as a resource that needs to be understood and maintained. They should establish which channels people can rely on during an incident and include the information environment in crisis exercises, alongside the operational response.

And the exercise should not end with restoring the network. It is important to establish what happens if a false explanation starts spreading. What if an organisation or executive is impersonated? What if a genuine grievance becomes attached to the incident? Who responds, through which channel, and who needs to coordinate?

Exercises cannot reproduce the reality of a crisis perfectly. But, as Buvarp puts it, they can at least help ensure that the relevant people “know who to call”.

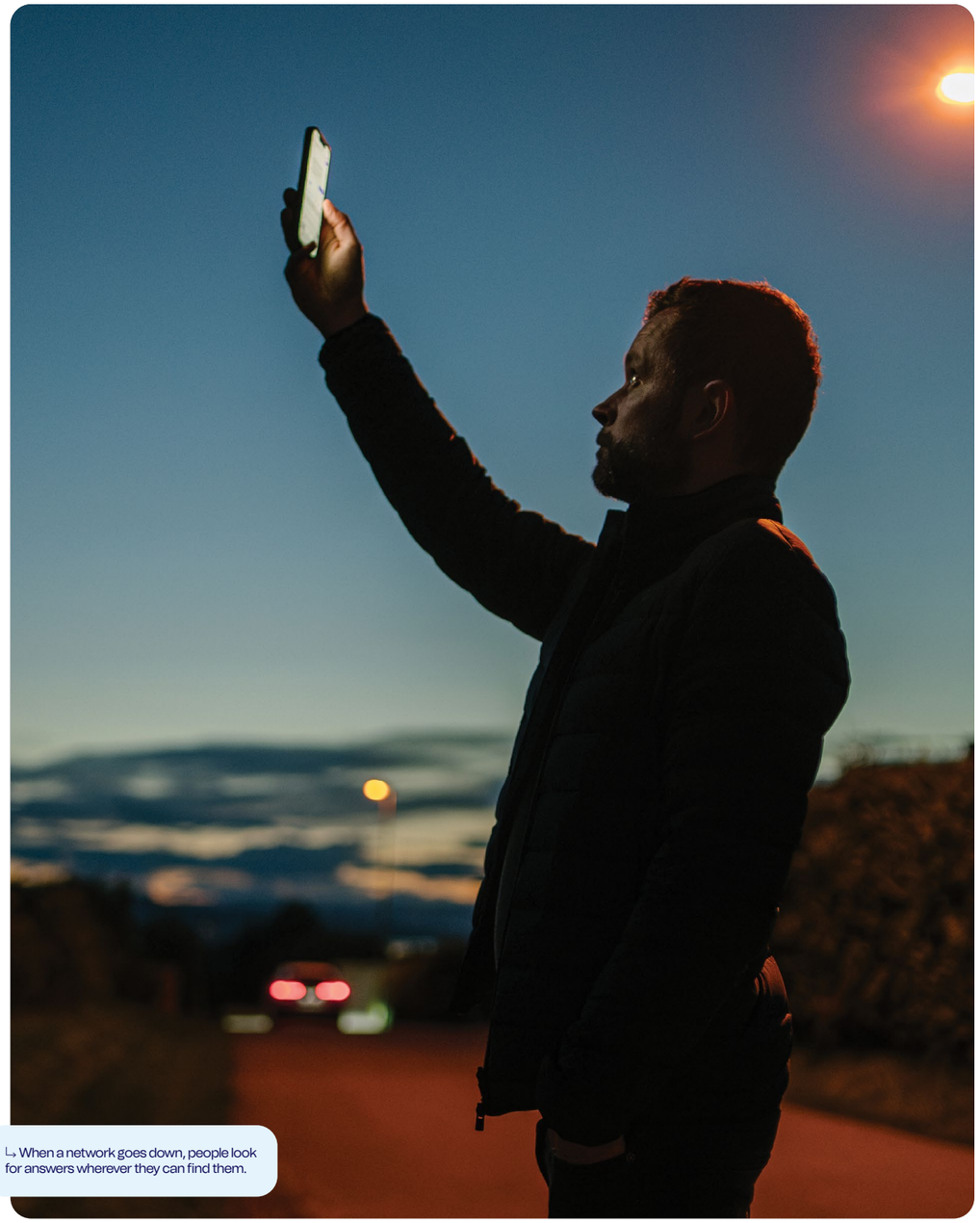
His most provocative advice is also perhaps the simplest.

