Risk Assessment of the Norwegian Electronic Communications Sector 2021

A Changing Sector

Norwegian Communications Authority

Photo: Gunstein Myre

Table of Contents

Summary 4

1. Experience from 2020 and the first half of 2021

Resumé 7

A period with few major outages in the electronic communications networks 8

Fibre breaches and mobile outages dominate notifications to Nkom 9

Still many GPS disruptions in Troms and Finnmark 10

Extensive phone fraud, although much is stopped 10

Increased digital attack activity 11

2. Threat and risk assessment

Resumé 13

Complex division of responsibility for the security of new 5G applications 14

Need for comprehensive protection of the national data centre infrastructure 16

Smaller providers could be attractive targets for new threats 18

The electronic communications infrastructure is exposed to weather conditions that are becoming more extreme 20

Front page photo: Anders Martinsen

Summary

In the years ahead, the Norwegian electronic communications sector will undergo major changes. An important driver is 5G, and the new opportunities that this technology brings to the smart community, to business and to industry.

New ecosystems and solutions within mobile and broadband services will characterise the electronic communications sector. We will see a greater convergence between fixed and wireless services, internet-based services and platforms, cloud services and data centres, and specialised/niche-based communications solutions. The result will be better and more efficient services, but also increased complexity.

For the sector to contribute to greater efficiency, innovation and business development in Norway, there must be inherent confidence in the fundamental digital infrastructure and services. The sector enjoys this trust today, and Norway is one of the world's most digitalised countries. However, the public sector, business and industry will be reluctant to adopt *new* solutions, for example based on 5G, if they do not have confidence that quality and security can be safeguarded.

Nkom sees a risk that new solutions and increased complexity may lead to uncertainty concerning who is responsible for security. In this respect, it is important that the electronic communications authority, the players in the electronic communications sector and the users – including business and industry – collaborate proactively to identify and deal with emerging challenges.

Confidence in the fundamental digital infrastructure and services will also be strongly challenged by external factors. In the logical domain, increased digital threat and attack activity is expected. The severity of the potential threats is emphasised by the serious digital attacks on critical functions in Norwegian society seen during the past year.

In the physical domain, the UN's new climate report states that we must expect further extreme weather conditions in the years to come. Nkom sees a particular need to strengthen regional and access networks. This will require increased investment in resilience, redundancy and reserve power supplies in the sector.

About the report

- This report is a brief description of Nkom's annual risk assessment of the electronic communications sector (EkomROS). The report will provide direction for authorities, enterprises in the sector, and enterprises outside the sector, for which electronic communications is a critical input factor.

- Nkom's assessments are based on knowledge and experience from management and supervisory work in the sector, and from EkomCERT. The assessments are also based on the threat and risk assessments made by the Norwegian security authorities (NSM, PST and the E-service).

- Nkom's website has more information about risk assessments concerning electronic communication. Here, municipalities, county governors, and public and private enterprises can find guidance for performing their own risk analyses of electronic communications.

Photo: Gunstein Myre

1
Experience from 2020 and the first half of 2021

Resumé

- There were few major outages in the electronic communications networks during the period, but the number of outages notified to Nkom increased. Fibre breaches still dominate the notifications, accounting for 50 per cent of all notifications.
- The scale of GPS disruptions in Troms and Finnmark persists. During the period, Nkom was notified of 12 incidents that affected aircraft and helicopter traffic in the county.
- There is a high prevalence of phone fraud, even if the operators manage to stop much of the fraudulent traffic. Nkom is an active driving force in reducing the extent of this fraud.
- Digital attacks have increased in volume and become more sophisticated. This is affecting all sectors, including the electronic communications sector. Norwegian electronic communications providers have had to handle ransom demands, with threats of extensive denial-of-service attacks.

Photo: Gunstein Myre

A period with few major outages in the electronic communications networks

In 2020 and the first half of 2021, there were few incidents involving major outages in electronic communications networks and services. Throughout the period, only three storms were defined as extreme weather conditions by the Norwegian Meteorological Institute, two of which were due to extreme flood levels. The third was the extreme weather phenomenon, "Frank", which hit northern Norway in January 2021, causing strong winds. The storm only led to minor, scattered mobile network coverage outages.

Measurements of accessibility and stability in the Norwegian mobile networks, which are carried out annually by CRNA[1], also show good results in 2020. The measurements in 2020 were based on 147 measurement points spread across Norway and connected to Telenor, Telia and ICE's mobile networks. Availability in 2020 exceeded 99.99 per cent at 60 to 80 per cent of the 147 measurement points, and the data connection performance was stable.

