There's no time to waste

Nordic Digital Security 2024

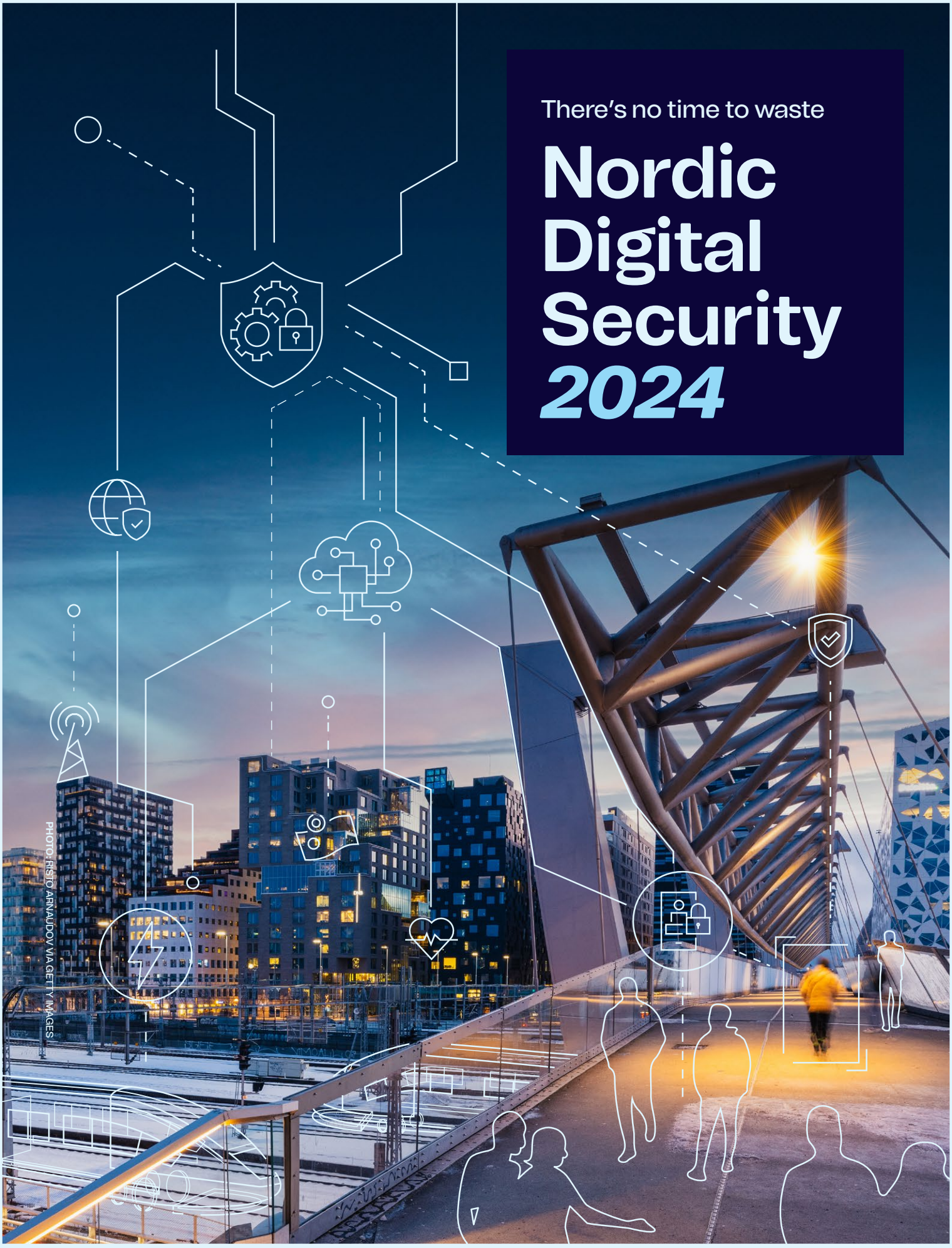


PHOTO: RISTO ARNAUDOV VIA GETTY IMAGES

telenor nordics

Table of contents

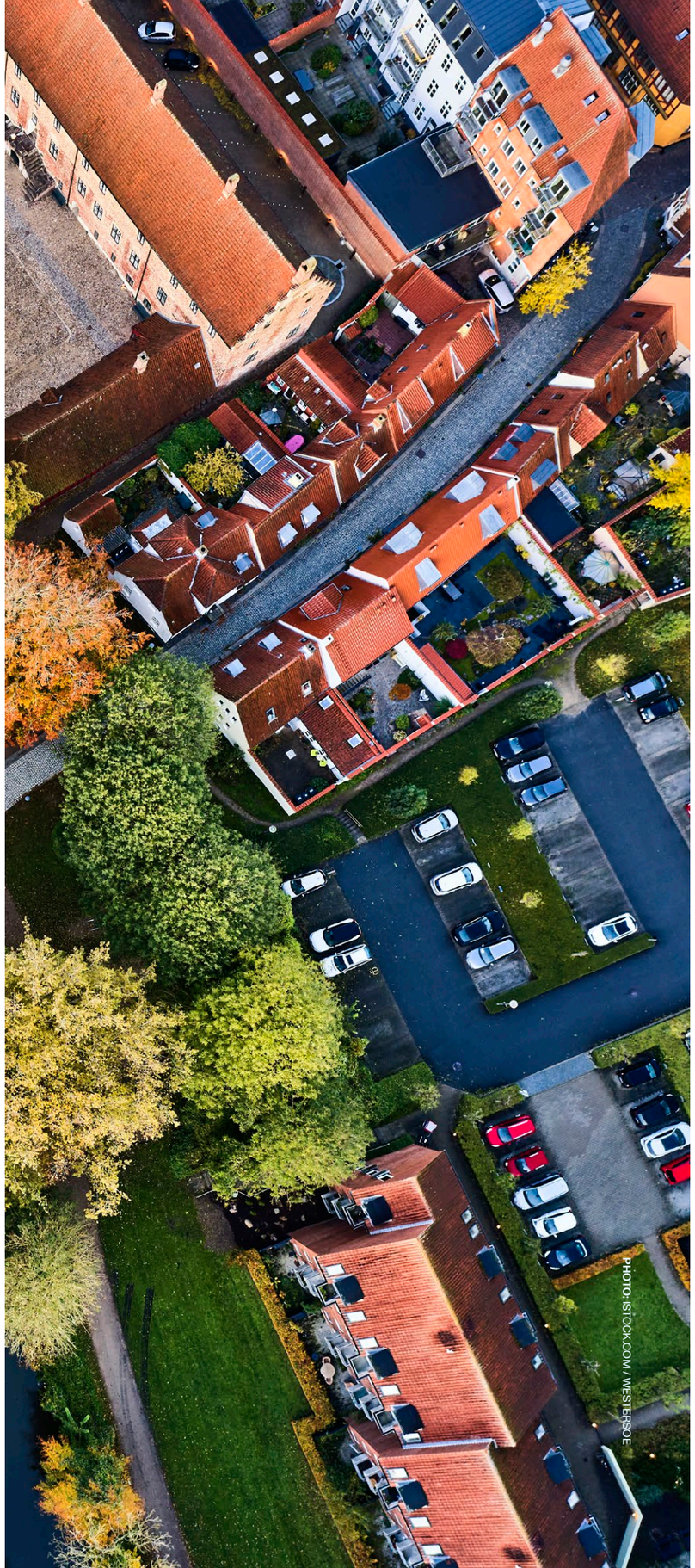
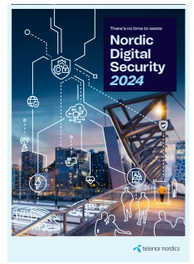


PHOTO: ISTOCK.COM / WESTERSOE



Previous edition:

Content: Where an external author or origin is not explicitly stated, the assessments, advice, and expertise presented in this report are based on the knowledge and experience Telenor Norway and Telenor Group has amassed building a holistic security approach to safeguard and protect ourselves and our customers, and to help fulfil our social responsibilities.

External sources: Text from external sources with source references are direct quotations.

The editorial process was completed in August 2024. **Design:** NewsLab. **Images:** Getty Images, iStock, Harald Pettersen, Ole Jørgen Bratland, Hans A. Rosbach, Harald Spjelkavik, Equinor, Bertel O. Steen, Telenor. **Print:** Involve.

Digital version: *https://www.telenor.com/about/our-companies/nordics/digitalsecurity/2024*

Disclaimer: Some of the content in this report has been translated from its original version in Norwegian to English with the assistance of artificial intelligence. It has undergone internal quality assurance by the publisher, Telenor Group, as well as by external authors. Please note that there may be minor deviations in language and technical terms due to the translation process.

It's time to move from words to action

In a security environment that is more uncertain and threatening than it has been in decades, those responsible for critical infrastructure across the Nordic region must prepare for scenarios that were once unthinkable. It's a situation that requires us all to ramp up efforts to strengthen our resilience.

THE THREAT LANDSCAPE IN AND AROUND THE NORDIC COUNTRIES has shifted dramatically in a short period of time. An attack on communication services and networks could have severe societal consequences. Therefore, we must collectively enhance our focus on resilience and robustness, while strengthening our ability to protect our digital infrastructure to withstand potential attacks. By doing so, we can ensure adequate security for our operations, our customers, and society.

NORDIC CO-OPERATION focused on aligning security legislation and establishing a coordinated Nordic regime for security clearance has been increasingly recognised as crucial within broader national and regional security discussions. With Sweden and Finland now members of NATO, the potential for strategic co-operation have never been greater. The requirements for national autonomy should be operationalised in a way that makes it possible to use personnel across borders, as well as share technical solutions and infrastructure. The urgency of this task cannot be overstated—simply put, there's no time to waste.

ACCESS TO CRITICAL EXPERTISE is a shared challenge across the Nordic region that impacts the defence sector, as well as key preparedness actors in the civilian sector and the business community. A more unified Nordic approach to fostering innovation could to a larger degree motivate multinational technology providers to establish competence centres in the region which would significantly strengthen our collective digital resilience in the Nordics. This, in turn, would enhance Nordic innovation and competitiveness. The Nordic countries must pool their resources and create larger, more robust frameworks for collaboration. This can ensure access to relevant expertise and capacity needed to deliver products and services in conditions of emergency and heightened levels of alert.

ALL NORDIC COUNTRIES NEED A WELL-FUNCTIONING MARKET FOR PREPAREDNESS AND SECURITY SERVICES. This can be achieved by ensuring that customers in both the private and public sectors increasingly demand products and services that meet strict security standards. Preparedness is costly. It can only be sustained if key public sector entities, such as state and municipal authorities, to a larger degree define the safeguarding of long-term preparedness considerations and national security interests as a firm requirement in public procurement processes. This is key to establishing a broader market for preparedness and security services in support of critical societal functions. It would not only improve security but also strengthen our collective resilience.

CLOSER INTEGRATION OF THE BUSINESS COMMUNITY into national security and preparedness frameworks is an area where more progress is needed across the Nordics. Many larger businesses that are relevant to these frameworks are still not regularly included in relevant forums. This represents a serious weakness in our overall national and regional resilience and is cause for concern. To address this, relevant authorities across the Nordic countries should ensure that key businesses are systematically integrated into security and preparedness structures, with a particular focus on enhancing information sharing, not only between the public and private sectors but also across Nordic borders. Improved mechanisms for two-way sharing of threat and security intelligence within and between Nordic countries would ensure that both businesses and national authorities are better equipped to respond to evolving threats that could escalate across borders. We need to move into high gear to better integrate the business community into our national and regional preparedness efforts.

"Ensure key business actors are systematically involved in national and regional security and preparedness planning."

As the threat level rises, investing in the safeguarding of the infrastructure that underpins our societies and services on which we depend is a vital preventive measure. The most important step we can take together is to move from words to action. We must continue to train for realistic scenarios across sectors, integrate the business community more closely into national and regional preparedness frameworks, and strengthen co-operation within the Nordic region and with our NATO allies.

» We need to move into high gear to better integrate the business community into our national and regional preparedness efforts.

Jon Omund Revhaug
EVP and Head of Telenor Nordics

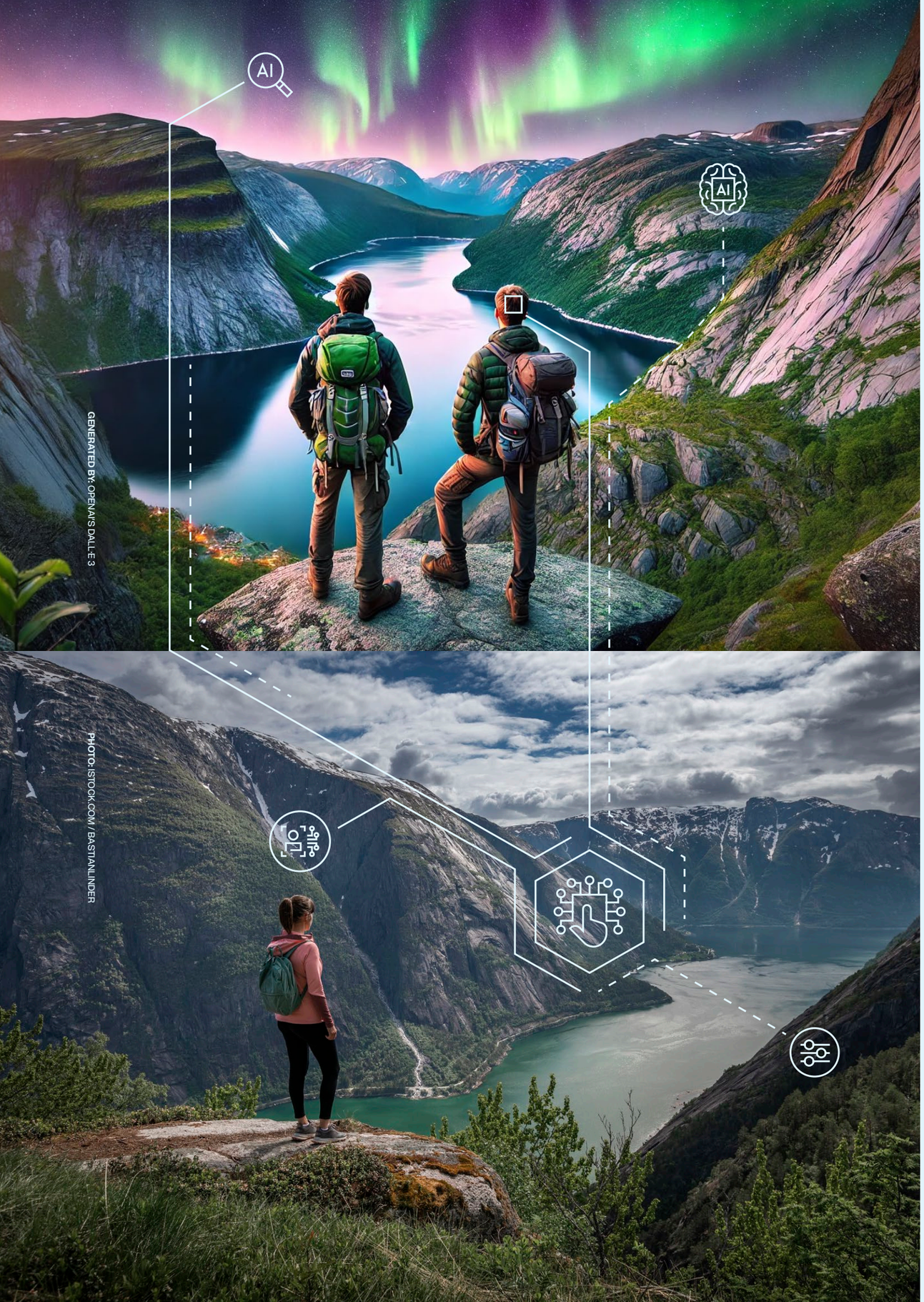
Birgitte Engebretsen
CEO, Telenor Norway

Jussi Tolvanen
CEO, DNA Oyj

Bjørn Ivar Moen
CEO, Telenor Sweden

Lars Thomsen
CEO, Telenor Denmark

PHOTO: TELENOR



2

AI – playing both offense and defence

ChatGPT, Bard, DALL-E and GitHub Copilot. The development within artificial intelligence (AI) is moving at a rapid pace. While the benefits are many, AI presents never-before-experienced security challenges. The question is: can the safety mechanisms designed to protect us keep up with the development of malicious use of AI?

Left: With the fast development of AI-tools, it's sometimes hard to separate reality from fiction. During the summer of 2024 AI-generated images gave a false impression of Norwegian scenery. For the record, the top image is AI-generated, whereas the bottom image is a photograph.

This article is inspired by Telenor's whitepaper "The rise of artificial intelligence: New threats, new regulations and new solutions". To read the full report, please visit telenor.com.

Artificial intelligence, or "AI", is an emerging technological force that is reshaping business and society. We are just starting to see the transformative effects of this technology in delivering value to industries, organisations and individuals. AI is not a futuristic technological concept. As we've already seen thanks to tools like ChatGPT, Bard, DALL-E and GitHub Copilot, AI is already well-integrated into our daily lives and plays an important role across a range of industries.

At the same time, we are still at the very beginning when it comes to secure implementation and use of AI, in terms of cyber-security as well as from a wider security and safety perspective.

As with any new technology, AI comes with security challenges

The breakthroughs and public availability of generative AI for text, images, voice and video, have brought AI to the attention of a much larger audience. However, most of us have in fact interacted with AI functions for years, as machine learning and AI models for categorisation and prediction are already widely applied. AI is found in services such as personalised viewing recommendations on Netflix, in voice assistants, or in customer service chatbots.

We have already seen several examples of how well-intentioned applications of predictive AI can have serious, unforeseen, and negative consequences. These include reinforcing bias, propagating discrimination, and in subtle ways embedding undesirable values and preferences from the data sets used to train the AI. As generative AI continues to take centre stage, we are also witnessing how careless applications can lead to misinformation being accepted as fact, even in legal settings. More worryingly, we have also observed that threat actors, driven by both criminal and more sinister motives, are exploiting this technology to further their malicious intents.

The secure use of text-generative AI, even in a common business function use-case like a chatbot, has already proven its potential for unintended consequences. This was recently experienced by a Canadian airline whose chatbot had given an excessively favourable offer to a customer. The airline argued that the chatbot was a separate legal person or entity for which the airline was not accountable nor legally liable, a sentiment to which the Canadian small claims court did not agree.

Researchers are proving that the securing of AI models and its applications, from a technical security standpoint, is still in its infancy. They have amongst others, documented how "prompt injection," or innovative and creative feeding of text into a text generating AI system, has led to unexpected and troubling outcomes. Although these AI systems are built to handle random inputs, some tests have managed to compromise the underlying computer system on which the models operate.

AI-driven assistants are entering our workplace at full speed, and with a varying degree of control. Businesses are now starting to realise that the AI input and output open a whole new realm of data security. This includes the information returned back to the users from the AI assistant, and in equal parts, all the data that is shared by the employees as part of AI processing and training. The latter risk is less obvious for many. It all needs to be secured.