“I’d take out the word ‘facts’ from all plans and procedures.”

He is not suggesting that facts do not matter, or that organisations should communicate anything that is not factual. His point is that facts alone are not enough.

9 When trust becomes the target

Photo: Simen Prestaasen / DSB



↳ When a network goes down, people look for answers wherever they can find them.

9 When trust becomes the target

Photo: Finnish Secretariat of the Security Committee



Annukka Ylivaara, Assistant Secretary General of Finland's Security Committee.

“If it's just informing people, it's not enough.”

People will try to make sense of what is happening. They will construct a story around an incident whether the organisation at its centre participates or not.

For organisations preparing for the next crisis, that creates a second resilience challenge alongside restoring the system: helping people understand the story while it is still unfolding.

Resilience is built on relationships

If Paul M. H. Buvarp's perspective shows how quickly trust can come under pressure, Finland's approach to comprehensive security starts with what needs to be in place before that happens.

“Trust is an essential element in the Finnish approach, even the foundation,” says Annukka Ylivaara, Assistant Secretary General of Finland's Security Committee.

Finland's model is built around collaboration between authorities, businesses, organisations, and citizens to safeguard society's critical functions. That collaboration depends on trust.

“Without trust, this overarching collaboration in society is not possible,” Ylivaara says.

And when a crisis comes, Finland does not treat the operational and information dimensions as separate problems. A disruption may play out simultaneously in the physical, cyber, and information environments. The same principle applies across them: the structures and relationships needed to respond should already exist.

“If we are trying to create those kinds of entities when the crisis is coming, it takes time,” Ylivaara says. “They have to exist before the crisis.”

Know who to call

That is one reason exercises play such a prominent role in Finland's preparedness. Tabletop exercises bring together the organisations expected to play a role in a particular scenario. Working through the scenario can quickly reveal whether an important actor is missing. But exercises also do something less tangible: they allow people to build relationships before they have to rely on them.

“During exercises you also get to know those counterparts,” Ylivaara says. “If there is a problem, you know who to contact.”

It is an approach Finland has cultivated over decades. National defence courses bringing together representatives from government, authorities and the business community date back to 1961. Today, Ylivaara says Finland is exercising more frequently with companies and NGOs as well.

Communication is part of the response

There is also common ground between the Finnish approach and Buvarp's warning about leaving an information vacuum.

Communication during a crisis needs to be “active and not passive”, Ylivaara says. But she argues that organisations need to go further and treat communication as part of strategic leadership and management.

That does not mean protecting trust by shutting down disagreement. Ylivaara argues that a resilient society must leave room for legitimate criticism. Silencing it can itself be dangerous. High trust, in other words, should not mean unquestioning trust.

Resilience starts long before the crisis

A serious disruption can put systems and trust under pressure at the same time.

Buvarp talks about how quickly uncertainty can be filled by speculation, competing narratives and deliberate manipulation. Ylivaara's perspective shows why the response starts much earlier: with relationships that already exist, people who know whom to call, and organisations that have practised working together.

The same applies to communication. Organisations may not have every answer when a crisis begins. But they can be prepared to communicate what they know, acknowledge what they do not, and explain what they are doing next.

When a crisis comes, the response depends on trust, relationships, and ways of working established long before the disruption begins.

CHAPTER 10

Resilience checklist

Is your organisation continuity-ready?