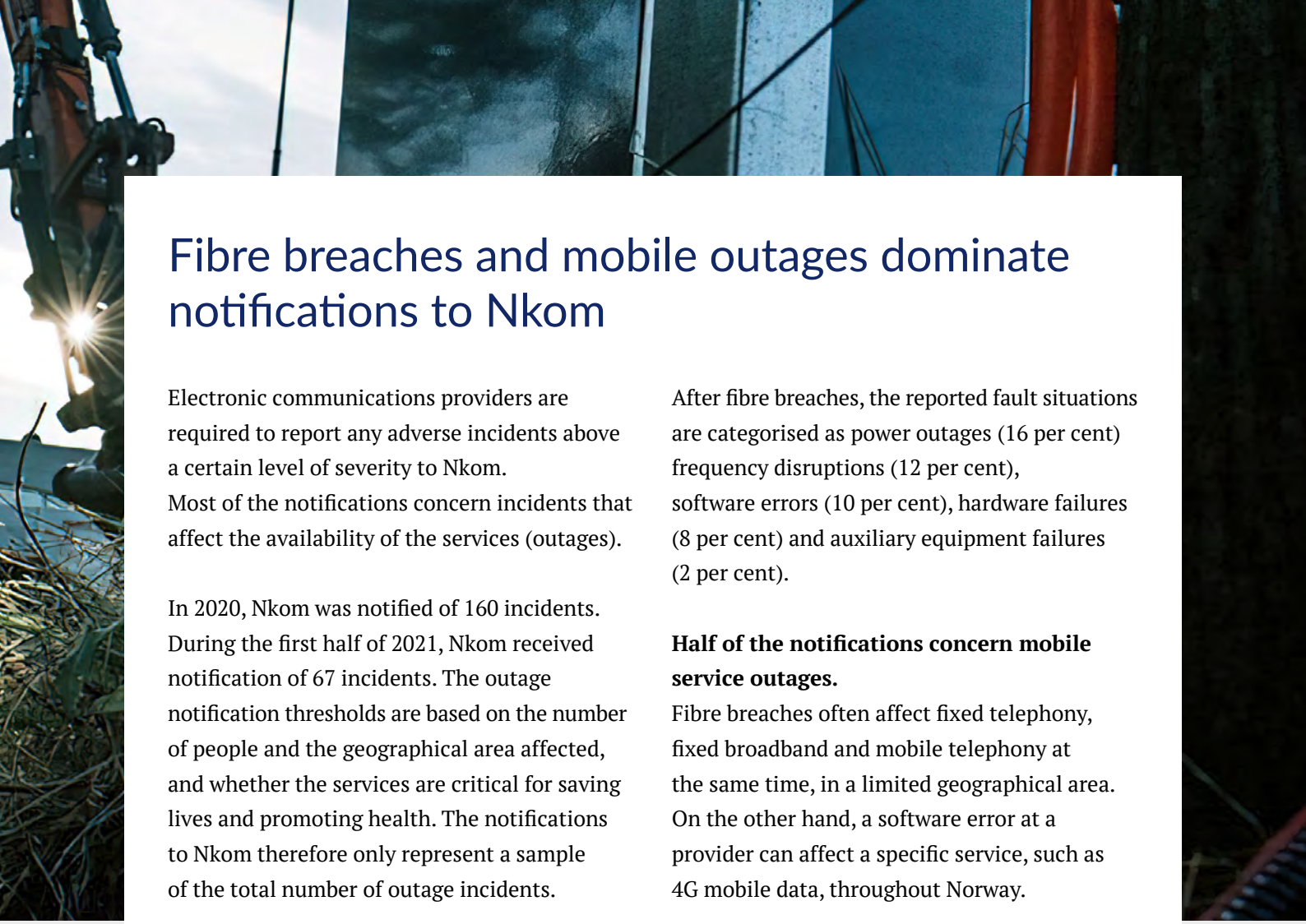
Quick clay landslide at Gjerdrum

The quick clay landslide at Gjerdrum on 30 December 2020 prompted an intense and complex rescue operation that involved the rescue services, private organisations, voluntary organisations and the Norwegian Armed Forces. Emergency networks were vital for coordination and interaction, and were continuously operational, even though capacity was challenged in some periods.

The mobile networks of Telenor, Telia and ICE were also operational throughout the incident and provided important coverage in the affected area. The mobile operators continuously reported their operational status to Nkom, and also assisted the emergency rescue services with electronic tracking.

The next generation of emergency and rescue communications services will be implemented in the commercial mobile networks. The Norwegian Directorate for Civil Protection (DSB) led the work on a concept evaluation report, in collaboration with Nkom.

[1] "Norske mobilnett i 2020" (Norwegian mobile networks in 2020), Status report from the Centre for Resilient Networks and Applications, Simula, 2021.



Fibre breaches and mobile outages dominate notifications to Nkom

Electronic communications providers are required to report any adverse incidents above a certain level of severity to Nkom.
Most of the notifications concern incidents that affect the availability of the services (outages).

In 2020, Nkom was notified of 160 incidents. During the first half of 2021, Nkom received notification of 67 incidents. The outage notification thresholds are based on the number of people and the geographical area affected, and whether the services are critical for saving lives and promoting health. The notifications to Nkom therefore only represent a sample of the total number of outage incidents.