There is little doubt that all manners of AI technology will be applied to gain potentially dramatic improvements in efficiency across all kinds of business processes and systems. It will also enable us to cope with – and thus adopt – processes and systems of growing complexity. When coupling AI decision making with automation, however, the risks need to be properly understood. Having a human in the loop for high-risk decisions may often be required.

» We have already seen several examples of how well-intentioned applications of predictive AI can have serious, unforeseen, and negative consequences.

» Just as we expect AI to be pervasively transformative for businesses and society, it will likely prove to become just as available to threat actors.

It's not only "AI for good"

The newfound availability of free or very affordable generative AI services for text, images, audio and video has found a relatively immediate application with cybercriminals. They use it either as a directly applied tool in perpetration of fraud or in support of social engineering in more elaborate cybercriminal endeavours. Being able to write in a foreign language with perfect grammar, emulate a company's or demographic's tone of voice, alter your voice to impersonate another person, or even alter your live video appearance to do the same, are all obviously useful capabilities for criminal application.

With all of this is now being applied for criminal use, severe losses are being incurred as a result, for both individuals and businesses. A recent example is the attack on an employee of a Hong Kong-based business. He was initially sceptical, and reluctant to accommodate a suspicious request to conduct money transfers. He was then invited to a live video conference with what appeared to be several known company executives, all of which were in fact so-called "deepfake" altered video streams. He was thus convinced that the assignment to transfer the funds was genuine. He proceeded to transfer approximately 20 million US dollars to the criminals.

However, while it garnered much attention, this is far from the only malicious use-case for AI technologies. Just as we expect AI to be pervasively transformative for businesses and society, it will likely prove to become just as available to threat actors. Other malicious applications include efficient, automated, and scaled exploration of vulnerabilities and execution of attacks, evasion of behavioural detection, the improved and automated 'mutation' (polymorphism) of malware to escape detection, and attacks on machine learning systems themselves – all of which are actively being developed and tested by threat actors right now.

PHOTO: ISTOCK.COM / GORODENKOFF

Fighting AI back – with AI

Thankfully, however, AI technologies are also being applied to the defensive side of security.

In the past, many organisations attempting to introduce so-called Data Loss Prevention tools were overwhelmed by the effort required to finetune and maintain them. So, they would either abandon their efforts or be forced to apply the tools to a relatively narrow set of easily identifiable sensitive data types. AI is now re-invigorating this category of security capabilities, fuelled by its potential to perform meaningful analysis of highly complex sets of unstructured data.

The application of AI in phishing and social engineering is also not the exclusive domain of threat actors. AI technology is also being applied in the security capabilities intended to identify such texts, and to identify AI-generated texts in general. Thus, something as mundane as email filtering is now essentially an AI-versus-AI fight.

In cyber-security monitoring and detection, when venturing beyond the detection of what is known to be malicious, anomaly detection is applied to identify events of interest, worthy of further investigation and potentially symptomatic of a security incident. This is traditionally a challenging discipline, involving constant improvement and the finetuning of rulesets and thresholds to determine when an event is anomalous enough to warrant further investigation by human analysts. While simple automation can help streamline certain process steps, such as data enrichment prior to exposure to human analysts, the introduction of AI into anomaly detection holds potential to significantly improve efficiency. AI can better distinguish between genuine threats and false positives, thus radically improving the "signal-to-noise ratio". Similarly, we are now seeing AI-driven products come to market which address the currently labour-intensive normalisation of data from heterogenous sources, to make it suitable for detection and querying.

Transforming threat intelligence into effective detection is currently a relatively labour-intensive discipline for cyber-security organisations. This entails moving from the comparatively simple generation of atomic indicators of compromise to the detection of more complex event patterns on specific technologies. The coupling of multiple AI capabilities is poised to yield radical efficiency gains in this area, enabling more rapid development and widespread deployment of effective detection methods. This area of improvement extends to the generation of preventive measures, such as block rules and policies. Where false positive rates prove negligible, and when operational risk permits, we will likely see a gradually increasing level of automation when it comes to detection, fully removing the human from the loop.

In addition, Security Operations Centres (SOC) and Incident Response teams stand to gain significantly from AI technologies. Many tasks typically handled by the so-called "first line" SOC analysts can be automated or greatly aided by AI. The initial analysis and damage assessment can be supported in a manner that reduces the need for heavy expertise and thus lowering the skill level for filling such a role. This, in turn, helps address the global "cyber-security skills gap".

It is also worth noting how AI-driven large language models (LLM) can enhance efficiency in SOC and Incident Response teams. In the short term, we will see benefits such as the interaction between tools, data and knowledge bases, as well as the support the AI-driven language models can give by writing timelines, reports, presentations and other communications.

It's not only the criminals trying to deceive us – we're also trying to trick the fraudsters. Deception technologies have long been applied in cyber-security. This includes the creation of fake assets, such as files, accounts, computers or entire networks, that appear attractive, valuable and/or vulnerable but are not actually part of a real, operational system . This serves several purposes, most notably the high-fidelity signals from monitoring such assets, the ability to study the attacker's tactics, techniques, and procedures (TTPs) , and the diversion of the attacker, leading said attacker to

What is signal-to-noise ratio (SNR)?

SNR measures the proportion of relevant, actionable alerts (the "signal") to irrelevant or false alerts (the "noise") in a system. It indicates the clarity and effectiveness of a detection system in identifying real threats. A high SNR means the system is good at distinguishing real threats from non-threatening anomalies, leading to fewer false positives. This allows security teams to focus on genuine security incidents without being overwhelmed by irrelevant alerts. Conversely, a low SNR results in many false positives, making it harder to identify and address actual threats.

focus on the fake assets rather than the real one. However, attackers using AI for adversarial attacks can gain sufficient information over time about defence systems and identify honeypot networks, thus learning to avoid them in subsequent attacks. The introduction of AI-based dynamic honeypot assets (a tempting target that appears legitimate), aims to counter this through automatically reconfigurable traps that adjust and handle attacks based on the attacker's behaviour.

AI technology plays both offense and defence

It is evident that AI technology and its uses bring a multitude of new risks and security considerations. Within cyber-security, we see that AI drives yet another escalation, improving attacks and simultaneously advancing defences to keep up. Some argue that for once, the benefits to cyber-security defence actually exceed those offered to our adversaries - but we're still in early days.

As security professionals, we naturally tend to be somewhat dystopian in our thinking. When it comes to the evolution and exploding application of AI, this mindset is certainly not helped by the warnings voiced by several prominent technologists and AI experts that AI is an existential threat to humanity. Seeing how AI can also be applied in a security context, though, leaves one with hope.

It's all about understanding the risks and applying corresponding measures. From the safety and security measures of the AI systems and applications, to how they are applied in wider business processes, to the new security capabilities required in the business as a result, to putting a human in the loop, or even curbing our appetite for efficiency and automation, this is everyone's job and a critical leadership responsibility.

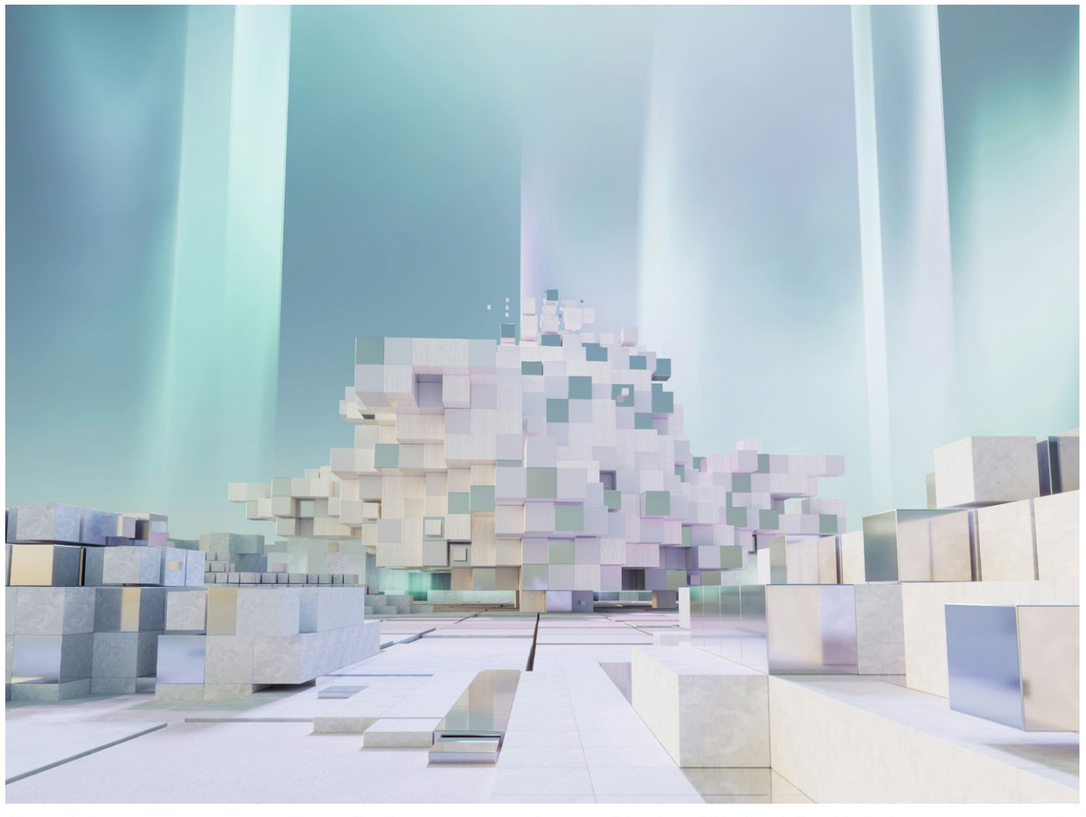


ILLUSTRATION: LINUS ZOLL / GOOGLE DEEPMIND

A human's illustration of text-to-image diffusion. The illustration is part of the project "Visualising AI" by Google DeepMind, where artists were invited to create illustrations of different aspects of AI. This illustration was created by Linus Zoll.

3

Cyber defences put to the test

The automotive group Bertel O. Steen has significantly ramped up its digital security practices in the last few years. This paid off, when hackers appeared in their systems.

Left: In 2022 Bertel O. Steen was affected by a massive cyber-attack. Following the attack, they decided to upgrade their digital security.

PHOTO: BERTEL O. STEEN

In recent years, the Norwegian automotive group Bertel O. Steen has undergone significant transformation to accelerate their digital development.

Additionally, the group has undertaken an equally important internal reassessment of their digital security practices. This is already paying off.

"I have been asked about the worst possible outcome in the event of a cyber-attack. My response is always that this is a question for our business managers, as they will face the most significant consequences," says Steingrim Soug, Head of Data Security at Bertel O. Steen.

Today, the group has a defined plan for managing security and defence-in-depth, a type of cyber-security in which several layers of control are used so that there's always a back-up in place. However, not long ago, criminals were at their doorstep – charging in at full speed.

When the warning lights flash

"As we supply products to both the military and the police, we are likely to be more attractive targets for certain types of attacks. This is a reality we have to deal with. We also experienced a specific incident that served as a significant eye-opener for many," says Soug.

To most Norwegians, the name Bertel O. Steen is synonymous with cars. This is no surprise, given their over 100-year history of importing popular car brands – with their portfolio including cars from Mercedes-Benz, Kia, and the Stellantis brands.

However, the family group is also an important name within real estate, the defence industry, and the energy sector.

Hence, when 30 shops in one of their car dealership chains Mobile were affected by a massive cyber-attack in 2022, the people at Bertel O. Steen held their breath.

"When the news broke, many likely felt that the hackers had come too close for comfort. Mobile is an independent dealer within the Bertel O. Steen group and is therefore not directly connected to the same systems or networks. Still, it made the group's top management react," says Soug.

Following the extensive cyber-attack, the group conducted a maturity analysis and decided to upgrade their digital security. Soug himself was hired to be Chief Information Security Officer (CISO), with responsibility for internal IT security.

This decision may have come in the nick of time, as it wasn't long before the warning lights were flashing again.

PHOTO: BERTEL O. STEEN

BERTEL O. STEEN

3,000	100	6,000	7,000
EMPLOYEES	COMPANIES	USERS	END POINTS

Fortifying internal defences

Among the measures implemented by Soug and his team was the introduction of guidelines to make the group's systems and network solutions more resilient in the event of an attack.

For several years, Bertel O. Steen has had an ongoing agreement with Telenor for the surveillance of their security platform. Telenor acts as the group's Security Operation Centre (SOC), taking on the day-to-day responsibility for implementing security measures against external threats.

"We already had a strong security 'shell', which made it difficult to gain access to our network. Our challenge was that if someone managed to breach the first layer, there were too many open paths leading deeper into our network," Soug explains.

The goal became to implement measures that would minimise the potential damage if a hacker managed to breach the outer layer of security.

However, for a large group like Bertel O. Steen, this isn't achieved by simply pressing a few keys on the keyboard.

"Our entire structure is comprised of more than 3,000 full-time employees across over 100 companies. In our network we operate more than 6,000 different users and we have over 7,000 endpoints. In addition, we manage several thousand operational technology (OT) units. Because of this, the network had to be divided into different zones, which allowed us to isolate a potential attack."

This approach was also applied to their cloud solutions. Nothing was to operate with more than the necessary configurations and permissions, and the overall defence-in-depth security was to be strengthened.

"For instance, our encryption keys are now stored in different locations, making it impossible to lock the entire network from any single point within the system. This follows the same logic as not keeping the keys to all your cars in the same safe at the dealership," says Soug.

» If someone managed to breach the first layer, there were too many open paths leading deeper into our network.

Strengthened preparedness

Additionally, the emergency preparedness and contingency planning for IT security needed an upgrade. This was partially addressed by creating standard procedures for handling attacks or incidents.

Bertel O. Steen utilises an ISO-certified management system that covers their entire business. This means there are specific, formal requirements for how actions are to be performed and documented at all levels, including within IT and security.

"These procedures are part of the group's overall crisis management plan, which outlines how different types of crises should be handled. The plan defines specific roles, each with its own tasks and areas of responsibility," Soug explains.

Along with a clear specification of purpose and scope, the procedures include a detailed description of the CSIRT (Computer Security Incident Response Team), along with its members and functions. The procedures also outline how to alert and summon the crisis management team, and the key points that should always be covered in these meetings.

The group has also developed action cards, which describe the different roles in the crisis management team and their respective tasks.

"The action cards are essentially checklists detailing what to evaluate, what to remember for damage limitation, and the steps to take to ensure a return to operations and the resolution of the crisis," Soug says.

The alarm bells sound

However, as the work to implement the new measures and procedures is well underway, the alarm at the SOC suddenly goes off. Telenor has detected suspicious activity in one of the group's login portals.

"We have a solution that allows users to sign in through a website that provides access to a range of applications. The system is designed so that users only see the applications they have permission to access," Soug explains.

By mistake, the solution was momentarily downgraded, making it vulnerable to a security flaw known as Citrix Bleed. In principle, this means that a hacker could take control of an already signed-in user, along with all their inherent permissions.

"We noticed that they had extracted a list of usernames from the login system and installed a couple of trojans, malware hidden in legitimate applications. Fortunately, the security systems quickly detected the trojans, and they were automatically removed."

PHOTO: BERTEL O. STEEN

Cyber defences put to the test

» When you are in the middle of an attack, the situation can feel quite stressful. This is where management systems and action cards come in handy.

The hackers then attempted to sign in to the different applications in the portal. However, they were thwarted by the two-factor authentication requirement.

"When you are in the middle of an attack, the situation can feel quite stressful. This is where management systems and action cards come in handy. They provide an opportunity to double-check what you are supposed to do in any given situation," Soug says.

Today, both the operations and IT departments at Bertel O. Steen have their own incident response teams that handle issues and report to the group's overall emergency response team.

"One of the defined roles in our procedures is that of a log-keeper. This role has a single task: to log all decisions made and the reasoning behind them. This is incredibly important for evaluating our crisis management after the crisis."

Bertel O. Steen's action card for IT security incidents states that systems that are hacked or infected should not be restarted, but isolated. The reason for this is that restarting a system often initiates a standardised setup, which deletes all logs and applications installed on the server.

"Sadly, a mistake was made in this instance. The incident was interpreted as an operating error rather than a security error. The instruction for operating errors is to restart to recover quickly. This made it difficult to uncover exactly what had happened and complicated the handling of the situation."

If Bertel O. Steen had isolated the portal instead, which they had the opportunity to do through the zoning of the network, all the digital traces would have been available after the incident.

Without multi-layer security, the hackers could have easily penetrated deep into the network. There, they could have potentially deleted or downloaded all the customer data in the group or encrypted all their systems.

Soug believes the consequences could have been catastrophic.

Thinking holistically

"Over the next few weeks, we observed thousands of log-in attempts from places like Russia and Bulgaria. Luckily, these largely consisted of blind password guessing, and we saw that they started to give up after a while."

"It is easy to develop guidelines and procedures but implementing them takes time. A structured approach is essential. We now have a security strategy with defined goals for where we should be within two years, encompassing both technical and organisational objectives."

Soug believes it is no longer possible to solve security challenges one by one.

"You have to think holistically. This means that the guidelines need to include everything from hardening—making devices and services more secure by changing their configurations or removing functionality—to training users and obtaining cyber insurance."

"Ultimately, IT security is about business operations. If your systems are affected, it can have a direct impact on both earnings and customer relations. If the systems shut down completely, we are talking about losses in the millions for each passing hour."

"If they are down long enough, it could mean that we lose our most important customers," Soug concludes.

» Ultimately, IT security is about business operations. If your systems are affected, it can have a direct impact on both earnings and customer relations.

PHOTO: MERCEDES-BENZ

PHOTO: TELENOR

4

Safeguarding critical infrastructure with embedded security for emerging risks

How do we ensure trustworthy and reliable mobile networks and critical infrastructure? In this article, we share insights into several aspects related to critical infrastructure and its evolution within the telecoms sector. This includes everything from 5G and the role of mobile networks in critical operations to the emergence of new technologies, such as confidential data processing and compliance with increasingly strict government regulations.

Written by:
Kaël Haddar, Customer Security Director, Ericsson

This article was written in English and has been editorially adapted for publication in Nordic Digital Security 2024.

Telecommunications has emerged as an indispensable facet of contemporary existence, seamlessly bridging individuals across the globe irrespective of geographical barriers. Its impact reverberates through economic development, industrial progression, and global connectivity. Any disruption in service directly impinges upon societal functioning, economic stability, and government operations.

With mobile networks now part of critical infrastructure, additional regulatory requirements have surfaced, necessitating audits and security assurance. The introduction of diverse use cases for connected business and industry will introduce new security and safety dimensions, shaping future research, development, and operational security aspects.

5G, resilience, and security

Governments and businesses are rapidly adopting advanced technologies driven by 5G, aiming for consistent performance and security assurance in mission-critical operations. The backbone of a robust 5G system lies in its ability to maintain uninterrupted availability, reliability, and responsiveness, even in the face of disruptions or attacks. These attributes, including reliability, availability, robustness, and security, not only protect privacy but also ensure continuous service.