A practical self-assessment for businesses and public authorities
Every organisation should know which services are critical, what they depend on, and how to maintain operations during a disruption. This checklist is designed to help businesses, IT, facilities, and procurement teams assess their preparedness together, rather than serve as a formal compliance assessment.

How to use the checklist. Mark each item Yes, Partly, No, or Not Applicable (N/A). Count an item as Yes only if it has a named owner, is documented, and has current evidence that all relevant continuity requirements are met, with no unresolved critical findings. Review evidence at least annually; test operational capabilities at intervals appropriate to the risk and after material changes. Partly means incomplete, untested, or covering only some critical services. Mark unknown capabilities Partly and flag them for verification. Record the reason for any N/A response.

Focus on critical gaps. One serious weakness affecting a critical service may matter more than several positive answers elsewhere. Select the three most important gaps and assign an action, owner, and deadline.

Checklist item	Yes	Partly	No	N/A
1. Critical services and recovery objectives				
Have you identified critical services, who depends on them, and how the consequences of disruption worsen over time?				
For each critical service, have you defined the minimum acceptable level of service and which users or functions should be prioritised under degraded conditions?				
Have you set the maximum tolerable interruption, target recovery time, and acceptable data loss for each critical service?				
Is the order in which critical services will be maintained or restored clear and approved by senior management?				
2. Dependencies and single points of failure				
Have you mapped the people, premises, power, connectivity, data, systems, and suppliers needed to deliver each critical service?				
Have you identified single points of failure and shared dependencies that could disable primary and backup arrangements at the same time?				
Do you understand how failure in one service, supplier, or infrastructure system could cascade into other critical operations?				
Have manual workarounds, alternative resources, or other continuity arrangements been shown to deliver the required minimum service safely and for the planned duration?				
3. Connectivity and communications				
Have you identified which critical operations depend on fixed broadband, mobile connectivity, private networks, satellite, voice and messaging services, or remote access?				
Do critical locations, systems, and roles have appropriate backup connectivity that supports the required minimum service for the planned duration?				
Have you checked and addressed shared failure points between primary and backup connections, including underlying providers, cable routes, sites, power, and login systems?				
Has switching to backup connectivity been tested under the load expected during disruption, and can relevant staff activate it without relying on normal online instructions?				
4. Power, premises, and people				
Do you know how long critical sites and systems, including local network equipment and essential user devices, can operate without grid power, and does this meet your continuity objectives?				
Are batteries, generators, fuel, and cooling arrangements maintained and tested under realistic conditions, including safe access for fuel deliveries and repair teams?				
Can critical work continue if premises are inaccessible because of extreme weather, transport disruption, or a security incident?				
Are sufficient trained staff available, and are essential contact details and instructions accessible offline?				

10 Resilience checklist

Checklist item	Yes	Partly	No	N/A
5. Suppliers and digital services				
Have you identified critical suppliers, their important subcontractors, and any shared platforms or providers on which several suppliers depend?				
Do relevant contracts specify minimum service, recovery, escalation, information-sharing, and crisis-communication expectations?				
Can alternative suppliers, substitution, exit arrangements, essential stocks, or emergency logistics be activated within recovery targets, including during widespread disruption?				
Do you know which critical services depend on cloud platforms, software services, data integrations, identity services, AI systems, or automated decision-support tools?				
Can essential functions continue if these digital services become unavailable, including through data recovery, human decision-making, or manual fallback procedures?				
6. Cyber, data, and operational recovery				
Are backups of critical data and configurations up to date and protected against alteration or deletion, even if administrator accounts are compromised?				
Can authorised staff access the backups, credentials, and encryption keys needed for recovery if normal systems and logins are unavailable?				
Have recovery tests shown that priority services can resume safely in a clean, trusted environment within agreed recovery-time and data-loss limits?				
Can teams detect a serious incident and isolate affected systems while maintaining essential operations where safe?				
7. Incident leadership and crisis communication				
Is decision-making authority, escalation thresholds, responsibilities, and the point at which senior management becomes involved clearly defined?				
Are contact lists, decision logs, and a shared record of the incident and its effects current and accessible if normal systems are unavailable?				