Half of the outages are due to fibre breaches.
This is the same picture as in 2019 and 2018. Fibre breaches are often due to accidents in connection with excavation and construction work, and adverse weather conditions. The distribution of other types of incidents is also relatively similar to the situation in 2019 and 2018.

After fibre breaches, the reported fault situations are categorised as power outages (16 per cent) frequency disruptions (12 per cent), software errors (10 per cent), hardware failures (8 per cent) and auxiliary equipment failures (2 per cent).

Half of the notifications concern mobile service outages.
Fibre breaches often affect fixed telephony, fixed broadband and mobile telephony at the same time, in a limited geographical area. On the other hand, a software error at a provider can affect a specific service, such as 4G mobile data, throughout Norway.

Experience shows that mobile service outages have a great impact on people's everyday lives and sense of security. Of the reported incidents, around half concerned mobile service outages, such as mobile voice, mobile broadband and/or messaging services. The second most common impact on services was outages in fixed broadband services.

Incidents by category

- Fibre breaches (50%)
- Power outages (16%)
- Frequency disruptions (12%)
- Software errors (10%)
- Hardware faults (8%)
- Auxiliary equipment faults (2%
- Other (2%)

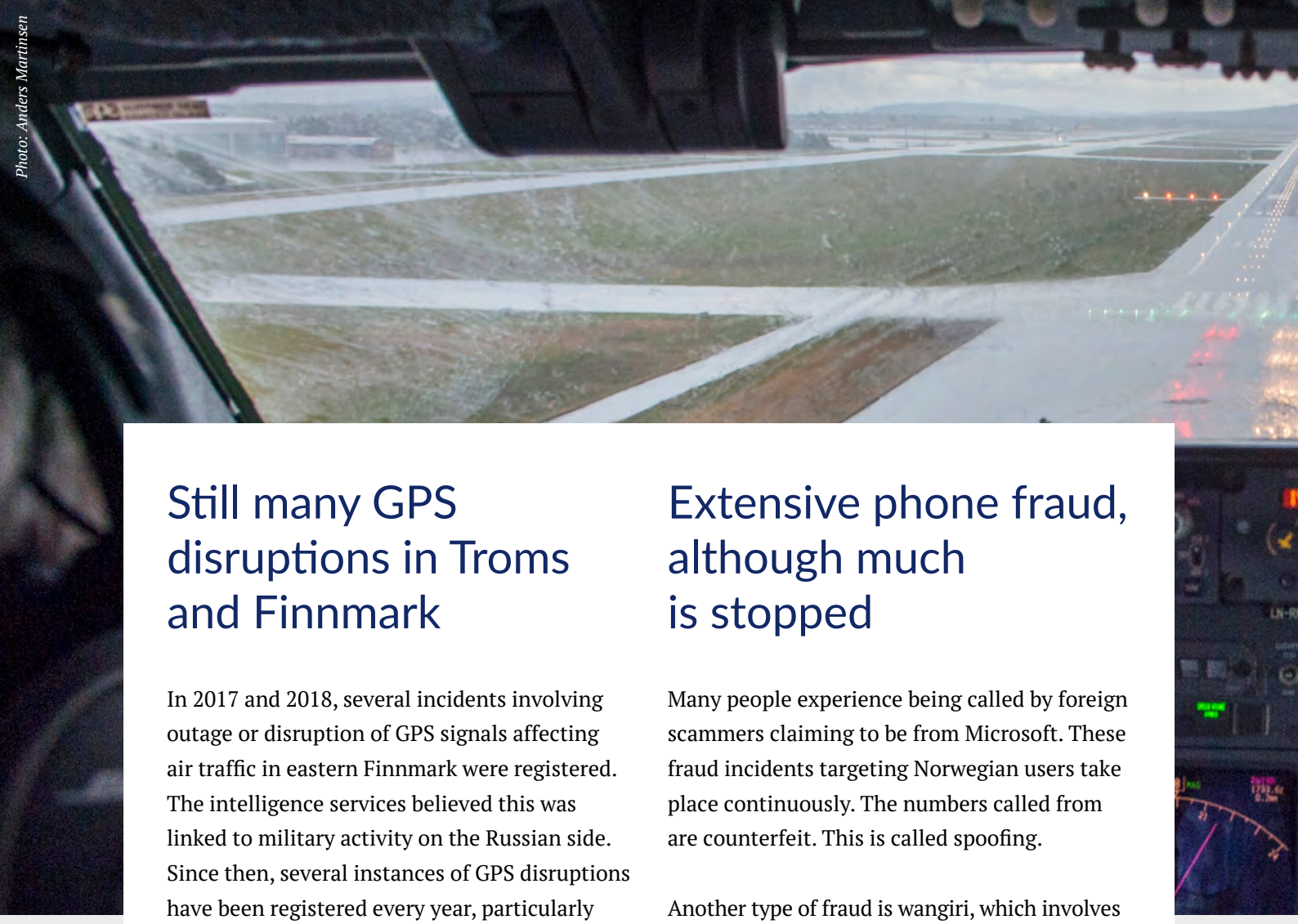


Photo: Anders Martinsen

Still many GPS disruptions in Troms and Finnmark

In 2017 and 2018, several incidents involving outage or disruption of GPS signals affecting air traffic in eastern Finnmark were registered. The intelligence services believed this was linked to military activity on the Russian side. Since then, several instances of GPS disruptions have been registered every year, particularly in Troms and Finnmark.