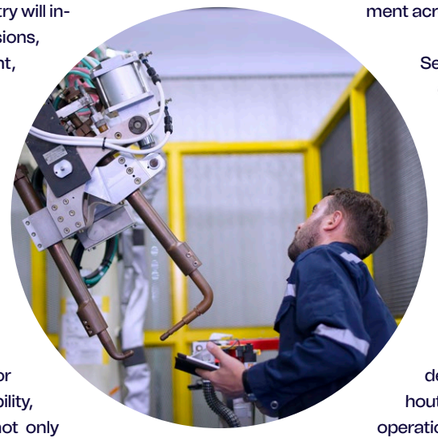


PHOTO: EYESFOTO VIA GETTYIMAGES

As digital transformation sweeps critical functions into the digital realm, telecom networks emerge as indispensable pillars, supporting existing operations while enabling innovative use cases. For example, the rise of remote-controlled machinery demands instantaneous communication, ensuring rapid responses to potential threats.

The landscape of critical infrastructure is swiftly evolving, with intelligent network platforms offering a spectrum of essential properties such as security, privacy, reliability, and robustness, tailored to diverse use cases. As we transition from 5G to 6G, fortifying these networks with advanced building blocks becomes increasingly crucial to ensure their resilience and effectiveness.

Confidential computing emerges as a pivotal technology in bolstering security within virtualised systems. By protecting data during processing and storage, confidential computing instills confidence among users and regulators alike. Its integration into network architectures lays the groundwork for secure identity management and enables automated trust assessment across all network elements.

Secure identities and protocols are another cornerstone of network security, essential for safeguarding communication channels across various industry segments. Evolving technologies like trusted identities, authentication frameworks, and access control management ensure secure communication at every layer, promoting unified identity management and automated data governance.

Furthermore, security assurance and defense mechanisms are pivotal throughout the development, deployment, and operational phases. While current methodologies primarily focus on product security, future solutions will incorporate built-in assurance mechanisms, ensuring compliance with security standards and regulations, for example, regulations such as GDPR (General Data Protection Regulation) in the European Union.

Regulatory landscapes play a crucial role in shaping security and privacy standards within critical infrastructure. Adhering to stringent regulations fosters trust among stakeholders and ensures alignment with evolving security specifications and standards.

» The backbone of a robust 5G system lies in its ability to maintain uninterrupted availability, reliability, and responsiveness.

Navigating the path to resilient networks

As we navigate towards resilient and secure network infrastructures, collaboration, innovation, and regulatory compliance will remain paramount in safeguarding critical assets and driving sustainable growth across industries.

To address the evolving threat landscape effectively, three key development components are crucial for building trustworthy systems. These components drive innovation and resilience, empowering 5G networks to adapt and thrive in an ever-changing environment.

Trustworthiness

Trustworthiness of the wireless infrastructure is built through use of globally agreed standards, strong security solutions, and well-defined processes. This is complemented by threat intelligence, actively and continuously updating on current security threats.

Security at scale

Security at scale includes safeguarding huge volumes of devices and data, for a large variety of use cases. To accommodate this, we research adaptable, scalable, and automated security solutions for future networks and connected devices.

Policy-driven automation

Policy-driven automation that aligns with industry frameworks, together with rule-based analytics (for known threats) and AI-based analytics (for anomalies and unknown threats) will enable holistic and cost-efficient security for future use cases.

Our approach to telecom security is built on four key pillars: **standardisation**, **product development**, **deployment** and **operations**. These four areas contribute toward creating a secure platform that is an ideal foundation on which to build large-scale, security-sensitive systems.

Ericsson has a long history of systematically incorporating security and privacy considerations into all relevant aspects and phases of our product value flow. We follow a well-established internal control framework known as the Security Reliability Model (SRM). The SRM enables a managed, risk-based approach to security and privacy implementation where requirements are tailored to the target environment and demands. This approach helps us meet stakeholders' expectations and cater for the rapid evolution of technology and the continuous changes in legislation globally.

ZTA represents a paradigm shift in cyber-security, rejecting the traditional perimeter-based security model in favour of a more granular and dynamic approach.

Achieving Zero Trust architecture for critical infrastructure

Among the myriad challenges faced by critical infrastructure environments, the interest is increasingly turning towards operational resiliency. Maintaining operational resilience in an era marked by escalating cyber threats, natural disasters, and evolving work patterns poses an ongoing dilemma for numerous organisations. These challenges necessitate a comprehensive approach to security and resilience, encompassing robust protocols, advanced technologies, and proactive risk management strategies.

As threats continue to evolve, both Mobile Network Operators (MNOs) and governmental bodies are actively embracing the concept of Zero Trust Architecture (ZTA) for safeguarding critical infrastructure. ZTA represents a paradigm shift in cyber-security, rejecting the traditional perimeter-based security model in favour of a more granular and dynamic approach. By assuming that no entity, whether inside or outside the network, can be trusted by default, ZTA mandates strict access controls, continuous authentication, and real-time monitoring to mitigate risks and prevent unauthorised access.

However, achieving ZTA entails more than just adhering to industry standards. While the 3rd Generation Partnership Project (3GPP) standards provide a foundational framework for implementing zero trust in areas such as network functions (NFs) and interfaces, operational security often lies beyond the realm of standardisation. Operational security encompasses a wide range of practices and procedures aimed at safeguarding network infrastructure, data, and resources from internal and external threats. This includes regular security audits, vulnerability assessments, incident response planning, etc.

Furthermore, successful implementation of ZTA requires a deep understanding of the unique network context and operational requirements of each MNO. It is essential to tailor ZTA deployment and configuration to align with the specific challenges and constraints faced by the organisation. This involves conducting thorough risk assessments, identifying critical assets and dependencies, and establishing clear policies and procedures for implementing and managing ZTA controls.

Ericsson products have the ambition to offer the necessary capabilities to deploy a ZTA, and we are actively engaged in the ZTA journey alongside MNOs and industry bodies such as the O-RAN Alliance, 3GPP, and ATIS. Realising a ZTA that aligns with all the NIST seven principles of zero trust and CISA ZTMM requires a high degree of automation and visibility in mobile network security operations. To this end, Ericsson provides a security management solution designed to automate and orchestrate security operations, thus fortifying mobile networks against external and internal threats.

Need for continued collaboration across the industry

It is evident that achieving a robust security posture in deployed networks requires a multifaceted approach that goes beyond standardisation efforts alone. With the increasing importance of critical infrastructure security and privacy needs, coupled with evolving regulatory perspectives, it is imperative for industry stakeholders to collaborate effectively on cyber-security implementation.

This collaboration effort should of course prioritise business outcomes in network performance and availability but also embrace the principles of Zero Trust Architecture (ZTA).

By consolidating security controls and offering comprehensive recommendations, these types of initiatives pave the way for the industry to successfully realise the three key development components that are critical for building reliable systems and ZTA in 5G networks - trustworthiness, security-at-scale, and policy-driven automation. Moving forward, continued collaboration and alignment with regulatory frameworks will be essential to ensure the resilience and integrity of mobile networks in the face of evolving threats.

PHOTO: ISTOCK.COM / SANDY BELL

5

The Nordic threat picture

With threat levels on the rise due to geopolitical tensions and the increasing capabilities of threat actors, Telenor is in a constant state of readiness. For us this means maintaining a systematic approach to the threat landscape, while keeping a firm eye on all indicators of potential attack. Today's threat landscape also requires us to have continuous focus on resilience building across all parts of the company and among our people. In this chapter, we examine the current Nordic threat picture as seen through the lens of Telenor's security experts.

Left: Telenor's presence in the Arctic places higher demand on the need to assess security, preparedness, and threats.

PHOTO: DAVID MERRON PHOTOGRAPHY VIA GETTY IMAGES

PHOTO: TELENOR

Staying on top of the rapidly evolving Nordic threat landscape

The telecommunications industry is considered an attractive target for threat actors, consistently ranked among the top three by intelligence agencies. This ranking underscores the industry's strategic importance and the high stakes involved in safeguarding its networks. Companies in this domain have access to a substantial amount of sensitive data and can operate as digital gateways to other potential targets. On top of that, the industry's attack surface is larger than in most other industries, and some telecommunications companies own, operate, and safeguard national critical infrastructure, which is essential for daily life.

Telenor is one of the largest Nordic providers of content, telecommunications, and data services. This makes Telenor an especially attractive target, both due to its symbolic value and broad customer base.

The threat landscape presented in this chapter takes a holistic view on Telenor's security challenges. It considers the intentions of potential threat actors in relation to Telenor's customers, including private customers, corporate customers, businesses, and national authorities. As such, this perspective recognises the importance of understanding the values of our customers, which Telenor takes part in protecting.

» In Europe, the security situation is now more dangerous than it was a year ago.

In Telenor, we systematically gather security information from a diverse range of sources and use it in our broad internal security network. This information includes assessments by national authorities in our operating regions, open-source reports from major security companies, and data from partners and commercial threat intelligence services. In addition, we leverage insights from our company-wide threat communities and their extensive networks. This comprehensive approach ensures we consistently build knowledge and awareness about current and emerging threats targeting both Telenor and the broader telecommunications industry.

The rapidly changing geopolitical landscape requires us to continually align our defences with the evolving threat landscape. This alignment enables us to implement the most effective security measures, ensuring the protection of both Telenor and society during uncertain times. Since Telenor owns and operates critical infrastructure across the Nordics, a serious security incident could have severe consequences for the entire region. Therefore, we place great emphasis on continuously assessing and updating our understanding of threats.

A worsening threat picture

The threat situation in the Nordics has undergone significant change in recent years, with increasing geopolitical tensions that will continue to affect the region. Managing this requires robust preparedness, up-to-date understanding of the situation, and well-prepared solutions.

The year 2024 is marked by a continued escalation in global uncertainty in the digital domain, with states actively employing cyber operations to advance national interests. The growth in geopolitical tensions, especially between the major powers, creates a complex and dynamic threat landscape. Attacks by state-sponsored actors, which were previously directed at specific strategic targets, are becoming increasingly diversified and extensive. With technological development also comes new opportunities for threat actors, as well as more areas to protect. Both state and non-state threat actors are rapidly adopting advanced technology to use to their advantage and are more targeted in their attempts to achieve their goals. The ability to quickly adapt to changes in the threat landscape is more important than ever.

European security during wartime

In Europe, the security situation is now more dangerous than it was a year ago. This is primarily due to Russia. Factors including whether Russia will increase its military build-up in the coming years, and the outcome of the war in Ukraine, will influence the security situation in the Nordics. This directly affects how we work with security in Telenor Nordics. The security of Telenor Nordics not only applies to our company and our customers, but it is also critical for the region's ability to communicate in any situation. In times on conflict, such as now, it is critical that this is prioritised.

Building greater resilience among Nordic critical infrastructure

Telenor Nordics continues to upgrade its national infrastructure to withstand increased digital threats. Our efforts to secure both the private and public sectors play a critical role in this context. In line with the evolving threat landscape, co-operation in the Nordic defence and security sector is being strengthened, as well as in the private sector. The intention is to ensure robust communication networks and critical infrastructure adapted to the current situation. The heightened threat to critical infrastructure can affect Telenor both directly and indirectly. The dependencies in critical infrastructure are significant. Outages in Telenor will directly impact many other parts of the Nordics – while outages in other parts of critical infrastructure could affect our operations, such as in power and utilities. As a result, our resilience is more important than ever before.

New opportunities stem from stronger Nordic presence in NATO

Recent initiatives to bolster security and defence co-operation in the Northern Nordic region highlight the importance of a co-ordinated response to emerging threats. For instance, the enhanced co-operation between Norway, Sweden, and Finland, particularly following the latter two countries' NATO membership, underscores a historic shift in Nordic security policy. This collaboration is crucial for protecting our infrastructure and ensuring that we are prepared to face any challenges that may arise. As part of this effort, both public and private sectors are working together to strengthen the resilience of our critical systems, ensuring the stability and security of our region in these uncertain times.

Finland exemplifies close co-operation between the public and private sectors in continuity management, resilience, and crisis management, a practice honed over decades and further developed in response to recent geopolitical changes. The importance of critical infrastructure has always been integral to overall security and continues to be developed with national authorities and critical service providers, including telecom operators.

Finland's strong defence capabilities and investments, alongside Sweden's accession to NATO, significantly enhance the Nordic security landscape, boosting collective defence and interoperability. Both countries possess high levels of technological and scientific expertise, making them prime targets for corporate espionage. The Finnish Intelligence Service has highlighted corporate and public sector espionage as a major concern. Consequently, it is crucial for entities such as Telenor's operation in Finland (DNA), to ensure the safety of their customers and services, fulfilling their social responsibility by continuously developing operations and services to secure societal functions in a rapidly changing world.

Threat actors target broader scope of sectors

For our customers, the need for secure and reliable methods of communication is increasingly vital. Telenor Nordics has many customers within areas such as specialised technology, engineering, and science sectors, all of which are attractive targets for industrial espionage. This requires increased security, which is cause for concern, as these sectors typically do not have the same security culture as, for example, the defence industry. Addressing this requires strengthened infrastructure from Telenor to meet the new requirements of these companies.

In recent years, we have also observed not only societal changes that affect the prerequisites for the threat landscape, but also that the threat actors' room to manoeuvre, risk appetite and capabilities are changing. This impacts how increased digitalisation and technological development are utilised, potentially amplifying risks and complicating security efforts.

Changing the rules of the game: Hybrid warfare

The changes we are now seeing in Europe affect the security and the priorities that we set. The situation is more unpredictable, unstable, and dangerous than before. What many previously perceived as theoretical concepts such as "hybrid warfare" or "grey zone tactics" are now incorporated into security assessments. The conflict in Ukraine has demonstrated that hybrid warfare is not a new phenomenon but rather a pressing reality that necessitates our immediate attention and response.

Hybrid warfare combines conventional military force with irregular tactics, cyber operations, and disinformation to destabilize a target. This strategy includes guerrilla tactics, cyber-attacks, and spreading false information to create confusion and weaken the target without triggering a full-scale military response. The aim is often to achieve strategic goals while maintaining plausible deniability.

Grey zone activities are actions that exist between war and peace, such as economic pressure, cyber-attacks, and political manipulation. These tactics are designed to undermine a target's stability and sovereignty without crossing the threshold that would justify a direct military response, making them difficult to counter.

The rise of adaptive and opportunistic cybercriminals

In Telenor, we observe an increase in resourceful, opportunistic threat actors in the digital domain who can quickly change their tactics and adjust their methods to tailor attacks against our company and our customers. Criminal actors with financial motives continue to exploit the opportunities that lie in societal changes and technological development. They increasingly customise their attacks on our company and our customers, and they employ new technological methods to streamline their attacks.

Increasing instability in supply chains

The increased geopolitical turbulence can also lead to supply chain disruptions, resulting in greater supplier complexity or requiring immediate replacement of subcontractors. This can lead to instability, thereby increasing associated security risks. The level of conflict is also increasing in the Middle East and parts of Asia. Regional conflicts can quickly affect security of supply. This can affect access to specialised technology, in the form of availability of goods on ongoing contracts in other parts of the world, and it can increase delivery times due to trade routes disruptions and delays. A steady and resilient supply chain is becoming both more difficult, and more important, to maintain.

Disguising attacks as human error

Security-threatening incidents that are designed to appear as forgivable errors - for example, sabotage that is designed to look like a failure of equipment with an unknown cause - are expected to become more common in the future. This trend is increasingly seen in Europe, often related to critical infrastructure. Europe has in recent years experienced several suspicious incidents involving physical sabotage of critical infrastructure. This included the sabotage of communication cables in Germany in 2022, resulting in major train disruptions, and in France in 2024 when fibre optic cables were sabotaged in parts of the country, causing significant disruptions. These actions are often seen as warnings or retaliation against countries that support Ukraine. Infrastructure such as pipelines and subsea cables are particularly vulnerable to physical sabotage, and we have witnessed state actors that are willing to carry out such operations to destabilise the region and send political signals to the West.

No one is actually untouchable

In early 2024, Ukraine issued an ominous warning to the West: "No one is actually untouchable." The head of the country's cyber-security department revealed that Russian hackers brought down the country's telecoms giant Kyivstar in December, causing more than 24.3 million customers to lose phone reception. The attack was attributed to Sandworm, a Russian military intelligence cyberwarfare unit, which had been lurking in the system for several months undetected, Ukrainian officials said.

Sources: *Timeline: POLITICO (Timeline: Europe under cyber siege in 2024 & Ukraine says Russian hackers penetrated major telecoms network for months).*

Outlier events indicate potential security threats

To identify hybrid threats, it is important to monitor activity outside the norm, especially in relation to frequency and consequence. This is particularly important in Telenor's northern- and eastern-most regions.

We are also closely monitoring any changes in normal day-to-day operations. By benchmarking changes against what is typical, we can identify peculiarities and outliers that may indicate threatening changes in the security environment. Since many of our customers and suppliers are dispersed across the Nordics and play very important roles in critical functions, detecting these changes is key to ensuring the security and resilience of our operations.

Increased vulnerability in the Nordics

The Nordic region has become increasingly vulnerable with war in its vicinity and active support of Ukraine. The increased Nordic contribution, both financially and with ready-to-use equipment for Ukraine, has increased the threat profile for the region.

This has positioned us as a target for more severe and destructive cyber-attacks, both by nation state hackers, as well as rogue groups, that sympathise with Russia. The increased pressure has prompted Telenor Nordics to prioritise certain security efforts, at an increased pace.

Further escalation of the security situation in Europe will likely increase the threat of destructive sabotage, whether physical or logical, that could directly or indirectly affect Telenor. We must address this uncertainty with robust systems, effective detection and a contingency mindset.

Military and political signalling are foreign policy means of pressure where the threat actor hints at their capabilities and carries out actions to imply an unspoken threat. This strategy is also used to create fear and uncertainty with the aim of influencing political decision-making, and public opinion without having to use military means in such a way that it can trigger war. It is more likely that Telenor will be (directly or indirectly) affected by security incidents by state actors in the current situation than earlier years. This is why we continuously emphasise Nordic co-operation and collaboration within security and operations.

Russia-linked cyber actors have increasingly carried out targeted attacks against European infrastructure since the war in Ukraine began. According to the EU-NATO Task Force on the Resilience of Critical Infrastructure, Russia has demonstrated that it sees critical infrastructure as a target through its actions in Ukraine. The Task Force also states that Russia is mapping critical infrastructure in the Euro-Atlantic as potential targets. The attacks that are focused on critical infrastructure and public institutions often have a stronger political dimension than before. When Distributed Denial of Service (DDoS) attacks are used, they are often executed by so-called "hacktivists". Such coordinated DDoS attacks have also been seen in the Nordic countries, often associated with activity or political decisions that Russia opposes. Other targets have included companies that actively contribute to supporting Ukraine in the war.

» Europe has in recent years experienced several suspicious incidents involving physical sabotage of critical infrastructure.