Can you communicate with employees, customers, citizens, suppliers, and authorities through alternative channels if normal channels fail?				
Are messages and notification procedures prepared for major outages, cyber incidents, and degraded services, and have they been practised under pressure and with incomplete information?				
8. Testing, governance, and improvement				
Is there a named senior owner for continuity, supported by clear responsibilities, sufficient resources, and appropriate funding?				
Do exercises include prolonged disruption, concurrent failures, unavailable key staff and suppliers, loss of normal communications, and failed software or configuration changes?				
Do incidents and exercises lead to prioritised actions with owners, deadlines, and funding, and is evidence that each action works required before it is closed?				
Are continuity arrangements reviewed at planned intervals and after material changes, incidents, and exercises, with results reported to senior management?				

Your three priority actions

Choose the gaps that create the greatest risk to critical services, not simply the easiest actions to complete.

Priority gap	Action required	Owner	Deadline
1.			
2.			
3.			

A useful continuity plan is not necessarily the longest one. It is the plan that has been understood, tested, and improved before it is needed.

CHAPTER 11

What authorities should prepare for

Digital resilience cannot be built by asking each organisation to prepare in isolation. Nordic authorities need to agree which essential services must keep working, coordinate preparations across sectors and borders, test recovery arrangements, and protect trusted communication. Responsibilities and funding for exceptional preparedness should be settled before a crisis occurs.

11 What authorities should prepare for

Photo: Telenor



↳ Restoring one service often depends on another. Operators, suppliers and authorities need to plan together.

Essential services depend on each other

When electricity fails, communications services can come under pressure. When connectivity is lost, energy operations, payments, and health services can be affected. Cloud platforms, suppliers, and specialist staff connect these services in ways that are easy to overlook until something goes wrong.

In the survey for this report, around half of respondents say their organisation is well prepared to maintain critical operations during a serious digital disruption: 49% in Denmark, 47% in Sweden, 49% in Norway, and 56% in Finland. These figures reflect respondents' assessments of preparedness, rather than results from practical tests. They nevertheless show that confidence in continuity is far from universal.

"A crisis is the wrong time to discover that neighbouring countries use different assumptions."

Even a sound contingency plan can fall short if an organisation's power supply fails, a key supplier cannot deliver, or a critical digital service becomes unavailable. Authorities therefore need to work with businesses to prepare for disruptions that affect several essential services at once. This requires clear responsibilities and practical arrangements for cooperation across sectors and borders.

The Nordics have capable institutions and a strong tradition of public-private cooperation, but each country has its own starting point. Action should build on existing arrangements and work already under way, address remaining gaps, and make it easier to give and receive support across borders.

For Telenor, five priorities stand out: set clear resilience outcomes and fund what is required; build trusted infrastructure while keeping markets open; coordinate preparedness across sectors and borders; exercise together and close the gaps identified; and treat trusted communication as an operational capability.

11 What authorities should prepare for

A. Set clear resilience outcomes and fund what is required

Preparedness starts with practical questions. Which services must keep working? At what minimum level, and for how long? Who should be prioritised when capacity is limited, and what should be restored first?

Authorities should answer these questions with operators and the sectors that depend on them. Expectations should reflect the importance of each service and allow operators to choose how best to meet them. Public procurement should give appropriate weight to continuity, recovery and support throughout the contract, alongside price. Buyers should ask for evidence that these capabilities have been tested.

Expectations must be proportionate and coordinated to avoid overlapping or conflicting requirements. Where services, networks, and suppliers cross national borders, Nordic authorities should seek comparable definitions, compatible crisis procedures, and clear points of contact. A crisis is the wrong time to discover that neighbouring countries use different assumptions about priorities, information sharing, or mutual assistance.