In January 2020, in cooperation with Avinor and the Civil Aviation Authority of Norway, Nkom established a separate warning scheme concerning disruptions of navigation satellite systems. During 2020 and the first half of 2021, Nkom received 12 notifications of GPS outages in aircraft and helicopters in Troms and Finnmark.

In total for the entire country, GPS disruptions are an increasing trend, although fewer incidents were registered in 2020 than in 2019.

Extensive phone fraud, although much is stopped

Many people experience being called by foreign scammers claiming to be from Microsoft. These fraud incidents targeting Norwegian users take place continuously. The numbers called from are counterfeit. This is called spoofing.

Another type of fraud is wangiri, which involves scammers calling up and then cutting the line from a premium-rate number, to entice the user to call back and be charged for the call.

Providers have taken several measures that have significantly reduced the incidence of spoofing and wangiri. Nkom is actively driving this work. However, this is an ongoing battle against international crime, where it is not possible to stay abreast of all new fraudulent schemes.

Another significant fraud trend in 2021 is Flubot. Mobile users receive a text message, e.g. disguised as a text about a parcel delivery, but with a link to an app or website controlled by scammers. Telenor report that they stop around 20,000 of such scam messages per day.[2]

[2] "Valgene vi tar - Digital sikkerhet 2021" (The Choices we Make - Digital Security 2021), Telenor, 2021

Increased digital attack activity

Cyberattacks affected businesses in every sector during the past year. The most discussed in Norway are the data breaches affecting the Storting (Parliament) in autumn 2020 and spring 2021, and the ransomware virus attack on Østre Toten Municipality in January 2021.

In December 2020, it became known that threat operators had established backdoors in the Orion software of the American software provider, SolarWinds. The software is used by various businesses to manage networks, systems and IT infrastructure. This vulnerability, which could be exploited for remote code execution, was spread via software updates to over 18,000 business customers. Norwegian business customers were also affected.

Attacks of this type are called value chain attacks, or supply chain attacks, and can affect operators in every sector. Several attacks of this nature were registered during the past year, and more are expected in the future.

In 2020 and 2021, as in previous years, the electronic communications providers handled an increasing volume of distributed denial-of-service (DDoS) attacks. These attacks target both the provider's customers and the provider's own network infrastructure.

DDoS ransom demands

A clear trend during the past year has been DDoS attacks combined with ransom demands. In these instances, businesses have been subject to a 'limited' denial-of-service attack, followed by a ransom letter threatening a significantly more powerful attack unless a ransom is paid in cryptocurrency.

During this period, several DDoS extortion campaigns took place internationally (see fact box). The campaigns also affected operators in Norway. This type of attack is also offered and traded as services between criminal operators.

On several occasions, EkomCERT (security incident response team for the telecom sector, established at the Norwegian Communications Authority) advised Norwegian providers who were affected. The advice was based on experience from EkomCERT's international collaboration network and was used by the providers as a basis for risk assessments and to take more effective countermeasures.

Nkom EkomCERT

Nkom EkomCERT is the Norwegian electronic communications sector's digital response environment, and constitutes an operational unit with national and international points of contact. EkomCERT works closely with the electronic communications operators' security organisations, the Norwegian National Cyber Security Centre (NSM NCSC) and other sector response environments (SRM).

EkomCERT has cutting-edge expertise in the digital vulnerability and threat picture in general, and sector-specific challenges in particular. In the event of serious digital incidents, EkomCERT provides assistance to the electronic communications operators in the form of information collection, advisory services and coordination.

EkomCERT is a member of the global security organisations FIRST and Trusted Introducer.

www.nkom.no/sikkerhet-og-beredskap/nkom-ekomcert

Photo: GreenMountain

2
Threat and risk assessment

Resumé

- 5G will create completely new ecosystems, and the responsibility for security will be considerably more complex. One risk created by this complexity is an unclear division of responsibility between providers, suppliers and customers. Unclear division of responsibility can delay innovation and development facilitated by 5G technology.

- The electronic communications infrastructure is increasingly converging with the data centre and cloud service infrastructure. Data centres and cloud services deliver a high degree of security to their customers. There is nonetheless a risk that the national data centre infrastructure *as a whole* is not adequately protected to meet society's needs in times of peace, crisis and war.