PHOTO: NIGEL KILLEEN / GETTYIMAGES

The strategically important North and East

For Telenor, it is necessary to evaluate the different regions in the Nordics in terms of inherent geographical risk. Although we largely rely on the comprehensive and national backdrops presented by the Nordic intelligence and security services in their annual unclassified threat assessments, we also see a need to take a closer look at our most vulnerable regions: the High North and the Baltic Sea area.

For us in Telenor Nordics, it is extremely important to be observant of local conditions that can impact the services we provide. Given the current security situation and the authorities' warning about which sectors of society most at risk, we are especially focused on our customers in the High North and Baltic Sea areas. These regions are subject to different aspects of Russian interaction, requiring heightened vigilance.

Telenor Nordics has an active presence in Arctic regions. Operating a reliable service in the North is not only important for our customers, but an important part of Telenor's social responsibility. In practice, we need to assess security, preparedness, and threat analysis - with a special focus on the northern regions of Norway (including Svalbard, Jan Mayen and Bjørnøya), Northern Sweden and Finland. The security situation here is more closely linked to events in Russia than in any other region in which we operate. This is a daily reality for our companies, and it's also the feedback we receive in our dialogue with local authorities.

In Svalbard, Telenor is in a unique position as one of the largest, most important and longest-established companies. Telenor's position and operations in Svalbard is likely of great interest to other countries that also have a presence here or wish to establish themselves in the region. Finland's long border with Russia brings unique challenges for critical infrastructure. For example, Northern Lapland and Åland are subject to special risk management and threat assessments due to their geographical location. For all our northern regions, we consider that Telenor's activity will be of greater interest to foreign states than before. This is likely to result in increased intelligence pressure – especially from Russian and Chinese actors.

The Arctic areas not only have climate conditions that require particularly robust services and follow-up, but they also have greater potential for sensing security policy tensions, which demands extra vigilance. At a time when infrastructure in Europe is under a higher threat level than before, with Russia, in particular, considered to pose a hybrid threat, we are closely examining our critical infrastructure and how it is linked to other critical infrastructure. The interdependencies between different parts of critical infrastructure require thorough preparedness.

Both Russia and (increasingly) China are important players in the High North. Their presence underscores the need for heightened security measures and continuous monitoring to protect our interests and maintain the integrity of our operations in this strategically significant region.

Climate change is causing the ice to melt faster, opening new sea routes. An increase in both military and civilian traffic in the High North enhances its strategic importance, especially for a country like Russia. An increased military presence from both allied states and Russia means that this area has the potential to become even more tense from a security perspective.

The Baltic Sea area is another area where Telenor operates, and where we pay close attention to the developing security situation, especially following the Russian invasion of Ukraine. This area has experienced several security incidents targeting transnational communications cables, as well as oil and gas pipelines. Subsea infrastructure, vital for communications between countries, is increasingly vulnerable to sabotage and other security threats.

While the geographical footprint of Denmark is relatively small, our eastern-most borders in the Baltic Sea is cause for caution since the NordStream2 incident in 2022. There are several communications cables connecting Denmark, Sweden, and Germany that are at risk, highlighting the need for well-defined contingency plans.

The focus of Nordic governments and NATO on critical cables has increased, and special attention is now paid to the resilience of transnational cable connections connecting and expanding from the Nordics. This increased vigilance and collaborative effort aims to enhance the security and reliability of these vital communication connections.

The top 7 changes we see in cyber-security

1) Blurring the lines between state and non-state actors

The distinction between what is state actor and what is non-state actor is becoming less clear – as state actors use non-state actors to hide their association with malicious acts, and because methods are shared between them. This means that we can no longer confidently predict which methods will be used against us based on which players we believe are of interest to Telenor. Nevertheless, we can make several generalisations that are relevant to security thinking in the cyber domain. The threat actors that are active or may conceivably be active against companies such as Telenor may be interested in everything from creating disruptions to targeted intelligence gathering, including reconnaissance of networks for possible destructive attacks.

2) Rise of cybercrime for profit

We see an increase in attempts to defraud Telenor Nordics and our customers. This trend is closely tied to technological development. The development of digitalised threats has accelerated sharply, making cybercrime more prevalent and sophisticated. Technological progress and professionalisation of cybercrime have made it easier for threat actors to access and utilise advanced tools and techniques. Previously, attackers needed their own technological expertise to carry out attacks. Now, they can more readily buy this as services from professional criminals. This shift has significantly broadened the scope and impact of cyber threats.

3) Evolving ransomware threats

Ransomware continues to be a significant threat to all businesses. This development requires a strengthened response from businesses through advanced detection and recovery systems and strengthened internal (and possibly external) preparedness. These attacks are happening faster than ever, and the ability to detect, report, and deal with them is more important than ever. Previously, ransomware primarily involved encrypting networks to demand a ransom. Now we also see this is combined with threats to sell the encrypted information. It is important to emphasize that paying a ransom does is not guarantee the safe return of the information or the integrity of data. Therefore, businesses must prioritise robust security measures and incident response plans to mitigate these risks effectively.

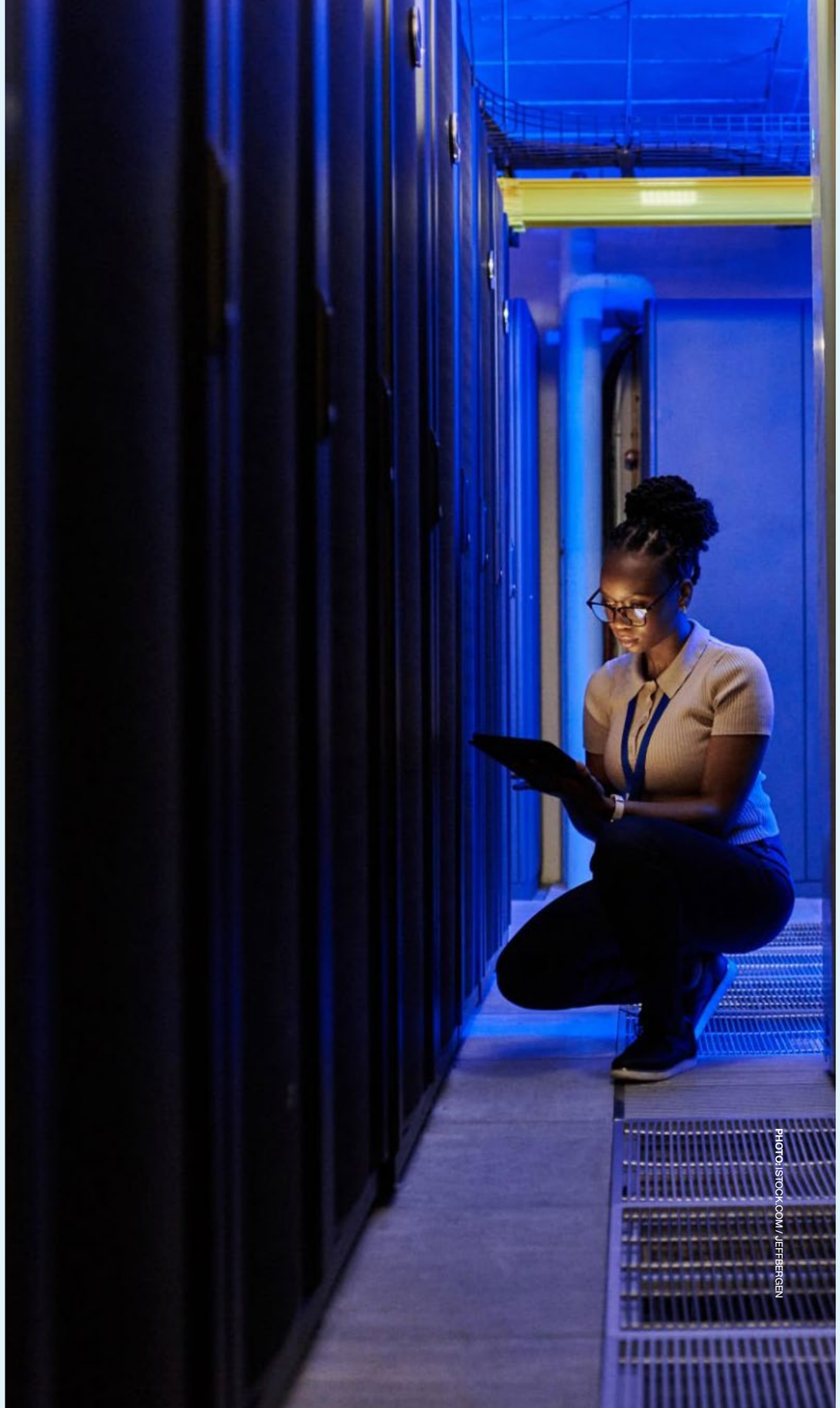


PHOTO: ISTOCK.COM/ JEFFBERGEN

4) Increase in social engineering attacks

As with many other forms of security threats, we are also seeing an increasing use of targeted attempts at social engineering to gain an initial foothold. We have less and less time to detect and respond to digital attacks, hence much of the preventive work lies in a good security culture in all parts of the company. At Telenor, this is something we work on actively every day to ensure that all employees are aware of and prepared for potential security threats. Social engineering has enabled threat actors in other parts of the world to acquire legitimate identification to log on to networks and carry out significant ransomware attacks. Such login is more difficult to detect, as it requires recognising abnormal behaviour or traffic in the network. Reliance on malware detection alone is no longer sufficient. Awareness campaigns and strong protection and verification of identity at login are particularly important. A compromised login method that grants access to networks can cause great damage.

5) The evolution of phishing and spearphishing

To gain access to a foreign network, we also see that threat actors continue to use phishing or spearphishing (targeted phishing). Phishing as a method is constantly evolving and will likely continue to be adjusted to bypass changing security recommendations. We are observing a variety of methods, with some of the latest including the use of QR codes in targeted email and using iMessage for attacks. Moreover, phishing attacks are increasingly incorporating elements like social media impersonation and deepfake technology to deceive targets more effectively. Attackers may create fake social media profiles to build trust before launching phishing attacks or use deepfake audio and video to impersonate trusted individuals. These developments make it even more crucial for organisations to not only focus on technological defences but also to foster a strong security culture where employees are vigilant and aware of these sophisticated tactics.

6) Threats to cloud infrastructure

As the adoption of cloud services continues to accelerate, cloud infrastructure has become an increasingly attractive target for threat actors. These adversaries often exploit “legitimate entrances” such as compromised credentials, misconfigured settings, or vulnerabilities within third-party applications to infiltrate and manoeuvre within cloud platforms. This makes it challenging to detect security breaches and underlines the need for strengthened network monitoring and response strategies specifically adapted to cloud technologies.

7) State actors and advanced techniques

To the extent possible, state actors and their proxies use the same methods as other actors to access (steal and/or encrypt) information or to make systems unavailable. State actors use their advanced methods such as zero-day vulnerabilities, which are unknown software vulnerabilities that allow attackers to bypass existing security measures undetected. However, using zero-day carries the risk that these will be revealed and neutralised. For us, it matters less who is behind the attack. Whether it is a state actor or a rogue group, we must be able to handle it regardless.

A constant eye on the threat picture

Continuous prioritisation and updating of which threats currently used in the cyber domain is important to have relevant protection. Reducing reliance on outdated systems that no longer receive updates and ensuring rapid patching of vulnerabilities are essential strategies.

A reminder of this occurred in the summer of 2024, when a faulty software update from CrowdStrike led to a global IT outage. This incident affected over 8.5 million devices, grounded thousands of flights, disrupted hospital systems, and knocked banks and media outlets offline. The widespread chaos underscored how critical it is to keep systems updated and patched to mitigate such vulnerabilities and prevent significant disruptions.

A proactive approach helps mitigate risks and ensures that our security measures remain effective against evolving threats.

On the lookout for indicators of mapping

Indicators are the "tracks" we follow to come to the right conclusion in our security work. Assessing safety reports and analysing what this says about a situation is important. When we in Telenor detect indicators that someone is mapping our business, it is taken very seriously. Mapping activities can involve actions such as taking pictures of an installation or suspiciously contacting employees. The indicators can appear both in the digital and physical domains. Since mapping has no immediate harmful effect, there is a risk that it will be overlooked and downgraded in favour of more immediate needs. However, recognising and responding to these indicators is essential for maintaining security. Mapping is often among the first steps a threat actor takes before further action.

While mapping does not automatically mean a malicious act will be carried out, it can suggest that someone is planning or creating the impression that such actions are possible. Threat actors might engage in repeated mapping to gather information for potential future use, giving them the ability to strike when desired. Indicators of mapping, whether in the physical or digital domain, must be taken seriously. Mapping is done for a reason, and can provide valuable insight into how to manage security work. Although some mapping may be done to disturb or draw attention elsewhere, its occurrence indicates potential interest from a threat actor. Given the current security situation, it is important to take mapping indicators very seriously.

Raising awareness among employees, customers, and suppliers is important in order to receive reports of "suspicious incidents" and to be able to identify whether mapping is in progress.

» Raising awareness among employees, customers, and suppliers is important in order to receive reports of 'suspicious incidents'.

Preparedness has never been more critical than right now

Protection of critical infrastructure will always be essential for a society to function optimally, as is preparedness for situations in which society is under pressure. This helps businesses become more resilient to complex threats.

Contingency planning is an absolute necessity in today's environment where hybrid threats are high on the agenda. This is not only something that companies should do, but also something that all employees should think through.

Reflect on these questions: Do you know what to do if your company is exposed to a ransomware attack tomorrow? Do you know what to do if critical services go down? Where do you meet up? What is your role?

At Telenor, we are constantly working on these issues to ensure that the communication solutions we deliver will be available and reliable over time. We are also looking at how we will operate if those who provide services to us are no longer able to do so.

As an operator of critical infrastructure and provider of services critical to society, we see our business continuity as an imperative. By maintaining a robust approach to both infrastructure protection and individual preparedness, we aim to ensure that our organisation, customers, and society at large can withstand and quickly recover from any disruptions or threats.

PHOTO: ISTOCK.COM / UNISELLER

PHOTO: ISTOCK.COM / IGNATIEV

6

The booming cybercrime business

Cybercrime is poised to surpass illegal drugs as the primary source of income for criminal networks, according to experts. Here, we shed light on some of the methods used in digital crimes against Nordic consumers and businesses today.

What we've seen so far in 2024

Phishing-as-a-service fraud tools served on a silver platter

Fraudulent text messages are sent via the internet to bypass security filters

Exploiting stolen usernames and passwords and targeting edge devices for cyber-attacks on Nordic businesses

Eavesdropping equipment used to scam private individuals

Safe-account fraud social manipulation to make you to think the criminals are from the police or bank

Prevailing Nordic fraudulent SMS and calls 56.6 million fraud attempts via SMS and calls blocked in Norway alone in first half of 2024

Generative AI opening new shortcuts for scammers

Scammers exploit updated LinkedIn information

Left: Telenor blocks millions of fraud attempts for its customers across the Nordics each year. The image is an illustrative photo.

Last year, when a Malaysian citizen was arrested in the Norwegian capital Oslo with a car filled with surveillance equipment, the Norwegian Police Security Service (PST) assumed it was a case of espionage.

However, it turned out to be part of a massive SMS fraud and a new method to bypass existing security filters.

Over the past year, cybercriminals have adopted an increasing number of non-traditional approaches to reach their victims, whether they are businesses or average individuals on the street.

Many of the individuals behind these phishing attempts and frauds are new as well. With significant help from AI, among other tools, new fraudsters connected to criminal networks are emerging across the Nordics.

Rise in fraudulent SMS and calls

The vast number of fraud attempts blocked by Telenor in the Nordics each day is clear proof of how big and serious a problem online crime is.

The people behind these fraud attempts are well-organised criminal networks that possess both the competence and resources to carry out sophisticated attacks on a large scale.

In Norway alone, Telenor blocked an astonishing 56.6 million attempts via text messages and calls in the first half of 2024.

In a survey conducted by YouGov on behalf of Telenor in March 2024, 1 in 2 Norwegian adults responded that they had experienced an attempt of digital crime in the first half of the year. In Finland, spam messages, fraud and phishing (SMS and email) are on top of the list of digital crimes experienced or seen as the biggest risk amongst consumers, according to DNA's annual Digital Life 2024 survey.

This data illustrates the pervasiveness of cyber threats and underscores that fraud is a lucrative source of income for criminals, and many will go to great lengths to bypass the security measures set up by Telenor and other businesses. Criminals are constantly developing new methods and going to greater lengths to harm businesses and customers.

These findings are consistent with broader trends across the Nordic region, where digital security is a significant concern due to the region's advanced technological infrastructure. With a highly developed digital economy, the Nordics are particularly vulnerable to such attacks, making robust security measures and continuous vigilance critical.

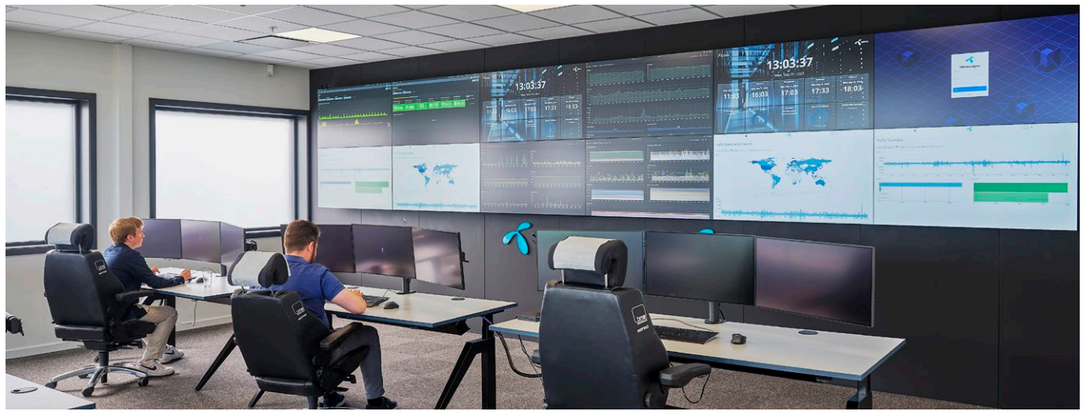


PHOTO: HARALD SØLKAVIK

A positive development can be seen in Finland, where the authorities, telecom operators, and financial sector are collaborating closely to prevent the use of Finnish fixed and mobile telephone numbers in fraud and to reduce the number of foreign scam calls and SMS. The effort is based on three pillars: a technical solution validating if the call or SMS is legitimate or from a scammer, the implementation of regulation[1] from the Finnish Transport and Communications Agency, Traficom, on the interoperability of communications networks and services, and lastly, filtering by all Finnish telecommunications operators.

In addition to this, during spring 2024 Traficom has enabled the registration of protected SMS Sender IDs. This allows for example banks and financial institutions sending out SMS to Finnish citizens to register their SMS Sender ID in order to make sure that no one else can use the same one to falsify sender information.