Resilience has a real cost. Redundant capacity, backup power, spare equipment, secure services, specialised personnel, and realistic exercises all require investment. Competitive markets can deliver much of this, but they will not automatically fund every capability society may want to reserve for an exceptional crisis.

Authorities should distinguish between three layers: (1) the proportionate baseline that every operator should provide; (2) enhanced resilience supported by ordinary customer demand; and (3) exceptional capacity or preparedness required for wider societal or national-security purposes. Responsibilities and funding should be explicit at each layer. Where authorities require capacity, geographic redundancy, stockpiles or readiness beyond this baseline and normal commercial demand, requirements should be stable and predictable, with public funding or co-financing agreed in advance.

B. Build trusted infrastructure without closing markets

Control over critical data is becoming a greater concern. Across the four countries, the survey for this report showed that 63–78% of the respondents expect digital sovereignty to become more important for their organisation. This includes where critical data is stored, who can access it, and which jurisdiction protects it.

For authorities, the practical questions are who controls a critical service, who can access its data, and whether it can be maintained and restored if a supplier becomes unavailable. Neither the supplier's nationality nor the location of its data centres is sufficient on its own. Assessments should use transparent, proportionate criteria covering jurisdiction, governance, security, and operational capability, including dependence on individual suppliers and access to credible alternatives. Requirements for national control should reflect the sensitivity of the service and the risks involved.

Using several suppliers, making systems work together, and enabling data or services to move between providers can create useful alternatives. These measures should reduce risk enough to justify their cost and complexity. Resilience also needs attention throughout the life of systems and equipment, from design and supplier selection to maintenance and replacement. Where suppliers must be replaced, deadlines should allow time to test replacements and maintain security and service continuity during the transition.

Digital sovereignty should be understood in this practical sense: the ability to make informed choices, retain control of critical functions, reduce unacceptable dependencies, and remain operational in a crisis. It should create credible options while preserving access to trusted capabilities and partners. Cooperation can strengthen this control without requiring national self-sufficiency.

C. Coordinate preparedness across sectors and borders

A hospital may have backup power but still depend on connectivity, cloud services, or deliveries that are disrupted. Restoring one service may require another to be restored first. Telecommunications networks depend on reliable power, while energy operators rely on communications to monitor, operate and restore their systems. Several providers may also rely on the same cable route, cloud platform or subcontractor. Authorities and operators therefore need a shared understanding of the dependencies that could prevent essential services from continuing.

The priority is to identify the most consequential weaknesses and agree how to respond. Authorities should agree priorities in advance, with input from essential service operators. These should cover how scarce fuel, equipment and specialist staff are allocated and the order in which services should be restored. The priorities should account for dependencies between services and be flexible enough to change as the incident develops. Authorities should also establish who can decide between competing needs. They should clarify what operational information can legally be shared to support those decisions and how its confidentiality can be protected. That information must be kept current and shared securely.

These relationships need to be established before an incident. Authorities, operators, and critical suppliers should know whom to contact, what information they can share, and who can take decisions. Critical infrastructure operators should have an established role in cross-sector preparedness planning and crisis coordination. This should include secure access to relevant threat information and involvement in decisions on shared resources and restoration priorities. Joint contingency plans should address these dependencies and be tested through regular cross-sector exercises, with particular attention to telecommunications and energy. Authorities should also clarify what logistical and protective support operators can expect when restoring infrastructure in unsafe or inaccessible areas.

Nordic arrangements need not be identical, but they must work together under pressure. Compatible approaches to classifying incidents and sharing information should help teams coordinate across borders. Staff, equipment, and capacity should be able to move where they are needed. Authorities should allow evidence from audits or certification to be reused across borders where it meets equivalent requirements, subject to applicable legal and security safeguards.