- Increased digitalisation is expected in manufacturing and commerce throughout Norway, and people will continue to work from home. Nkom expects local and regional electronic communications providers to be a more important part of the value chain for the new digital services. The smaller electronic communications providers may not be as well-equipped as the larger providers to withstand advanced threats and attacks. This will increase the risk of them becoming more attractive targets for digital attacks.

- The Norwegian electronic communications infrastructure will face increased stresses from nature in the years to come. At the same time, society's digitalisation will impose ever stricter requirements to ensure the stability and accessibility of the digital infrastructure. Nkom can see a particular need to strengthen the regional and access networks. If confidence in the resilience of the electronic communications infrastructure is undermined, this may weaken the rate of digitalisation.

Photo: unsplash

Complex division of responsibility for the security of new 5G applications

The mobile operators are currently expanding with new 5G base stations that provide increased speed and capacity, while still using core networks based on 4G technology. The full potential of 5G will be realised during the next couple of years when operators also implement the 5G technology in the core network. This will facilitate completely new application areas in industry and business, massive IoT and critical communications services.

With 5G, the mobile networks will become a cloud-based architecture that facilitates dynamic and scalable solutions adapted to various types of user needs. Mobile networks can be divided into several virtual mobile networks (disc sharing), with dedicated resources and characteristics for various different uses. Services can be produced at different locations, both centrally and locally (edge computing), and are operated on the basis of various types of models, such as private, public or hybrid 5G networks.

Many different user scenarios and operating models will challenge providers, suppliers and any third-party operators, and users of the services, to clarify responsibility for the security of 5G service performance. Nkom is also aware that there may be regulatory grey zones in these intersections.

If important security responsibilities are not sufficiently clear, this can lead to error situations and vulnerabilities that can undermine confidence. In turn, this could put obstacles in the way of further innovation and development facilitated by 5G technology.

5G frequency auction – an important milestone

An important milestone in Norway's 5G expansion was reached on 30 September 2021. This was when Nkom completed the auction of important 5G frequencies in the 2.6 and 3.6 GHz bands.

The frequencies were awarded to Altibox, ICE, Telenor and Telia for a total price of almost NOK 3.9 billion.

The frequencies include special obligations for broadband expansion in rural districts, and obligations towards industrial and commercial operators, so that they can introduce 5G for new industrial applications.

Measures

Nkom will contribute to identifying and handling any regulatory challenges concerning new 5G applications. Arenas for identifying current issues include the 5G Special Interest Group (5G SIG), on which Nkom and NSM collaborate.

Electronic communications providers should raise awareness of responsibility for security in the development of new 5G services and applications for business customers. They should spotlight the security pros and cons of various types of user scenarios.

Municipalities and other public and private enterprises should undertake exhaustive risk assessments to find suitable models adapted to the needs of their own business activities. They should ensure the transparency and clarification of responsibility for security between their own activities, providers and any third-party operators.

Photo: GreenMountain

Need for comprehensive protection of the national data centre infrastructure

In recent years, the Norwegian data centre industry has made significant investments. This is a very positive contribution to the goal of strengthening Norway's position as a data centre nation, thereby facilitating the production of cloud services in Norway.

Data centres are increasingly becoming an integral part of the electronic communications infrastructure – the digital foundation. In addition to electronic communications providers delivering connectivity to and between data centres, the providers' own services are also increasingly being produced as cloud services in data centres. This applies particularly to 5G mobile services.

The enterprises that are to use cloud services, or who place their own equipment in data centres, are responsible for ensuring their own security. Cloud service providers and data centre operators will then, as 'subsuppliers', be subject to the requirements set by customers.

At the same time, data centre operators are not currently subject to comprehensive national security and emergency preparedness regulation. This leaves a risk that the overall national data centre infrastructure, with the accumulated societal values held in the data centres, is not adequately protected in order to meet society's needs in peacetime and at times of crisis and war.