While these national efforts are crucial, the broader European regulatory environment is also evolving to address these threats. The European Commission's proposed third Payment Services Directive (PSD3) aims to harmonise the regulation of payment services across the EU. If adopted in its current form, PSD3 could strengthen fraud and consumer protection in our region. One of the key proposals includes fostering stronger co-operation between payment service providers and telecom operators to combat "spoofing" scams, where fraudsters impersonate employees in payment institutions. By encouraging this collaboration, PSD3 aims to ensure that both sectors work together more effectively to detect and prevent fraudulent activities, thus providing an additional layer of security for consumers. Further, PSD3 would also provide a robust legal framework for businesses to voluntarily share fraud-related data, further bolstering efforts to the monitor and prevent financial crime.

How businesses are being attacked

Our Security Operations Centres (TSOC) are critical components of efforts to protect business customers' networks and equipment through monitoring, detecting, and responding to security threats. Recently, Telenor's security centres have been handling an increasing number of serious incidents per month on average.

This includes both the prevention of ransomware attacks, and the removal of so-called "information thieves" in the network, which are being used by criminals to extract lists of usernames from the company's network. As the value of crypto-currencies rise, we also note an increase in cryptojacking, where crypto-mining malware is attempted placed on a device to exploit the machine's resources.

In addition to these attacks, we have also registered an increase in DDos attacks (distributed denial-of-service attacks) in the Nordics since the start of the Ukraine-Russia conflict. DDoS attacks aim to overload and paralyse servers and networks by flooding them with excessive traffic, thereby disrupting normal operations and potentially causing significant downtime for businesses.

In the last year, our security centres have registered two particularly important trends in the ways businesses are attacked:

1) Stealing employees' usernames and passwords

One of the most widespread methods used to attack businesses involves criminals taking control of and exploiting legitimate user accounts, rather than exploiting system weaknesses.

Examples of how this is done:

- Attackers use leaked passwords from data breaches within other services, and match these with users who utilise similar passwords for their work accounts
- Attackers try their luck with the most commonly used passwords across thousands of user accounts within different businesses
- An employee is tricked into installing an "information thief" on their computer, which copies and sends out login details and session cookies to the attacker
- An employee is tricked into submitting their username and password through a phishing scam

If the business utilises cloud services, such attacks can have serious consequences, as the attacker could gain access to many different systems through a single account.

To withstand these threats, businesses should implement measures such as two-factor authentication, hardware keys, certificate-based authentication, and passkeys with biometric sensors for PC and mobile devices.

1 Update of Traficom's Regulation 28 on the interoperability of communications networks and services.

2) Getting in through *edge devices*

Another method currently used by attackers is to actively target so-called edge devices within a business' network.

These are endpoints in the network that are directly exposed to the internet, often because both employees and partners need easy access to documents and other information.

These include virtual private network (VPN) endpoints, mobile device management (MDM) servers, email servers and file-sharing servers. Many of these have limited security systems and can be compromised very easily.

After gaining access through such a unit, attackers can extract lists of usernames and gain deeper access to the network.

To protect against this kind of attack, it's important to have strong access controls and cloud monitoring. In addition, a good tip for businesses is not have more endpoints with open network access than are absolutely necessary.

As shown in Figure 1, to protect against attack continued Threat Assessments are used to prioritise defences through kill chain analysis, using MITRE ATT&CK® to bind the threat landscape with frequency of identified methods of compromise.

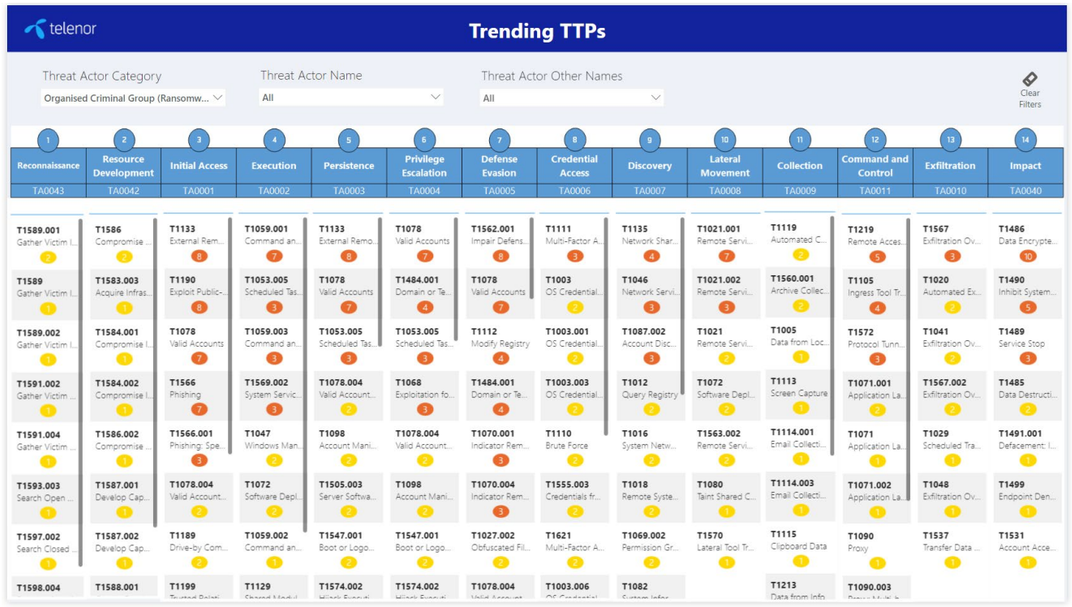


PHOTO: TELENOR

Figure 1: Binding between the threat actors TTPs (Tactics, Techniques and Procedures) and mitigating controls

Scammers exploit LinkedIn information

More recent fraud attempts indicate that criminals are paying close attention online to exploit newly available information to attack businesses and private individuals. Telenor has experienced that information from LinkedIn, in particular, is frequently used for this purpose.

The approach occurs almost in real time: Shortly after an employee has updated their profile with a new title, the employer's HR department is contacted by criminals impersonating the employee.

In the email, the HR department is asked to update the employee's stored information with a new account number. When payday comes, the employee's wages are mistakenly transferred to the account, which is controlled by the criminals.

A similar method, where fresh information is also used for scamming, has been used several times when people sell their used cars. In cases from Norway's biggest online marketplace, Finn.no, the victims receive a false message from the Norwegian Public Roads Administration (Statens Vegvesen), instructing them to pay a fee as part of the sale or the transfer of registration.

Eavesdropping equipment used to scam private individuals

Among the tools and scam methods that were used in attacks against private individuals in the last year, we also find QR codes, artificial intelligence, new online services – and in the case of the aforementioned Malaysian citizen – an IMSI catcher.

The reason the Malaysian citizen drove around with eavesdropping equipment in the car was not to spy on the authorities or private citizens. He did it because it allowed him to send text messages to passersby without using the mobile network.

By using a so-called IMSI catcher, he created a direct connection to all of the nearby mobile phones. In this way, he was able to bypass Telenor's security filters – as well as AI and SpamShield technology.

Many of the recipients of the messages were just random passersby who were busy with their holiday shopping. This increased the likelihood that people would be inattentive and thus respond quickly and uncritically to messages about undelivered packages or unpaid bills.

How the IMSI catcher was used

- **An IMSI catcher** is a type of false base station used for surveillance of mobile communication by breaching the communication between mobile phones and the real base stations. IMSI stands for International Mobile Subscriber Identity, which is a unique identifier associated with every mobile phone that connects to a cellular network
- **It is generally illegal** to use such equipment for anyone other than authorities that have been granted special permission
- **The device is often used for eavesdropping** and espionage, but it can also be used to distribute text messages without using the mobile network. Essentially, the IMSI catcher tricks nearby mobile phones into connecting to it, enabling the interception and monitoring of communications and data from those devices
- **Last autumn, a Malaysian citizen** was detained for having used an IMSI catcher in a vehicle to distribute fraudulent text messages to passersby in Bergen and Oslo, Norway
- **People in the vicinity** of the IMSI catcher received a text message, seemingly coming from DHL, or the Norwegian banks DNB and Bank Norwegian. These messages led the recipients to a false website that requested their card information or prompted them to sign in with BankID, a personal electronic identification method in Norway

Currently, there is little indication that such equipment is actively being used by criminals on a large scale. Nevertheless, it illustrates how new methods are being used to bypass security mechanisms in mobile networks and in IT systems.

Text messages sent online: iMessage and RCS

Although Telenor blocks millions of digital fraud attempts every month, the increased awareness among Nordic people regarding suspicious links and security functions that block fake websites has made it more challenging for criminals to reach their victims this way.

This has led to many opting to use QR codes instead of links when they try to lure victims to fake websites.

However, a text message on the mobile phone is the most attractive and efficient bait to trick people into giving up their personal information – simply because many still fall for it.

As a result, the number of blocked fraudulent text messages has surged significantly. However, criminals are adapting to these defences. When Telenor blocks text messages with links to fake websites, criminals quickly try to find new ways to reach their goals.

This has led to a notable increase in fraud attempts via alternative messaging services. In other words, if you receive a suspicious message through iMessage (on iPhone), RCS (on Android) or WhatsApp, you should be extra cautious.

Messages sent through iMessage or RCS (Rich Communication Services) on Android phones are sent with end-to-end encryption via the web.

The reason fraudsters target these channels is that Telenor and other operators are unable to block these messages, because they, like messages sent from an IMSI catcher, are not coming from the mobile network.

Use of QR codes in Denmark

QR codes have been increasingly utilised by scammers globally to carry out phishing attacks and other fraudulent activities. These scams often involve placing fake QR codes in public areas.

In recent developments, QR code scams have emerged as a threat in Denmark. The Danish police have in June 2024 issued warnings after incidents of fraud were reported at charging stations for electric vehicles. Scammers have been placing fake QR codes over the legitimate ones on these charging stations. When unsuspecting users scan these codes, they are redirected to fraudulent websites designed to steal their payment information or personal details.

These scams exploit the trust that people place in QR codes as a convenient way to access services quickly. By mimicking legitimate websites, these fraudulent sites can easily deceive individuals into entering sensitive information, such as credit card numbers or login credentials. This trend highlights the growing need for vigilance when using QR codes, especially in public spaces where scammers may easily tamper with legitimate services. The Danish police advise the public to double-check the URLs they are directed to after scanning a QR code and to be cautious of any requests for payment or personal information that seem out of place.

Source: *https://www.dr.dk/nyheder/indland/politiet-advarer-mod-qr-svindel-efter-snyd-paa-ladestandere*

Phishing via undelivered packages still the most common

The content you will find in phishing messages distributed on alternative channels can be about anything from exciting job offers to unpaid debt collection claims.

Messages about undelivered packages or a problem with an online order remain the most common ones. These messages are often used as the first part of both simple and more elaborate frauds.

A typical approach is to trick the recipient into thinking there has been an error regarding an order or a delivery, and then lure them onto a fake website or to a conversation with someone posing as a member of customer service.

This is where the victim will likely be tricked into giving up sensitive information such as credit card information or ID credentials. In some cases, scammers also use this opportunity to gain remote control of the victim's computer and access further personal data.

Even if phishing through messages about undelivered packages is not a new thing, it remains an effective tactic for the scammers. This is why they are constantly refining the approach.

Tax refund scams are also widespread, with phishing emails and SMS messages mimicking the Finnish Tax Administration to steal banking credentials. The fraudulent messages often include links to realistic-looking phishing sites that collect personal information. These types of fraud are linked to organised crime networks that are increasingly combining digital tactics with traditional criminal activities. Finnish authorities, including NCSC-FI, continue to warn the public and provide guidance on staying safe.

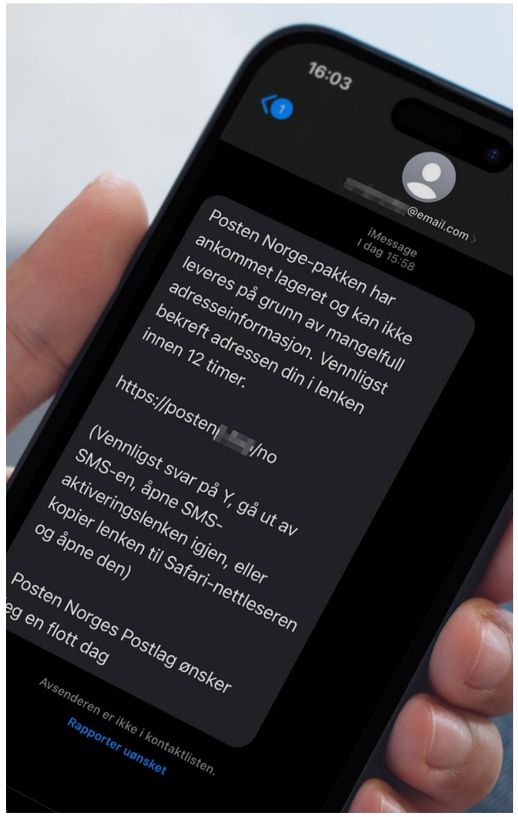
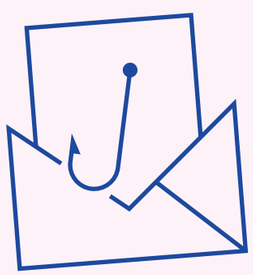


PHOTO: TELENOR



This is how a phishing kit is used:

1. A legitimate website is cloned – for example *www.telenor.se*
2. The login and/or payment page is replaced with a script that steals login details and/or account information
3. The modified files are compressed to a .zip file and saved as a phishing kit
4. The phishing kit is uploaded to a hacked website or a fake domain – for example *www.telenor-tjenester.top*
5. Emails are distributed with links to this spoofed website

ChatGPT and chatbots specifically developed for criminal activity, such as WormGPT and FraudGPT, allow cyber criminals to quickly obtain information ahead of an attack.

Phishing-as-a-Service: Fraud tools served on a silver platter

Recently, several online services have appeared which have made the phishing method described above more efficient and streamlined. This has made it very easy for criminals to tailor so-called "fraud packs"—even if they have limited technical expertise.

The new scam platform Darcula is a prime example of this.

The platform is a so-called phishing-as-a-service (PhaaS): a user-friendly online service that allows criminals to create and distribute messages based on pre-made templates with so-called phishing kits.

Unlike traditional phishing methods, Darcula uses modern technology such as JavaScript, React, Docker and Harbor—which makes it possible to always update and add new functionality without users having to reinstall the software.

The phishing kits offer users over 200 templates that disguise themselves as brands and businesses from more than 100 countries. These templates are generally high quality and come with local languages, logos and content to increase their credibility.

Darcula and platforms like it also make use of the aforementioned online detour, which sends the messages into the victims' inbox via iMessage or RCS.

Generative AI: Opening new shortcuts for scammers

Unsurprisingly, artificial intelligence is playing an increasingly important role in the everyday lives of both IT security specialists and criminals.

Among other things, ChatGPT and chatbots specifically developed for criminal activity, such as WormGPT and FraudGPT, allow cybercriminals to quickly obtain information ahead of an attack. This happens for example by asking the chatbot for all available information about a given company, including lists of suppliers and clients. This makes it possible to streamline the data collection process and the profiling of potential victims.

This technology has also made it easier to tailor and distribute fraud attempts across national borders, with far more realistic content in local languages than what was previously possible without large amounts of resources.

Meet the malicious GPTs

WormGPT is the Dark Web version of ChatGPT that enables the cybercriminal to quickly generate convincing phishing emails, malware, and malicious recommendations for hackers.

FraudGPT is a subscription-based malicious generative AI that uses sophisticated machine learning algorithms to generate deceptive content.

Traces to the criminal networks

Artificial intelligence, PhaaS services, and constant fine-tuning have made criminal approaches both more efficient and more easily accessible to far more people than before. An increasing amount of digital crime is found to be connected to Norwegian and foreign environments that have previously been associated with drug crime.

According to Sweden's Economic Crime Authority (Ekobrottsmyndigheten), Swedish criminals now make more from fraud than drug sales. Last year alone, Swedish criminals made 5.6 billion SEK (0.5 billion EUR) through fraudulent activity.

There is little indication that things are different in neighbouring countries. Many of these frauds likely take place across borders. Among other things, the documentary series "Uppdrag granskning" by Swedish national public broadcaster SVT recently revealed a Swedish criminal network that committed extensive frauds on the elderly in both Sweden and across the border in Norway.

Phishing messages about online purchases were also used here, with subsequent frauds where bank accounts were drained – often by the scammers posing as someone working at the bank, claiming that they had to move the victim's money to a "secure account".

"Safe account fraud"

In Norway, the police issued a press release warning people against a similar approach where the criminals call victims, posing as police officers. In some cases, the criminals also showed up physically outside a victim's residence to obtain their BankID (personal electronic identification method), bank cards and phones.

This winter, Telenor experienced a large increase in "social engineering" scam calls in which criminals posed as police officers. In just a single week in November, Telenor's security filters picked up over 1.1 million unwanted calls in Norway. During any ordinary week the number would be at around 400,000. The increase is largely due to many cases of these police frauds over the phone. This type of scam is part of a broader trend of social engineering attacks across the Nordic region, where criminals exploit trust in authority figures and official institutions to commit fraud.

In Denmark, the total value of credit transfer fraud was DKK 333 million last year. Of this, approximately 81 per cent were scams of private or corporate account holders transferring money themselves[2]. Even with the introduction and use of security measures such as two-factor authentication, fraudsters are continuously adapting their methods.

In the neighbouring country of Sweden, fraud is the category of crime that increased the most last year. According to the Swedish National Council for Crime Prevention, card fraud and fraud via social engineering, thereunder credit transfer fraud, increased the most among the fraud offences.

According to the police, this is how the scam unfolds over the phone:

1. The victim is first called by someone claiming to be from the police or Norwegian Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim). They often tell the victim that they are about to be scammed, for example because someone has taken up a loan using the victim's name
2. The phone call is then transferred to another criminal, who poses as someone from the bank who is there to help the victim
3. The victim is then prompted to offer their BankID authentication information and password and told to move their money to an allegedly safe account
4. The scammers then use the BankID information to access the victim's online bank
5. If the transfer is stopped, for example by the bank, the scammer could approach the victim at their home and ask for the BankID device, bank card, phone or similar items

2 Source: Finance Denmark, Nationalbanken

PHOTO: ARTBERNV / SHUTTERSTOCK.COM

7

The NIS2 clock is ticking in the EU. Where will compliance take us in the Nordics?

With the October deadline to comply with the EU's NIS2 directive rapidly approaching, Telenor explores the directive's expanded scope and its impact on critical infrastructure and important entities, highlighting the challenges and opportunities for organisations across the Nordics.

Left: NIS2 is building upon the NIS1 directive to ensure cyber resilience across Europa amidst a rapidly changing cyber threat landscape.

A bit of history: the evolution from NIS1 to NIS2

NIS1, which stands for "Network and Information Systems" was the first EU-wide sector-specific legislation on cyber-security, adopted in July 2016. This marked a significant step forward, as it was designed to enhance the level of cyber-security across the EU. However, as the digital landscape evolved, so too did the complexity and frequency of cyber threats. This necessitated a more robust framework, leading to the adoption of the NIS2 directive in December 2022.