Nordic cooperation should also make it possible to use infrastructure and operational capabilities in neighbouring countries to maintain essential services. Authorities should identify and address barriers to cross-border backup, recovery, and network operation where these arrangements improve resilience. These arrangements should be tested against clear requirements for security, control, and availability during a crisis. They should also specify who can activate backup capacity and how access will be maintained when several countries need it at once. In addition, authorities should identify and monitor concentrations of risk where multiple critical services depend on the same infrastructure, cloud platform, supplier or specialist capability. Understanding these shared failure points is critical, as a disruption affecting a single provider or dependency can have cascading consequences across several sectors simultaneously.

D. Exercise together and close the gaps

Exercises should test what happens when several things go wrong together. A prolonged power outage might coincide with a cyberattack, while damaged roads delay repair teams and customers receive conflicting information. Authorities and businesses need to practise making decisions in those conditions, including when their usual communications channels are unavailable. Exercises should also test deliberate attacks that exploit dependencies between sectors, bringing together security, operational resilience and crisis-management capabilities.

The participants should reflect the real response chain: operational teams, senior decision-makers, authorities, emergency services, municipalities, communications functions and critical suppliers. Exercises should test access to sites, prioritisation of services, information sharing, crisis communication, and the movement of personnel, equipment or capacity across borders. Where AI supports critical operations or incident response, exercises should test whether staff can check its output and take over if it fails.



Photo: Telenor Sverige

↳ Telenor Sweden at Telö, Sweden's national exercise for the telecom sector, where operators and authorities train together on handling crises in the networks.

For every significant weakness found in an exercise participants should agree who will fix it, how the work will be funded, and when it must be completed. Where a remedy requires action across sectors or levels of government, the participants should identify a lead authority and a clear route for escalating unresolved decisions. The correction should then be tested. Working through these problems together also builds the relationships that help people act when information is incomplete.

E. Treat trusted communication as an operational capability

During a serious disruption, people need to know what is happening and what to do. Delayed or conflicting information leaves room for rumours and manipulation and can make the response harder. Reliable public communication should therefore be planned and tested alongside service restoration.

Authorities and relevant organisations should build on existing arrangements to provide timely, reliable and accessible crisis information, including when normal communication channels are disrupted. Communication should be coordinated in line with established responsibilities and security and crisis-management procedures.

These communications arrangements should be exercised alongside security, technical response and crisis management. Scenarios should include AI-generated impersonation and test how organisations communicate when facts are incomplete, false narratives target the response and information changes quickly. Timely communication, transparent acknowledgement of uncertainty, and visible correction of errors help protect credibility under pressure and maintain public trust.