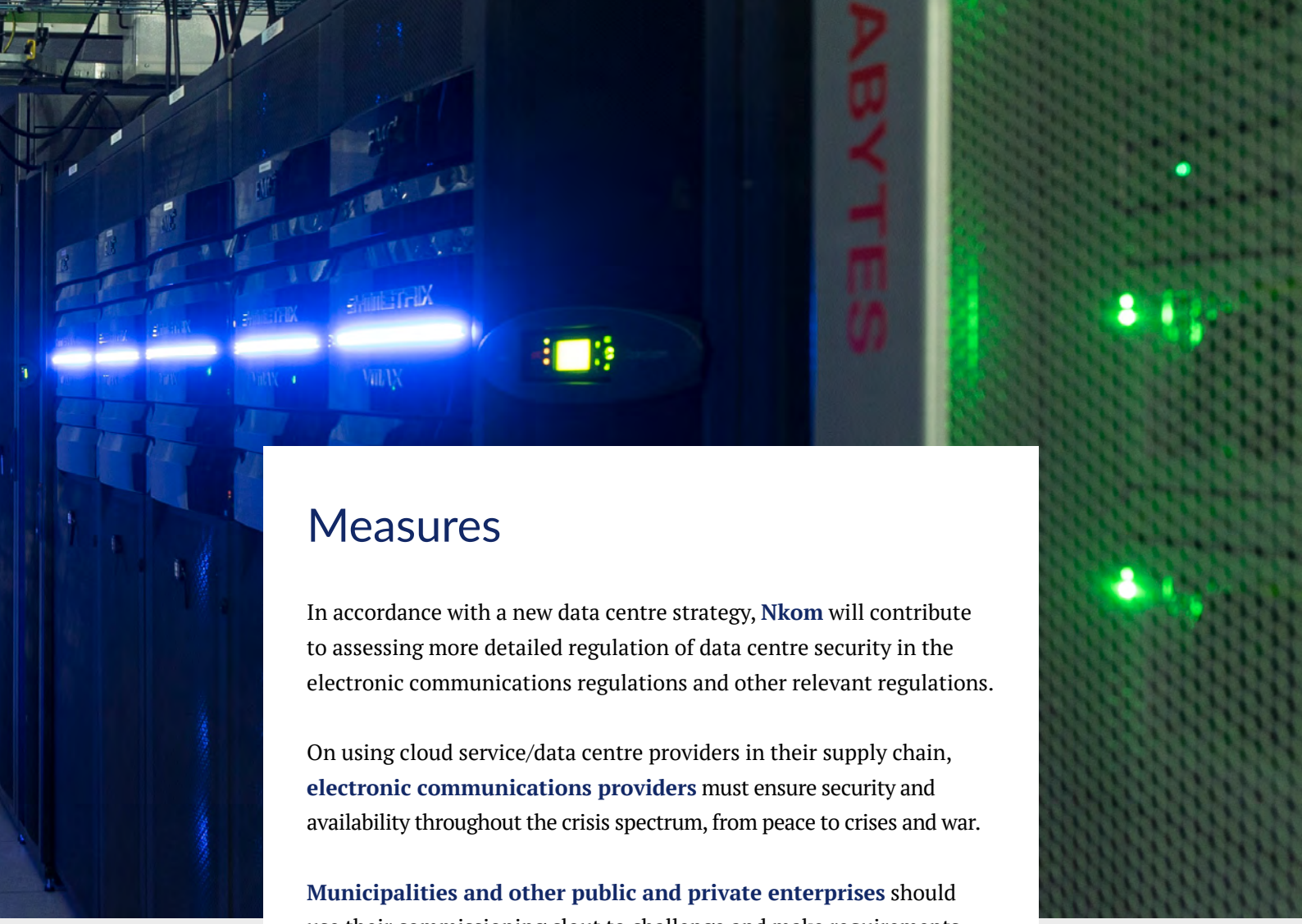
The Norwegian Government's new data centre strategy[3] provides for assessment of the strengthened regulation of data centre security within the framework of the Norwegian Electronic Communications Act. Nkom considers this to be appropriate. New data centre security requirements must also be balanced against the need for competition, business development and innovation. This is important in order to help to ensure that special security requirements do not create unnecessary entry barriers for cloud services and data centres in Norway.

In its risk assessment for 2021[4], **NSM** points to the extensive prevalence of cloud technology and cloud services. Cloud service providers often deliver more innovative and secure solutions than individual businesses themselves have the capacity and expertise to achieve.

The question is how the security of the services functions in a critical security policy situation. Major cloud service providers are often located abroad. They are based on digital infrastructure that crosses many borders and is vulnerable to sabotage, damage and security policy changes.

[3] "Norske datasenter – berekraftige, digitale kraftsenter" (Norwegian data centres – sustainable digital power centres), Norwegian Ministry of Local Government and Modernisation, 2021.

[4] "RISIKO 2021 – helhetlig sikring mot sammensatte trusler" (RISK 2021 – holistic protection from complex threats), Norwegian National Security Authority, 2021.



Measures

In accordance with a new data centre strategy, **Nkom** will contribute to assessing more detailed regulation of data centre security in the electronic communications regulations and other relevant regulations.

On using cloud service/data centre providers in their supply chain, **electronic communications providers** must ensure security and availability throughout the crisis spectrum, from peace to crises and war.

Municipalities and other public and private enterprises should use their commissioning clout to challenge and make requirements of their suppliers of electronic communications services concerning where/how the services are produced, and how security and accessibility are safeguarded, also in extraordinary situations.

Key milestones for the data centre industry in Norway

In 2021 and 2022, five new submarine fibre connections between Norway and abroad will be commissioned . These are Altibox's "Skagenfiber" (Larvik-Hirtshals), "Englandskabelen" (Stavanger-Newcastle), Bulk's "Mermaid" (New Jersey, USA – Kristiansand/Esbjerg) and "Havsil" (Kristiansand-Hanstholm). Tampnet has also expanded its submarine fibre network in the North Sea, with a new connection between Egersund and Aberdeen. These connections significantly strengthen the connectivity between Norway and abroad.