NIS2 builds upon the foundation laid by NIS1 and aims to address the shortcomings of the original directive. NIS1 focused mainly on the security of network and information systems across critical sectors such as energy, transport, digital infrastructure, and health. However, the flexibility given to member states in the implementation of this directive led to varying levels of cyber-security across the EU. This inconsistency, coupled with the rapid advancement of cyber threats, underscored the need for a more comprehensive approach. NIS2 is the EU's answer, a next step in their attempts to standardise cyber-security measures, enhance co-operation among members states, and broaden the scope of the directive to include more sectors and types of organisations.

For Telenor and the broader telecommunications industry, the provisions within the European Electronic Communications Code (EECC), which were issued prior to NIS1, will be replaced with the requirements in NIS2 once the directive is in effect.

The EU's response to a changing threat landscape

Since the inception of NIS1 in 2016, Telenor and others have borne witness to a dramatically changing cyber threat landscape. The EU has recognised this change and saw the need to address the increased frequency and sophistication of these attacks, which are targeting a broader range of sectors and critical infrastructure. Cybercriminals today are actively exploiting the increasing digitalisation and interconnectivity across society, which exposes new vulnerabilities and potential targets for attack. High-profile incidents such as ransomware attacks on healthcare facilities and supply chain breaches have put a global spotlight on the need for more resilient cyber-security frameworks in organisations of all types and sizes.

As the EU's strategic response to these growing challenges, NIS2 is a solid step in what is likely to be evolving legislation on this topic. With NIS2's expanded scope and stricter requirements, the directive is intended to mitigate risks and build cyber resilience across the continent and a broader range of industries. The updated directive recognises the interconnected nature of today's digital infrastructure and the potential cascading effects of cyber incidents, which has led to NIS2's emphasis of

What is NIS2?

The NIS2 Directive is the EU-wide legislation on cyber-security. It provides legal measures to boost the overall level of cyber-security in the EU. Businesses identified by the Member States as operators of essential services in sectors ranging from energy, health, and drinking water to digital infrastructure and ICT management will have to take appropriate security measures and notify relevant national authorities of serious incidents. Key digital service providers, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements under the Directive. The deadline to comply with the directive in the EU is 17 October 2024.

Source: *Directive on measures for a high common level of cyber-security across the Union (NIS2 Directive) | Shaping Europe's digital future (europa.eu)*

» NIS2 is a response to the growing digital interconnectedness across companies and industries, recognising that a cyber incident in one sector can have cascading effects on others.

more comprehensive and coordinated cyber-security measures across more organisations and sectors, including those that were not previously in scope with NIS1.

NIS2 is a response to the growing digital interconnectedness across companies and industries, recognising that a cyber incident in one sector can have cascading effects on others. For example, a disruption in the telecommunications industry may severely affect the power and utilities sector, impacting emergency operations and coordination capabilities between agencies and organisations, as cited in the recently released EU Cybersecurity Risk Evaluation and Scenarios for Telecommunications and Electricity. This report specifically mentions a scenario in which power outages can lead to widespread disruptions in data centres, the telecommunications industry, and other critical sectors. This interdependency reinforces the need for comprehensive and coordinated cyber-security measures, as outlined in the NIS2 directive.

Key intentions behind the NIS2 directive

Another key reason for NIS2 is to address the inconsistencies in the implementation of NIS1 across the EU. The varying degrees of compliance and the different national approaches under NIS1 have created gaps in the overall cyber-security posture of the EU. By introducing NIS2, the EU seeks to harmonise cyber-security requirements and ensure greater consistency across the region.

NIS2 also broadens the scope to include more sectors and types of entities. This is a crucial change to the directive, as it recognises the critical role that various industries play in the functioning of society and the economy. NIS2 includes digital service providers, public administration, and others that also play a role in protecting critical infrastructure and services.

Key measures in the NIS2 directive

The following key measures within the directive collectively aim to harmonise and strengthen cyber-security across the EU, to a greater extent than in NIS1:

- Expanded scope and uniform criteria (identifying 'essential' and 'important' entities and reducing discrepancies in implementation)
- Standardised security requirements
- Stricter incident reporting
- Strengthened co-operation and enforcement (through ENISA and the Cooperation Group)
- Mandatory peer reviews
- Focus on supply chain security
- Enhanced information sharing

NIS2: Who is impacted and what is required?

NIS2 expands the list of sectors and entities that are considered essential for the functioning of society and the economy. The directive categorises entities into two main groups: essential and important.

Essential entities include critical sectors such as energy, digital infrastructure, transport, banking, financial market infrastructures, health, and drinking water.

The rationale behind including these sectors is to ensure the smooth operation of essential services in the face of growing cyber threats. Disruptions to these services could have severe consequences for public safety, economic stability, and national security.

Important entities include some digital services like online marketplaces and search engines, as well as public administration, space, and food production and distribution.

By implementing robust security measures across these sectors, the EU aims to protect critical infrastructure and essential services from cyber threats and build greater resilience overall.

What does NIS2 require of you?

The NIS2 directive outlines requirements for essential and important organisations in the EU to enhance their cyber-security posture. This includes the following:

1. **Risk management measures:** Organisations are required to implement 'appropriate and proportionate' technical and organisational measures to manage risks posed to the security of network and information systems. This includes conducting risk assessments, developing incident response plans, and regular testing of security measures
2. **Incident reporting:** Organisations are required to provide early warning of significant incidents to the relevant national authority within 24 hours of becoming aware of the incident and a notification within 72 hours. This is to ensure a timely response to mitigate the impact of the incident and support better information sharing
3. **Supply chain security:** Organisations must address cyber-security risks in their supply chains to ensure that their vendors adhere to robust security standards. Given the increasing reliance on third party services, this is an especially key development in NIS2 to minimise the potential for supply chain attacks

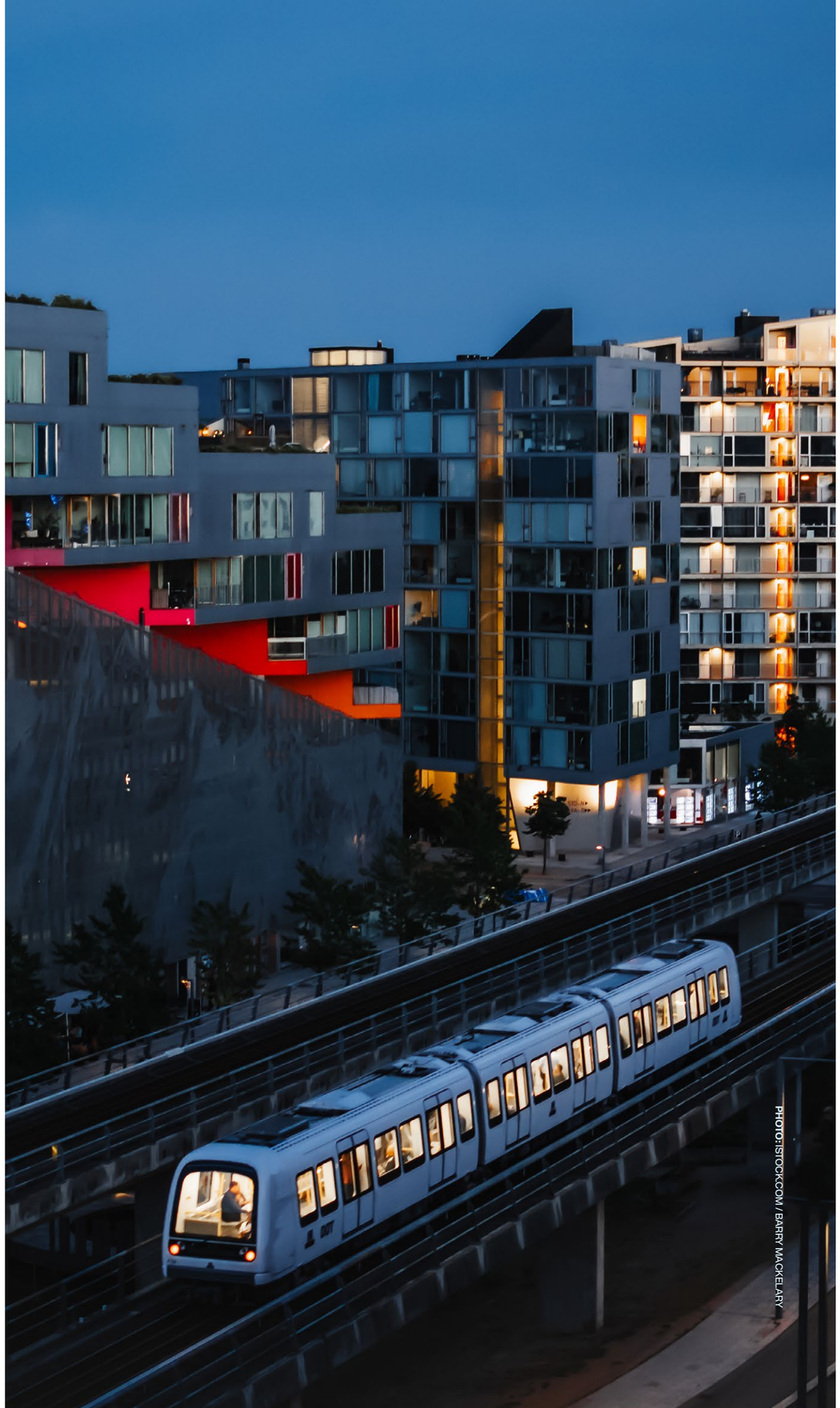


PHOTO: ISTOCK.COM / BARRY MACKELARY

Supply chain risks are particularly relevant for the telecommunications and electricity sectors, which rely on a complex network of suppliers and may be based outside of the EU. These dependencies can create vulnerabilities if the suppliers are not under adequate legal restraints, potentially leading to espionage and disruptions to critical services

4. **Co-operation and information sharing:** NIS2 supports enhanced co-operation and information sharing between organisations and countries, and their respective national authorities. This greater regional collaboration is intended to boost the overall resilience of the EU and its level of cyber-security

Reasons to support NIS2 compliance

The NIS2 directive imposes significant penalties for non-compliance, including fines and other administrative sanctions. Penalties for non-compliance carry fines up to EUR 10 million or 2% of the company's annual revenue (whichever is higher). In addition, NIS2 allows authorities within EU Member States to hold organisational leaders personally liable if gross negligence is proven following a cyber incident. To avoid such penalties, the directive requires member states to establish 'effective, proportionate, and dissuasive penalties' for non-compliance, to ensure that entities follow through with their obligations.

Compliance with NIS2 can also enhance an organisation's reputation and trustworthiness. As many companies have unfortunately learned in recent years, cyber-security incidents can severely impact reputation and stakeholder trust. Through comprehensive risk management practices, incident response planning, and the supply chain security measures required in NIS2, organisations are asked to continually maintain and improve their overall cyber resilience – which ultimately can serve as a competitive advantage.

Norway and NIS2

Though not an EU member, Norway is a part of the European Economic Area (EEA) as a means of accessing the European market. As such, the country typically adopts EU regulations and directives into local law. To align with the cyber-security standards in NIS1, Norway introduced its digital security law (Digitalsikkerhetsloven) to improve the security of critical infrastructure and services. Currently Norway is working to align with the NIS2 directive by introducing more stringent cybersecurity requirements to a broader range of organisations.

The road to NIS2 compliance in the Nordics: a legal perspective

The NIS2 deadline is around the corner, and Nordic organisations face a challenging road to compliance. Johanna Linder and Henrik Lindstrand, partners at Cederquist, a prominent Swedish law firm, share the legal perspective on NIS2 compliance and its implications for Nordic organisations.

Key NIS2 concerns among Cederquist's Nordic clients

According to Johanna Linder and Henrik Lindstrand, there has been a significant increase in client inquiries regarding NIS2 compliance – and the type of legal advice requested varies quite a bit.

Companies already compliant with NIS1 have a relatively straightforward path ahead and may simply seek assistance to update internal policies or supplier contracts. In the 'new' sectors now included in NIS2 directive, many organisations are seeking confirmation on whether they are subject to it, and, if so, how to organise their compliance work.

Lindstrand noted, "Many companies that were not subject to NIS1 are now trying to understand if they need to comply with NIS2, in the light of sector descriptions, thresholds, and cross-border aspects. If the conclusion is that they do, many face a long 'to do list'."

The challenge is further compounded by the fact that many member states have yet to implement the necessary legal acts to transpose the directive, creating uncertainty and delays. In Sweden, for example, the Swedish implementing act is expected to be adopted and come into force on 1 January 2025, but detailed national regulations from supervisory authorities are still pending.

How does NIS2 impact Nordic organisations?

The transition to NIS2 will significantly impact Nordic organisations, particularly those not previously covered under NIS1. Many companies are more or less starting from scratch with their information security work and will need to take extensive steps to meet the new requirements.

As Linder explained, "Many organisations need to do the basics first, that is to make an inventory of all digital assets used, classify their data, and identify security needs based on risk assessments to ensure confidentiality, integrity and availability. Only after this work is complete is it possible to implement security measures that are not yet in place and adopt policies and processes for risk and crisis management, as well as business continuity."

A key aspect of NIS2 is the emphasis on documenting security measures and assessments. Lindstrand emphasised, "Even if security measures are in place, documenting the security measures and the assessments you have made is critical under NIS2."

While NIS1 required organisations to work systematically with information security, NIS2 specifies more detailed requirements, necessitating governance and procedures to be revisited.

Additionally, new obligations under NIS2 include stricter notification requirements, increased liability for management, higher fines, and enhanced supply chain and business continuity requirements. This also means that service providers who are not directly subject to NIS2 may need to implement additional measures to comply with contractual obligations imposed by their customers under NIS2.

A perspective on the EU's intent with NIS2

The EU's motivation behind NIS2 is clear: to address the growing dependence on digital services and infrastructure and the increasing cyber threats. Linder and Lindstrand pointed out that the EU recognises the vulnerability of society to these threats, prompting a wave of national regulations aimed at enhancing cyber-security. The overarching goal is to harmonise rules across the EU and ensure a high level of cyber-security across all member states.

PHOTO: CEDERQUIST

In Sweden, the focus is on ensuring a minimum level of information security throughout organisations. As Lindstrand noted, "In general, we haven't seen that the draft Swedish Implementing Act goes beyond NIS2, just a few nuances. Other countries may tweak sanctions and liability, but the general framework shall remain consistent."

Draw on previous compliance work to achieve NIS2 compliance

Compliance with NIS2 can be more readily facilitated by companies that have already established a structured compliance organisation and processes, e.g. in relation to the General Data Protection Regulation (GDPR). These organisations can build on the existing compliance frameworks.

However, Linder and Lindstrand acknowledge that smaller companies may struggle due to a lack of resources and expertise, particularly within IT and information security and legal. They emphasised the importance of viewing compliance as an investment, not just a regulatory requirement. "This is something that will be a business advantage or market advantage. We can expect further regulations within the field from the EU in the future," Linder explained.

Advice for organisations

For organisations that are in the early stages of their NIS2 compliance work, the first step is to set necessary roles, adopt a structured methodology, and develop a plan for the compliance work.

Lindstrand stresses the importance of a coordinated approach, stating, "In light of all new regulations that are coming or expected to come from the EU within cyber-security, data and AI, set a general method and structure for compliance implementation and maintenance to avoid reinventing the wheel multiple times. Communicate how the compliance work will be done and align across functions and departments as compliance involves large parts of the business."

This holistic approach ensures that all legal frameworks are considered, and digital assets are managed in an integrated and efficient manner.

While the path to NIS2 compliance is challenging, it also presents an opportunity for Nordic organisations to enhance their cyber-security posture and gain a competitive edge. Linder and Lindstrand's legal perspective on this directive underlines the importance of preparation, structured methodology, and viewing compliance as a strategic investment for the future.

From compliance to risk management: Building stronger cyber defences in the Nordics

To understand the shift from compliance to robust risk management under NIS2, Telenor spoke with Tomomi Aoyama, PhD, Senior Director of Strategy and Product at Omny, an industrial cyber-security company. Aoyama provides insights into the differences between compliance and risk management, the challenges faced by organisations, and the broader implications for cyber-security across the Nordics.

Compliance vs. risk management

Aoyama emphasises that while NIS2 mandates compliance, it transcends simple checkbox exercises, urging organisations to adopt comprehensive risk management practises. She explains, "NIS2 is asking for compliance to regulation but at the same time, it is not asking to check boxes. It is asking organisations to ensure the effectiveness of cyber risk management. The challenge in the organisation is that regulatory compliance is often led by GRC (Governance, Risk, and Compliance), while risk mitigation measures might be implemented by other departments. Risk management needs to have more organisational muscle to run."

The directive's multi-layered approach requires a systemic understanding of dependencies and risks from the EU level down to individual organisations. Aoyama explains that NIS2 is designed to facilitate a co-ordinated EU-wide cyber-security posture.

"For the EU to understand dependencies and risk as a whole, they need to understand how each country is running risk management, how it is reported, and the incidents faced."

This requires robust reporting and feedback mechanisms to provide a comprehensive risk picture across the EU.

PHOTO: OMNY

Enhancing cyber defence in the Nordics

A key aspect of NIS2 is its impact on executive accountability for cyber risks. Aoyama hopes that this will lead to more active discussions about cyber risk at the executive level.

"One of NIS2's big asks is for senior leadership in organisations, including boards and executives, to be accountable for cyber risk. It used to be the CISO's responsibility, but now it's the CEO and Board who must ensure they are running the programme," she explains. This shift could foster a broader understanding of cyber risk as a critical business issue rather than just a technical concern.

Challenges and opportunities

When asked about the major blockers and opportunities presented by NIS2, Aoyama points to the detailed regulatory requirements and the challenges posed by supply chain issues. She explains, "There are some elements that will be challenging related to upcoming regulations, particularly around supply chain issues, which are not very detailed in the NIS2 document itself. We will see how each country interprets that in their context."

Despite these challenges, Aoyama views the integration of NIS2 into broader cyber-security programmes as a significant opportunity. She believes that NIS2 can drive a cultural shift within organisations, promoting shared responsibility for cyber-security across all levels.

The main challenge for cyber professionals in organisations is to start engaging with internal stakeholders and not see NIS2 as another GDPR. It's more about engaging with leaders and relevant departments, such as supplier management, to ensure NIS2 is integrated into their cyber programme," she notes.

Future perspective and synergy with other cyber regulations

Looking ahead, Aoyama sees NIS2 and the EU's Cyber Resilience Act (CRA) as complementary regulations that together will strengthen cyber-security across Europe.

"NIS2 is towards the critical infrastructure operators, while CRA is towards the product suppliers – any products with digital elements. They are trying to capture the whole ecosystem, including digital product suppliers, distributors, and users, with these two regulations," she explains.

The integration of these regulations is designed to ensure comprehensive coverage of cyber-security responsibilities across different layers of the digital supply chain. This holistic approach aims to enhance overall cyber resilience and provide consumers with more secure product choices.