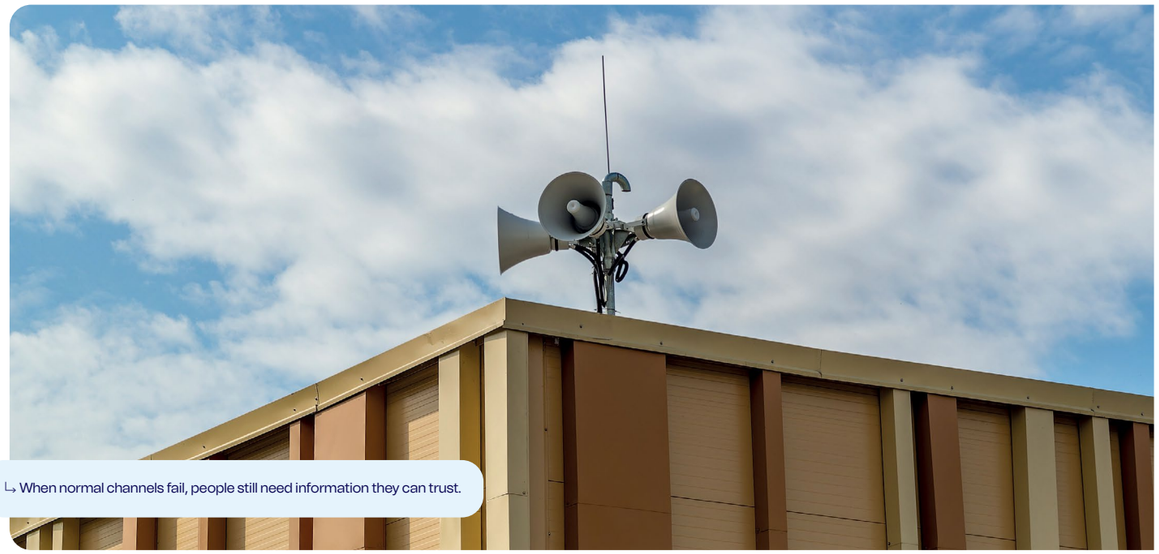


Photo: Telenor

↳ When normal channels fail, people still need information they can trust.

From awareness to action

European policy is already moving towards a broader model of preparedness. The EU Preparedness Union Strategy calls for public-private emergency protocols and regular cross-sector exercises. The Critical Entities Resilience (CER) Directive and the NIS2 Directive on cybersecurity establish requirements for assessing risks and strengthening resilience, alongside cooperation between responsible authorities.

Nordic cooperation should build on these initiatives and existing national structures, while avoiding duplicative or inconsistent requirements under sector-specific, cybersecurity, protective-security and civil-preparedness frameworks.

The Joint Nordic Declaration on Security of Supply, signed on 2 September 2026, provides a practical opportunity to strengthen this cooperation. It calls for obstacles to Nordic cooperation on security of supply to be identified and addressed. It also provides for a feasibility study during 2027 and a joint report with proposals from national authorities to be presented to ministers no later than autumn 2027.[1] Governments should ensure that these proposals address how telecommunications services can be maintained during crises, involving operators in practical arrangements for cross-border backup, recovery, and support.

Nordic governments should agree which gaps to address first, assign responsible authorities, and set dates for joint tests. Operators and other essential service providers should be involved from the outset.

Success means essential services keep working at an agreed minimum level, people receive information they can trust, and authorities and operators can restore services together.

1. Government Offices of Sweden, Joint Nordic Declaration on Security of Supply, 2 September 2026.

Telenor believes: policy asks on resilience, trust, and preparedness

The findings in this report point to five priorities for Nordic governments and public authorities.

1. Set clear resilience outcomes and fund what is required: Authorities should define essential functions, minimum service levels and restoration priorities, with risk-based expectations aligned across sectors and borders. Procurement should reward tested resilience. Operators should meet clear baseline duties. Exceptional preparedness beyond those duties and normal commercial demand requires explicit responsibility and predictable, proportionate funding.

2. Build trusted infrastructure without closing markets: Assess control, jurisdiction, security and recovery capability in relation to the service's sensitivity. Address unacceptable dependencies while preserving competition, innovation, and access to trusted partners. Support alternatives where they reduce risk and allow transition periods that protect service continuity.

3. Coordinate preparedness across sectors and borders: Identify shared dependencies, agree restoration priorities and involve critical infrastructure operators in crisis planning. Enable cross-border backup, recovery, and network operation where security, control and availability requirements are met. Agree how staff, equipment, and capacity will be shared when several countries need support at once.

4. Exercise together and close the gaps: Run joint exercises across sectors and borders to test responses to power and communications outages, supplier failures, cyberattacks, and deception using AI. Where operations depend on AI, check that staff can review its output and take over if needed. Assign responsibility, funding, and deadlines for fixing significant weaknesses, then test the changes.

5. Treat trusted communication as an operational capability: Authorities and operators should agree and test how they will provide timely crisis information, including when normal channels fail. Arrangements should cover uncertainty, impersonation, and cooperation with media.

From commitment to delivery: Telenor is ready to contribute operational experience to this work. Governments should agree the priorities, assign a lead authority for each action, identify the funding mechanism, and set dates for implementation and joint exercises.

11 What authorities should prepare for

Photo: Telenor



↳ Strong communities depend on resilient infrastructure.



part of telenor

Read the report online ⤵
dna.fi/pohjoismainen-tietoturvatutkimus-2026