Photo: Nkom

Photo: Gunstein Myre

Smaller providers could also be attractive targets for cyberthreats

New technologies are facilitating increased digitalisation in manufacturing and business throughout Norway, including in rural districts. As a consequence of the coronavirus pandemic, the use of home offices has also increased. This means that local and regional electronic communications providers can come to play a more important role as part of the value chain for the new digital services.

Threat sources are expected to target these new digital services, as well as weaknesses in home office solutions. Nkom therefore expects that, as part of this value chain, the hundreds of local and regional electronic communications providers will also be targeted by these campaigns to a greater extent. These might be attacks targeting weaknesses in wireless access points, firewalls and access networks.

Security mapping inspection

In 2021, Nkom undertook a mapping inspection of security management, including digital security, at 20 electronic communications providers of varying sizes and geographical affiliations in different market segments.

The inspection shows that Nkom should continue to work with the smaller operators in particular, in order to manage the digital vulnerability and threat picture.

Attacks may also be directed at the providers' administrative IT systems as a gateway to their operating systems.

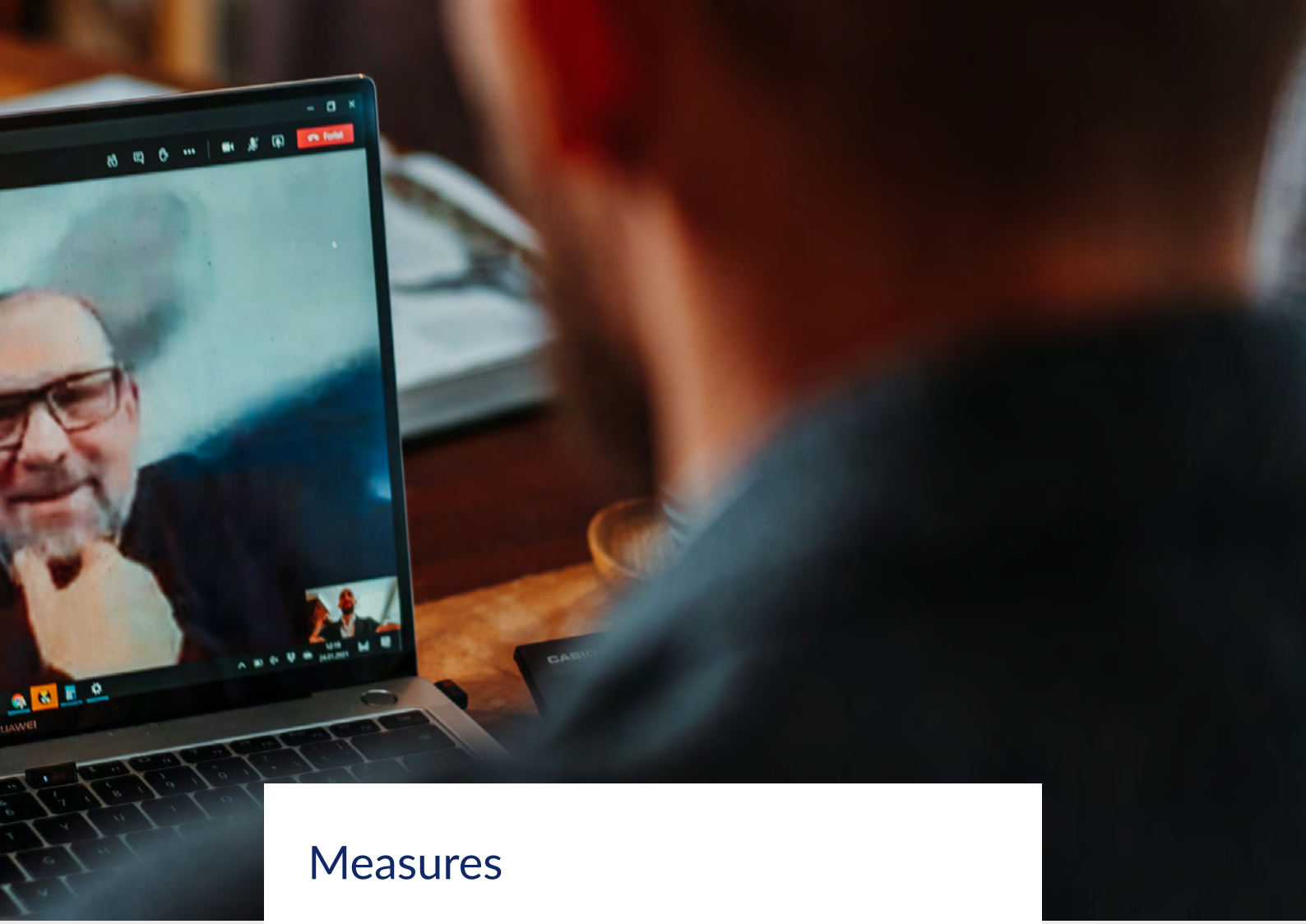
Many small operators do not have the same capability as large operators to build up their own security environments and expertise that are adequately dimensioned to ward off advanced digital attacks. On the other hand, digital security is increasingly becoming an important parameter of competition. In order to maintain market competitiveness, it is important that the smaller operators also scale up their digital security measures.