Omny's advice for Nordic organisations

For Nordic organisations, Aoyama advises leveraging commonly used cybersecurity frameworks, such as ISO 27000 or IEC 62443, to streamline compliance efforts. She acknowledges the challenges faced by SMEs in meeting NIS2 requirements but highlights the importance of viewing compliance as an investment. "It's crucial for organisations of all sizes to recognise this as an investment – not only regulatory, but also a performance driver in the business, to ensure that you can provide services to a broader group of companies," she explains.

Aoyama also underscores the need for ongoing dialogue between policymakers and practitioners to bridge gaps in expertise and ensure feasible implementation of cyber-security measures. "It's important to really talk to asset owners about what is feasible to deploy and what could be a blocker to innovation," she adds.

What becomes evident through this interview is that NIS2 is more than a regulatory burden; it is a catalyst for a strategic shift in how organisations approach cyber-security. By fostering a culture of risk management and shared responsibility, NIS2 aims to build stronger, more resilient cyber defences across the Nordics and hopefully, well beyond.

What is the EU's Cyber Resilience Act?

The Cyber Resilience Act (CRA) is the EU's new cyber-security rules to ensure safer hardware and software. It aims to safeguard consumers and businesses buying or using products or software that contain a digital component. The Act introduces mandatory cyber-security requirements for manufacturers and retailers of such products, with this protection extending throughout the product lifecycle.

Source: *EU Cyber Resilience Act | Shaping Europe's digital future (europa.eu)*

The potential of NIS2 to shape the future of digital security in Europe

The NIS2 directive marks a pivotal evolution in the EU's approach to cyber-security, with potential long-term effects on Europe's digital security landscape. By enforcing more stringent and standardised requirements across all member states, NIS2 aims to align countries with varying levels of cyber-security maturity towards a unified goal. This harmonisation will surely lead to a more resilient critical infrastructure across Europe, as more sectors adopt robust cyber-security measures to counter increasingly sophisticated cyber threats.

One of the potentially more transformative aspects of NIS2 is its emphasis on securing supply chains. The EU recognises supply chain security as a critical issue, especially given the increased frequency of supply chain attacks, as well as how supply chain dependencies can lead to increased vulnerabilities for critical infrastructure and services. The NIS2 focus on the supply chain could lead to widespread improvements in security practices across Europe, making digital products and services more secure and reducing the risk of supply chain attacks. In the long term, this could also prompt a shift in how businesses select and manage their suppliers, prioritising cyber-security as a critical factor.

The directive's stringent requirements may also act as a catalyst for innovation in cyber-security technologies. As organisations strive to meet NIS2's demands, there is likely to be increased investment in advanced solutions such as AI-driven threat detection, automated incident response, and secure communication channels. This push for compliance may lead to a future where European companies are not just consumers of cyber-security solutions but also leaders in creating them.

If NIS2 successfully reduces the incidence of cyber-attacks within the EU, other regions may look to Europe as a model for their cyber-security policies, potentially leading to the globalisation of NIS2-inspired regulations. In this way, Europe could emerge as a global leader in cyber-security innovation, setting new standards both within the EU and globally. In a world where cyber threats know no borders, the ability to set the rules of engagement could provide a significant strategic advantage for the EU.

As we view it in Telenor, NIS2 is not merely a regulatory update, it is a comprehensive framework poised to reshape digital security in Europe. By driving higher standards, fostering collaboration, and spurring innovation, NIS2 will help build a more secure and resilient digital environment, ultimately positioning Europe as a global leader in cyber-security.

Nordic NIS2 readiness

Percentage of companies surveyed that already provide the cyber-security training required in NIS2

- **49%** of Finnish companies
- **61%** of Norwegian companies
- **33%** of Swedish and Danish companies

Source:
Telenor Group and Norstat survey October 2023

» As we view it in Telenor, NIS2 is not merely a regulatory update, it is a comprehensive framework poised to reshape digital security in Europe.

PHOTO: ISTOCK.COM / REMUS KOTSELL

PHOTO: HARALD PETTERSEN / ©EQUINOR

8

This is why *resilience* is the new security

The threat landscape has changed how Nordic companies handle security. In this chapter, we take a closer look at some of Norway's most important companies, asking ourselves what would happen if public broadcaster NRK, the country's largest bank DNB, or energy company Equinor were attacked today?

Left: Companies like Equinor needs to be able to continue operating during emergencies. This requires robustness and resilience.

The global threat landscape has rarely been more complex. This has led to several changes in how some of Norway's most important companies handle security and manage security incidents.

A big part of this is about being adaptable to keep everything running smoothly, even during a crisis.

"Robustness and redundancy in infrastructure and systems have become necessary to protect against threats. So has the ability to withstand and recover from a serious incident," says Rolv R. Hauge, Business Continuity Manager at Telenor Norway.

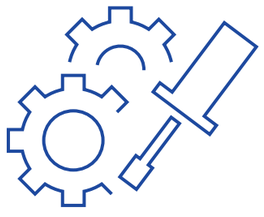
Like many others, Telenor has expanded its measures in recent years to ensure business continuity and the ability to quickly recover after an incident.

Hauge believes this evolution in security thinking has taken most companies on a journey.

"At first, it was all about protection. For a long time, having a firewall was considered sufficient security. Then came the gradual realisation that breaches still occur, and you need the ability to detect and manage incidents."

"Today, most have shifted their focus to survival and recovery after an incident".

That's why *resilience* has been chosen as the main theme for this year's edition of Nordic Digital Security.



» Robustness and redundancy in infrastructure and systems have become necessary to protect against threats.

This is *resilience*

- Resilience refers to an organisation's ability to adapt, withstand, and recover from a security incident
- An organisation or system is resilient when it has multiple layers of defence and can maintain or quickly return to operational status
- The terms robustness, resilience, and resistance are often used as synonyms. All of these can be seen as the opposite of vulnerability

PHOTO: OLE JØRGEN BRATLAND / ©EQUINOR

Resilience – from A to Z

Resilience is about an organisation's ability to endure and recover from a major incident, whether it's a cyber-attack or a natural disaster.

"In most organisations, critical inputs are essential for key processes. If these inputs become unavailable due to an incident, the first step is incident management, followed by recovery efforts. At the same time, we need to think about business continuity during the phase when critical inputs are missing", explains Hauge.

These business continuity measures can take many forms, from backup solutions that provide almost fully functional processes and production to emergency solutions that ensure only the absolute minimum operations. Measures to maintain business continuity and enhance recovery capability often need balancing, referred to collectively as Business Continuity and Disaster Recovery (BC/DR).

Serious incidents often create a crisis for the organisation, requiring a specific form of leadership that ensures proper prioritisation and clear communication throughout the process. To strengthen the ability to recover, implement continuity measures, and manage crises, good planning, training, and testing against various scenarios are necessary.

This approach has also been central to the efforts of NRK, DNB, and Equinor in recent years. Like Telenor, these organisations cannot simply pause operations. If their systems go down, critical societal functions must still operate.

NRK: "Must be able to communicate, no matter what"

As media organisations are continually targeted by complex DDoS attacks from hostile actors, having concrete contingency plans and backup solutions has become critical. At Norwegian public broadcaster, NRK, plans are in place in case a crisis occurs at their HQ.

"The biggest difference between traditional security thinking and working with resilience is the level of complexity. Today, most organisations rely on many systems, and it's not always easy to decide what to prioritise in a crisis," says Øyvind Vasaasen, Head of Security at NRK.

NRK has always needed a backup solution in case TV or radio broadcasts suddenly go dark. Today, NRK's role in ensuring crisis information for the public is also governed by the country's Security Act.

"NRK must be able to convey messages from the authorities to the public, whether we're at war or facing a cyber-attack. Continuity and resilience are things we work on constantly," says Vasaasen.

Ten years ago, NRK established a continuity plan, including measures to keep publishing if the systems at their Oslo headquarters are hit. In recent years, the plan has been further strengthened to adapt to today's threat landscape and NRK's production structure.

Even though technology has changed a lot, just having a PC isn't enough to broadcast news to all of Norway. That's why NRK must practise using alternative solutions.

"We regularly broadcast from our backup location because we need a 'warm' solution. If the main location goes dark, the alternative site can continue news updates and broadcasts until the NRK system is back up and running," Vasaasen explains.

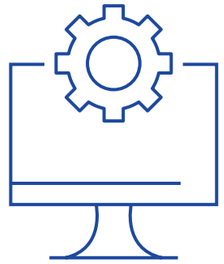
NRK's own threat assessment identifies several current threats, such as influence and disinformation, activism, uptime and publishing capability, weakened trust in content, misuse of the brand, data leaks, and information theft.

"Overall, the security situation for media houses is more challenging now than before. We face more DDoS attacks from actors trying to take us down, while fake news tests our editorial teams on a daily basis."

PHOTO: HANS A. ROSBACH, CC BY-SA 3.0, VIA WIKIMEDIA COMMONS

Today, NRK has an emergency plan to handle crises and a security management system inspired by ISO 27001.

"We have management documents at the organisational level, broken down into guidelines and procedures. When we work on security principles, our overarching document sets the framework for security work at NRK," says Vasaasen. He adds, "Different threats are often connected. Digital security also involves physical security, so procedures for who you let into the building are part of our digital resilience."



Resilience is an ongoing focus for NRK, including better operational IT security and detecting potential digital attacks. In recent years, they've significantly strengthened their IT security environment.

"NRK's emergency plan is based on the national crisis incident management (CIM) system. This system is separate from NRK and will function even if everything at NRK goes down. NRK has plans for various situations, down to detailed action cards," Vasaasen explains.

Vasaasen believes the most crucial step they've taken to enhance preparedness is having concrete plans and using them regularly.

"Many often think they don't need to use the crisis plan because they can handle the situation without it. However, it's often shown that things could have been managed better with more systematic decision-making and actions. It's a much more efficient way to work," he emphasises.

» Overall, the security situation for media houses is more challenging now than before.

DNB: "Redundancy at every level"

Despite a grim digital threat landscape characterised by ransomware and an aggressive Russia, the financial industry cannot revert to analog solutions. At DNB, a robust defense-in-depth strategy has led to a decrease in serious cyber-security incidents.

Norway's largest bank, DNB, has also placed great emphasis on continuity planning and robustness in recent years. For them, digital solutions are non-negotiable.

"It's no longer just about getting the IT system back up and running, but about how we can operate under such conditions," says Anders Hardangen, Chief Security Officer at DNB.

In 2023, DNB handled 20,208 cyber-security incidents and managed eleven incidents with "high potential for negative impact on DNB." Both figures are lower than the previous year, primarily due to efforts to make the bank's IT systems more resilient, according to Hardangen.

"Thanks to a robust defence-in-depth approach, we can stop more attacks at an earlier stage and mitigate their consequences. When we develop new products and services today, we think about redundancy throughout the entire process. The same goes for how we interact with customers."

In the financial industry, uptime and the ability to deliver digital services have been crucial for decades. However, recent developments in the risk landscape have led to changes at DNB as well.

"The many ransomware attacks have shown that anyone can be hit, and the business and customer consequences can be enormous. Russia's aggression is another factor that has underscored the importance of having good continuity plans and alternative solutions," says Hardangen.

"There are many important things in daily operations, so in a crisis, you have to prioritise. For the capabilities we prioritise, we need to be resilient and have good alternatives that work even under suboptimal conditions."

In recent years, DNB has renewed its entire business continuity framework, adopting an international standard that defines the most critical services and functions within the organisation.

"This involves setting up a structured process with impact analysis, risk assessments, establishing continuity plans, and testing them. This is challenging in a large digital ecosystem, and much of it is about prioritising the most important things first and ensuring they are adequately covered."

For a financial institution like DNB, digital solutions are essential. Thus, DNB focuses on finding digital solutions that meet their security needs.

"We can't go back 50 years to cash and bank branches on every corner. The global financial market moves too fast for that today. Even in extreme situations like in Ukraine, maintaining digital financial services became the only solution because it was too dangerous to transport cash."

"As a society, we are completely dependent on information and on having power and telecom infrastructure as the foundation. As a financial institution, we depend on digital services functioning – even in an emergency situation," says Hardangen.

PHOTO: EKELY VIA GETTY IMAGES

» For a financial institution like DNB, digital solutions are essential. Thus, DNB focuses on finding digital solutions that meet their security needs.

Equinor: "It's not enough to just endure the crisis"

Changes in the geopolitical landscape and an increased focus on the renewable market are among the reasons Equinor is now making changes to its emergency preparedness organisation. The company is now taking a more holistic view of security challenges.

Another company that must deliver during emergencies is Equinor. Norway's largest energy company has faced some of the most severe security incidents in Norwegian business, such as the hostage crisis at In Amenas in Algeria in 2013.

With a broad international presence and operations that sometimes carry high potential risks, preparedness and crisis management are integral to most of the company's activities. Changes in the geopolitical landscape, the adoption of the Security Act in Norway, and the company's shift towards the renewable market have also driven changes in their security and preparedness efforts.

"To adapt, we have made several adjustments to our emergency organisation. We have also developed and practised new scenarios that reflect the current geopolitical situation," says Asbjørn Ringstad, Director of Emergency Preparedness at Equinor.

Equinor's role as a supplier of energy to Europe brings responsibilities beyond Norway's borders.

"A lot of it is about being able to endure crises longer than we are used to. Additionally, we conduct exercises and coordinate across the private and public sectors," Ringstad explains.

Equinor takes a holistic approach to security and emergency preparedness.

"Simply put, it's the recognition that everything is interconnected. To handle and learn from incidents effectively, we must understand why and how they occur. This requires close collaboration and open communication between different specialist areas," says Ringstad.

PHOTO: OLE JØRGEN BRÅTLAND / ©EQUINOR

PHOTO: MIKE MORLEY VIA GETTY IMAGES

That is why Equinor has structured itself so that leaders with different responsibilities — cyber-security, physical security, personnel security, emergency preparedness, and business continuity — are part of the same leadership team, ensuring comprehensive risk understanding.

"Today, many external threats affect our operations. These are often closely tied to the geopolitical situation, over which we have little control but must still prepare for the consequences," Ringstad states.

Building robustness and resilience has been central in recent years, especially concerning the cyber threat landscape.

"This approach is now integrated into our overall preparedness work. Our complex operations make it challenging to quickly find alternative solutions to maintain operations unless we are trained and prepared."

» Building robustness and resilience has been central in recent years, especially concerning the cyber threat landscape.

"For us, it is crucial to do this work in advance, to practise, and to be conscious of priorities in collaboration with our partners. This creates the robustness we seek and makes the unpredictable more predictable in a crisis situation," says Ringstad.

Ultimately, having a strong organisational culture is most important, according to Ringstad.

"We have a strong culture when it comes to exercises and training. This commitment is found at all leadership levels. Our CEO practises his role in the emergency organisation four times a year. This culture is, and always will be, the cornerstone of everything we do," concludes Ringstad.

There's no time to waste

9

There's no time to waste

In a world where everything and everyone is connected, the Nordic digital security landscape has grown more complex and uncertain. The evolving threat environment requires businesses and organisations to be more closely integrated with the total preparedness of the region. There is a pressing need to prioritise and develop more common solutions for security, resilience, and robustness in a Nordic and allied context. We cannot affort to ignore the opportunitites that Nordic co-operation presents.

Left: In our message to the decision makers of the Nordics, Telenor underlines the fact that that there's no time to waste - we need to take advantage of the opportunities stemming from Nordic co-operation, both in military and civilian sectors.

PHOTO: ISTOCK.COM / NALMOID

Increased resilience

The telecommunications industry is the foundation of digitalisation in the Nordic region. Industry players build, operate, and develop telecom networks that underpin critical services essential for societal function, including power, finance, transport, and health. However, this infrastructure faces growing threats.

Telenor Nordics is particularly concerned about Russia's systematic dismantling of civilian infrastructure in Ukraine, including electricity, payment solutions, transportation systems, broadband, and mobile networks. Acts of sabotage, such as those targeting gas pipelines in the Baltic Sea and railway cables in Europe, also serve as stark warnings. Similar incidents could easily occur in the Nordic countries. If communication networks fail – if phones do not work, SMS cannot be sent, and businesses and individuals cannot connect to the internet—the functionality of our society is at significant risk.

In response to these threats, Finland is considering, for example, taking a proactive stance in safeguarding against evolving cyber threats by significantly increasing its cyber-security investment by 30% in 2024 to counter AI-enabled cyber threats.[3] This strategic move aims to enhance the nation's cyber-security defences across public and private sectors. This investment aligns with recommendations from the "Security Threat of AI-Enabled Cyber-attacks" (STAIC) report, a collaborative effort between Finland's state transport and communications agency Traficom, the National Emergency Supply Agency (NESA), and cyber-security leader WithSecure, emphasising the importance of adapting security measures to counter AI-driven attacks.

Resilience and security in telecom infrastructure are not luxuries but necessities. Telenor is reinforcing its internal resilience efforts by investing in more robust systems and enhanced cyber defences across the Nordic region. With Sweden and Finland joining NATO in 2024, along-side long-time members Norway and Denmark, the security landscape in the region has also been reshaped. This integration enhances the collective defence posture of the region, facilitating a more coordinated response to emerging threats against critical infrastructure and broader societal stability.

About Telenor as a Nordic preparedness actor

Telenor Nordics, comprised of operations in Norway, Sweden, Finland, and Denmark, owns and manages critical infrastructure, ensuring the secure and stable delivery of digital services across mobile, fixed networks, and broadband. This includes providing voice, data, and SMS, which are essential for the functioning of societies in these countries.

We take our commitment to provide stable and secure services during peace, conflict, crisis, and war very seriously. This responsibility requires us to maintain stringent control over ownership and operations within our critical infrastructure supply chain, reflected in our agreements with suppliers and partners. Recognising that we are a target for advanced threat actors, Telenor is acutely aware of our security responsibilities towards our customers, society, and ourselves.

We focus on integrating security and preparedness into all our processes and see great value in maintaining a good and transparent dialogue with authorities to uphold national security. Our operations adhere to national security laws across the Nordic countries, ensuring compliance and proactive measures to safeguard our infrastructure.

3 https://dig.watch/updates/finland-plans-30-increase-in-cybersecurity-spending-in-2024-to-counter-ai-based-cyber-threats

There's no time to waste

Robust and secure communication is essential for crisis management and national security, particularly during high-intensity conflicts.

Robust and secure communication is essential for crisis management and national security, particularly during high-intensity conflicts. The threat landscape can change rapidly, and we must learn to manage this uncertainty. To protect our digital backbone, we will continue to invest in resilient systems and enhanced cyber defences. This requires robust preparedness, an updated situational understanding, and holistic and thoughtfully designed solutions tailored to specific regional needs. This aligns with the recent NIS Co-operation Group's first report on the cybersecurity and resilience of Europe's telecommunications and electricity sectors, which calls for enhanced collective cyber situational awareness and crisis management.[4]

Access to expertise

The Nordic region faces a growing challenge in accessing expertise in technology and security fields. There is a shortage of specialised competence, particularly regarding the availability of personnel who can also get a security-clearance. This shortage impacts the ability to develop and maintain robust cyber-security measures and advanced technological infrastructure, which are critical for national and regional security.