The National Security Authority describes the situation in 2021 as exacerbated, with a higher level of activity directed at Norwegian enterprises and institutions compared to previous years.

The Norwegian Police Security Service (PST) threat assessment for 2021[5] points out that foreign intelligence services will devote considerable resources to breaking into Norwegian data networks. The primary objective will be information gathering, but PST also expects operations aimed at manipulating information and sabotaging digital systems.

Foreign intelligence services will exploit reduced digital security mechanisms in home office solutions, among other things.

[5] "Nasjonal trusselvurdering 2021" (National threat assessment, 2021), Norwegian Police Security Service, 2021



Measures

Nkom is strengthening its digital security activities in the sector, with particular focus on the smaller industry players. Cooperation with the Norwegian National Cyber Security Centre and the other sector response communities is being further developed.

The electronic communications providers must assess, and manage, the risk of being the target of advanced digital attacks directed at their own customer portfolio and as a consequence of increased use of home offices. Providers can strengthen their collaboration with EkomCERT, among other things through EkomCERT's information and collaboration portal.

Municipalities and other public and private enterprises should adhere to the Norwegian National Security Authority's "Basic Principles of ICT Security". They should be aware that on using outsourcing and cloud services, and home offices, broadband/internet service providers are also a key element of the value chain that needs to be risk assessed.

Photo: Anders Martinsen

The electronic communications infrastructure is exposed to weather conditions that are becoming more extreme

The new Intergovernmental Panel on Climate Change report published in August 2021 states even more clearly than before that anthropogenic climate change has resulted in extensive changes in the atmosphere, oceans and ecosystems.

In the years ahead, the electronic communications infrastructure will be subject to stronger impacts in the form of extreme weather conditions and serious natural events. There may be more extreme wind conditions, extreme precipitation levels with subsequent landslides, snow/ice problems and flooding of rivers and watercourses. We must also expect prolonged periods of drought, with subsequent forest and outfield fires.

In 2020, the electronic communications industry invested a total of NOK 12.6 billion in electronic communications networks and services, the highest level of investment ever in any year. Much of the investment concerns providing *access* to electronic communications services, as the basis for increased digitalisation and greater efficiency in society.

This will gradually lead to even stronger dependence on this infrastructure. In addition, critical functions in society, such as emergency and rescue services, will be realised in the commercial networks. The investments must therefore increasingly be directed towards *strengthening* the infrastructure.

Nkom can see a particular need to reinforce the 'periphery' of the electronic communications networks, such as the regional and access networks. This part of the electronic communications infrastructure is most vulnerable to stresses from nature. This will require increased investment in robust networks, redundancy and reserve power supplies.

Regional analyses and cooperation with the power sector

In 2019, Nkom undertook a detailed mapping and vulnerability analysis of the electronic communications infrastructure in Finnmark. Several measures were implemented with government funding.

An equivalent analysis will be conducted in Troms in 2021, and Report to the Norwegian Parliament 28 (2020-2021) – *Our common digital foundation* – proposes at least five new regional analyses.

Nkom has also initiated a project together with the Norwegian Water Resources and Energy Directorate (NVE) to strengthen cooperation with the power sector on emergency preparedness.

Measures

Nkom will follow up the strategy for a secure and robust electronic communications infrastructure in Report to the Norwegian Parliament 28 (2020-2021) – *Our common digital foundation.* Nkom is also working on revising the targets for the electronic communications infrastructure published in the "Robuste og sikre nett" (Robust and Secure Networks) (ROBIN) report from 2017.

In the development of new infrastructure, the **electronic communications providers** must give weight to climate adjustment measures. Security and resilience are increasingly becoming a competitive advantage. Providers should therefore raise awareness, provide guidance and cooperate with customers on security- and resilience-enhancing measures.

Municipalities and other public and private enterprises should assess natural risks and vulnerabilities regarding their own municipality/ activities and apply this assessment to the procurement of critical electronic communications services. They should assess alternative security solutions and products, and any independent backup solutions. For major procurement projects, reinforcement of the infrastructure may be an element of the negotiation with the provider. There should be an access obligation requirement for other providers of such reinforcement, in order to avoid lock-in effects.
Another important measure to facilitate efficient development and reinforcement is to register infrastructure and building and construction work in the electronic communications portal (www.ekomportalen.nkom.no).

Address for visitors: Nygård 1, Lillesand, Norway
Postal address: Postbox 93, NO-4791 Lillesand
Tel. no.: (+47) 22 82 46 00
nkom.no