In Sweden, the Security Service (Säkerhetspolisen) has highlighted the need to investigate how the Swedish security clearance system aligns with NATO's requirements. The introduction of a more efficient clearance system in Sweden could address the administrative burdens currently faced by oversight bodies and operators, particularly in light of Sweden's recent NATO membership.

Telenor believes that enhanced Nordic co-operation in areas hindering cross-border collaboration, such as on security clearance processes, can provide the necessary scale to address this issue. Here the roles of both the EU and national governments are important for creating harmonised frameworks that support cross-border security measures. However, this approach should carefully consider national contexts and specific regional needs, particularly where existing regulations already provide adequate security without imposing undue burdens. By aligning security policies and clearance standards across the Nordic countries, it becomes easier to share resources and expertise, facilitating a more robust and unified approach to cyber-security, technological development, and security that enhances our collective resilience against cyber threats.

Integrating business

In Norway, Telenor has long advocated for closer integration of businesses into Total Defence, i.e. a comprehensive national defence strategy that integrates both military and civilian resources to safeguard the nation during times of crisis or war. It is therefore positive that the recommendations from the Norwegian Defence Commission and the Norwegian Total Preparedness Commission clearly recognise the importance of using businesses as preparedness actors and resources. This approach should be expanded to a Nordic scale, incorporating regional initiatives that align business preparedness efforts across all Nordic countries. The long-term plan for the Norwegian Armed Forces states that it is "necessary to rethink how business actors can better be integrated into total defence".

4 https://digital-strategy.ec.europa.eu/en/news/risk-assessment-report-cyber-resilience-eus-telecommunications-and-electricity-sectors

Large business actors in the Nordics, operating in sectors such as finance, energy, food, and telecom, possess critical competencies and capacities essential for maintaining societal and national security. These companies own and manage vital infrastructure, making their role in total defence crucial. They provide valuable insight and expertise on the critical civilian functions they help maintain, contributing to the fulfilment of the Nordic countries' obligations under NATO's seven baseline requirements.

However, a significant challenge remains. Security laws and regulations in the Nordic countries have all become stricter, and their national implementations vary. The challenge is both horizontal and vertical: horizontally, regulations differ between countries; vertically, the implementation of security regulations varies across sectors within each national market.

For example, in Sweden, the current Security Protection Ordinance imposes significant restrictions on the ability of private corporate groups to share security-sensitive information within their own structures, hindering effective crisis preparedness and total defence planning. This regulatory burden leads to retrospective situational reporting rather than forward-looking crisis management. Amending the ordinance to allow for security protection agreements within corporate groups would be a crucial step towards more effective total defence integration. However, this amendment should also extend beyond total defence aspects to facilitate a broader scope of information sharing with the private sector.

Further, the Nordic dimension adds another layer of complexity. The lack of aligned implementation of security protection agreements and security clearances makes it difficult for companies to maintain shared infrastructure or fully engage in collaborative activities across the region. To overcome these obstacles, targeted alignment in specific areas hindering cross-border co-operation, with a focus on streamlined and efficient regulations, enabling smoother cross-border co-operation would be ideal. The Nordic Council has long championed the idea of removing barriers to cross-border co-operation and enhancing the freedom of movement within the region.

One significant hurdle for increased cross-sector collaboration is that businesses with a Nordic footprint lack adequate access to updated threat and security information and solutions for secure interaction with competent national authorities. This is a governmental responsibility and requires attention. Common initiatives across security authorities to provide open threat assessments would therefore be relevant for businesses working on risk management. One such initiative comes from Denmark, the tele-CERT proposal for how businesses and governments can collaborate more closely on cyber-security, integrating private sector capabilities into national and regional defence strategies.

Another example, specific to Norway but with the potential for wider Nordic application, is the Norwegian Business and Industry Security Council (Næringslivets Sikkerhetsråd – NSR). NSR is developing a new concept to enhance security and preparedness within the business sector. Their goal is to establish a Business Preparedness and Security Centre (NBSS), which will strengthen both physical and digital security, as well as overall preparedness in Norwegian businesses. The NBSS is designed to complement, not replace, existing collaboration between businesses and public authorities where those mechanisms are already effective. NSR sees significant value in integrating digital and physical security with preparedness under one framework. A key feature of the NBSS will be its capacity to send and receive warnings, ensuring that businesses are informed and prepared for any type of incident. For small and medium-sized businesses, which may struggle with the distinctions between these areas, the NBSS will offer predictability and clarity. Moreover, the NBSS will streamline communication between the business sector and public authorities, providing a unified point of contact that enhances co-operation and efficiency.

Telenor Nordics supports establishing closer co-operation on preparedness and crisis management. For such co-operation to be effective, governance and collaboration frameworks need to be formalised, especially regarding mechanisms for two-way information sharing. This requires significant speed and direction. It is also aligned with the NIS Co-operation Group's report that recommends enhancing resilience through improved co-operation and information sharing among stakeholders. Alignment across the Nordics would significantly enhance collective security and preparedness.

Three elements are fundamental for a robust total defence:

Strong societal resilience, cross-sectoral situational awareness, and the willingness and ability for mutual support and co-operation.

Source: *Report to the Norwegian Total Preparedness*

Procurement requirements for preparedness

Increased expectations for businesses in the context of increased preparedness levels result in higher costs. A report from the Confederation of Swedish Enterprise highlights a critical dilemma: "...a company's ability to survive and develop depends on the ability to get paid for the work performed." Both large and small business actors who have the capacity and wish to contribute to increased security and resilience face a significant challenge: few customers have the incentive or willingness to pay suppliers daily for the ability to deliver products or services continuously during war.

For business actors, predictable framework conditions and contract predictability are essential for making investment decisions. The Norwegian Defence Research Establishment (FFI) has identified challenges related to delivering services in the upper part of the crisis spectrum. This places entirely different demands on both authorities and businesses and will require new forms of co-operation and ways of working. This is challenging, but change can be facilitated within the framework of strategic partnerships.

Danish initiative: Nordic Tele-CERT – strengthening cyber-security across borders

Denmark, through a proposal from Teleindustrien, Dansk Erhverv, and DI (as outlined in their joint political initiative on Digital Infrastructure 2025–2030), has suggested the creation of a Nordic tele-CERT. This initiative is aimed at fortifying cyber-security co-operation across the Nordic region. The concept suggests the creation of a collaborative framework, similar to a Computer Emergency Response Team (CERT), that would operate at a regional level across the Nordic countries to address cyber-security threats and incidents affecting telecommunication infrastructure. This tele-CERT would involve the collaboration of telecommunications companies and possibly other stakeholders across the Nordic region to share intelligence, coordinate responses to cyber threats, and strengthen the overall security posture of the telecommunications sector.

The price of preparedness: can businesses sustain total defence demands?

The conditions for companies to survive and develop depend on their ability to get paid for the work they perform. Products or services that no one is willing to pay for in the long term will not survive and will be outcompeted. Businesses that carry too high a risk in relation to potential profits, and operations that incur higher costs than competitors, cannot survive in the long term. Increased expectations for companies to plan for their Total Defence needs lead to higher costs. Very few customers have the incentive or willingness to pay their suppliers on a daily basis to ensure that goods or services can be continuously delivered during wartime.

From the Confederation of Swedish Enterprise: *Konkurrenskraftiga företag stärker försörjningsberedskapen och totalförsvaret, Strategic Recommendations for Industry, February 2024 (translated)*

Security legislation creates barriers

National autonomy refers to the requirement that critical telecoms functions and their operations should be located within national borders. Authorities in all Nordic countries have, in different ways, tightened legislation and regulations related to national security. For telecom operators and their Nordic suppliers, a major challenge is the lack of alignment among national security laws in areas that affect cross-border co-operation and operations across these countries. Recent years have seen a trend towards fragmentation, which has unfortunately reduced the ability of businesses to build security based on common Nordic solutions. Further, the inability to share IT systems between Nordic countries due to these regulatory differences not only increases operational costs but also compromises security by necessitating the development of isolated, locally developed solutions.

For Telenor Nordics, fragmented security legislation in areas affecting cross-border co-operation and various national autonomy requirements mean we must dismantle systems, infrastructures, and competence we have built over years. This trend also impacts our suppliers, who have sought to establish "Centres of Excellence" in the Nordic region in recent years, an organisational setup that now is at risk of no longer functioning effectively. Such centres could also serve as hubs of innovation and training, attracting top talent and fostering cutting-edge research and development in cyber-security and related fields. Beyond enhancing the region's digital resilience, such co-operation can significantly boost Nordic innovation and competitiveness and attract international investment and position the Nordics as a leader in digital innovation and cyber-security.

The telecom industry is inherently international and technology-driven, relying primarily on international equipment suppliers. These suppliers typically have numerous offices in various countries, many of which are outside both Europe and NATO. It is natural and necessary for all telecom operators to use these suppliers to develop, maintain, and support the platforms they sell to remain relevant. It is neither practical, desirable from a quality perspective, nor economically viable to exclusively limit the set of suppliers. At the same time, it is extremely challenging to security-clear and authorise the entire supply chain. However, we acknowledge the criticality of supply chain security as set out in the NIS Co-operation Groups report.

As more businesses are likely to become subject to security laws, this challenge will only grow. This should be a serious concern for responsible authorities and represents a setback for Nordic co-operation, innovation, and effective competition. Telenor is also concerned that national "control" is being defined as national "ownership," which can undermine the broader framework that includes Nordic and NATO interests. We safeguard both national and our own interests within this framework and believe that a more integrated approach is crucial.

Leveraging opportunities in Nordic co-operation

Telenor's top priority for improved preparedness is a Nordic initiative aimed at overcoming obstacles to regional co-operation. By exploring solutions to better utilise scarce personnel resources between neighbouring Nordic countries and leveraging shared technical infrastructure such as fibre networks and data centres, we can enhance national supply security with more resources readily available near all countries in the Nordic region. This collaborative approach will also strengthen the Nordic region as a whole and encourage multinational technology providers to establish competence centres within the Nordics.

The Norwegian government on Nordic Integration:

"The government sees a clear need for Norway to adopt a highly unified approach with our Nordic allies regarding civil support for military forces. On the military side, close co-operation has already begun. However, close collaboration and direct coordination between civilian sectors in the three countries are also necessary. There is ongoing preparedness co-operation between certain civilian sectors and actors with counterparts in the Nordic countries. For instance, agreements have been made on crisis trade and supply co-operation between Norway, Finland, and Sweden. The government recognises the need to further strengthen Norway's civil preparedness co-operation with Finland and Sweden to support the collective ability to provide effective civil support to military forces in times of war."

From:
Prop. 87 S (2023-2024) The Norwegian Defence Pledge Long-term Defence Plan 2025–2036

There's no time to waste

Telenor Nordics expects Norwegian authorities to take concrete initiatives in their upcoming White Paper on Total Preparedness to follow up on the Total Preparedness Commission's proposals for co-operation on digital security and increased preparedness in the Nordics. Such co-operation will necessitate changes and carefully considered adjustments and targeted alignmentof national regulations in areas affecting cross-border co-operation. The Nordic industry can contribute to solutions within a Nordic and allied framework in areas such as mobile core networks, data centres, and transport networks. It is imperative to initiate these efforts promptly and for leadership on stepping up Nordic co-operation in the digital realm.

Realistic training and exercises

To prepare for new threats in our neighbouring areas, it is important for the Nordic countries to engage in targeted training and well-planned exercises that simulate previously unthinkable scenarios. These exercises should prioritise real-world challenges and scenarios that reflect the current threat landscape. By conducting across sector training, we can better understand the interdependencies among businesses and gain insights into potential ripple effects and the scope of actual crises.

Since 2017, Telenor Norway has organised 'Exercise Bukkesprang,' Norway's largest cross-sector 'live fire' exercise in digital incident management, in collaboration with the Norwegian Armed Forces Cyber Defense (Cyberforsvaret) and, since 2023, with the National Security Authority (NSM). This exercise aims to strengthen Norway's total defence and is a significant contribution to digital total preparedness.

Another notable example of a collaborative defence effort is the Nordic Response 2024 exercise, which involved more than 20,000 troops from 13 allied nations, demonstrating NATO's capability to defend the Nordic countries.[5] This exercise included extensive military and civilian co-operation, highlighting the importance of integrated training for both military and civilian emergency services. Further, the annual Exercise Locked Shields, organised by the NATO Co-operative Cyber Defence Centre of Excellence (CCDCOE) in Estonia, is the world's largest and most complex live-fire cyber defence exercise. Locked Shields 2024 involved 4,000 experts from over 40 countries, focusing on protecting critical infrastructure from cyber threats using cutting-edge technologies such as artificial intelligence and 5G. This exercise underscores the importance of international co-operation in cyber-security, preparing nations to face sophisticated cyber threats as a coalition.

In Norway, the Directorate for Civil Protection (DSB) will lead the planning, execution, and evaluation of digital exercise in 2025 in co-operation with the National Security Authority (NSM). The aim is to strengthen society's resilience against digital attacks by involving civilian sectors, the Armed Forces, and private industry to test and enhance Total Defence capabilities.

To maintain and enhance preparedness and response, Telenor supports continued interaction in incident management and security exercises involving businesses. There is a need for cross-sector training arenas to test co-operation, coordination, and leadership. A key shortfall is the lack of common platforms for information sharing. Increasing the use of exercises both within and across markets can strengthen co-operation and leadership at all levels, build knowledge of capabilities, and develop essential networks. By focusing on realistic training, the Nordic countries can significantly enhance their preparedness for various threats, ensuring robust and coordinated crisis responses.

» Since 2017, Telenor Norway has organised 'Exercise Bukkesprang,' Norway's largest cross-sector 'live fire' exercise in digital incident management.

5 https://www.forsvaret.dk/da/nyheder/2024/falles-nordisk-luftoperationscenter-i-luften-for-forste-gang/

Digital exercise 2025 in Norway

The Directorate for Civil Protection (DSB) has been tasked with leading the planning, execution, and evaluation of Exercise Digital 2025. This exercise is to be planned in close co-operation with the National Security Authority (NSM). The aim of the exercise is to strengthen society's ability to withstand digital attacks. The exercise will take place in the autumn of 2025 and will involve entities from civilian sectors, the Armed Forces, and private industry.

The exercise is intended to test the total defence's ability to detect, manage, and coordinate a complex digital incident across sectors. Additionally, it will assess the total defence's ability to communicate and co-operate during the management of the consequences of the digital incident.

From DSB: *Totalforsvarsøvelse - Øvelse Digital 2025*

Willingness to change

In today's rapidly evolving security landscape, it is imperative for Telenor to utilise our employees across the Nordic region, employ supplier personnel in our four markets, and share technical solutions and infrastructure across borders. Our ambition is to protect communication, content, and critical infrastructure without delay.

In an increasingly complex world with mounting pressures on talent and expertise, and a growing concentration of the supplier market with extended supply chains, each Nordic country individually becomes too small. Telenor therefore advocates for the establishment of a coordinated Nordic approach to security clearance and authorisation of personnel. While each country would continue to handle its own clearances, following aligned and streamlined principles are essential for seamless cross border co-operation. This approach should also include targeted initiatives on shared transport networks, mobile core networks, and data centres, enhancing resilience while upholding national autonomy.

The time for action is now. To achieve these goals, we must foster close technical co-operation between companies and organisations across borders, driven by results-oriented leadership. Achieving this will require balanced harmonisation of security legislation in areas hindering cross-border co-operation and significantly increased levels of collaboration between national regulators. Recent initiatives, such as the Nordic Defence Co-operation's (NORDEFCO) Vision 2030, emphasise the need for closer collaboration among Nordic countries to enhance joint military and civilian preparedness. This vision calls for strengthening of our collective defence strategies within NATO's framework.[6] In addition, the Nordic Council's exploration of deeper regional cyber-security co-operation highlights the urgent need for integrated efforts to address shared threats and enhance resilience across the region.[7]

Collaboration initiatives such as the Haga Co-operation have already proven effective for political and administrative coordination within civil emergency preparedness. With Sweden and Finland now part of NATO, there are significant opportunities to expand military co-operation on resilience, further solidifying Nordic collaboration and ensuring comprehensive regional security.

A united Nordic region within NATO provides a historically strong security policy foundation for changing attitudes and culture. By intensifying security co-operation across the Nordic region without delay, we vastly improve conditions for ensuring an effective, secure, and robust total defence. The stakes are too high to postpone action. We are committed to making the necessary changes now, as there is no time to waste.

6 https://www.nordefco.org/New-Vision-for-Nordic-Defence-Cooperation-2030

7 https://www.norden.org/en/event/nordic-day-2024-navigating-nordic-futures-strengthening-cooperation-peace-and-security

Telenor's call to action for Nordic governments and public authorities:

1. **Establish a Nordic regime for security clearance and authorisation:**
   Develop a coordinated Nordic framework for security clearance and authorisation of personnel, guided by shared principles. This framework would streamline the process of clearing and authorising personnel across borders, enabling more efficient cross-border co-operation while maintaining high security standards

2. **Operationalise national autonomy requirements:**
   Review and design national autonomy requirements to allow for cross border co-operation where appropriate. This approach facilitates the sharing of technical solutions and infrastructure in key geographical areas, ultimately enhancing robustness and resilience throughout the region. It strikes a balance between maintaining national sovereignty and leveraging the practical benefits of Nordic collaboration

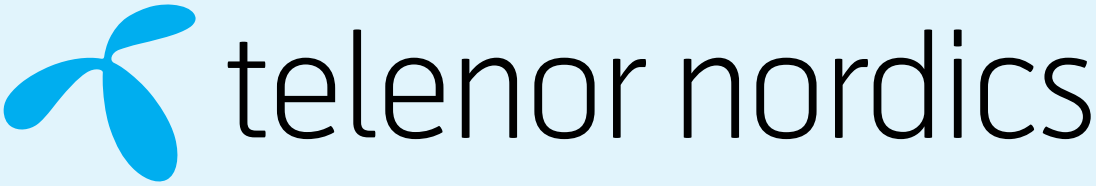
3. **Enhance information sharing:**
   Establish robust solutions for interaction and facilitate better access to two-way sharing of threat and security information between the public and private sectors, as well as between affiliated private-sector entities across the Nordics. This approach will ensure that both key defence actors and businesses operating in multiple Nordic regions are better equipped to respond effectively to evolving threats

4. **Integrate long-term preparedness in public procurement:**
   Implement requirements that ensure long-term preparedness and national security interests are safeguarded in public procurement processes. This is crucial as economic factors play a key role in maintaining a sustainable and secure infrastructure

Telenor

Snarøyveien 30
N-1360 Fornebu
Norway

www.telenor.com



Read the report online:

https://www.telenor.com/about/our-companies/nordics/digitalsecurity/2024