telenor

Table of contents

PHOTO: SØREN SIGFUSSON / NORDEN.ORG

Previous editions:

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 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 February 2024 **Design:** Publicis **Images:** Søren Sigfusson, Gunnar Ridderström/Unsplash, Yaroslav Krechko, Google Maps, ITproX, Telenor, Getty Images, Scanpix **Print:** Involve!

Digital versjon: *https://www.telenor.com/about/our-companies/nordics/digitalsecurity/2023/*

Would you like to get in touch with us? Email us at *desken@telenor.no*

Disclaimer: 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 Norway, as well as by external authors. Please note that there may be minor deviations in language and technical terms due to the translation process.

Everything has to work, all the time

Modern societies require a robust and secure digital foundation: Networks and infrastructure where vulnerability is reduced to a minimum. The premise of the digital foundation in 2024 is simple although demanding: *Everything has to work, all the time.*

The stakes now are higher than ever. The altered security situation affects the choices we make. In recent years, Telenor has adopted a holistic security approach to safeguard and protect ourselves and our customers, and to help fulfil our social responsibilities. A critical outage in our infrastructure or services could have major societal consequences and, in a crisis situation, could even impact national security interests. For that reason, it is imperative that our digital infrastructures are developed, built and operated for a high level of security, robustness and emergency preparedness. In this way, we fulfil our responsibility to the community as well as our customers and company alike.

The changed security environment has an impact on government and industry in all Nordic countries. According to the Norwegian security and intelligence services the threat to Telenor in Norway, our customers and Norwegian businesses are impacted by China on the offensive[1], and Russia prepared for a permanent rupture with the West[2]. We see that critical infrastructure is becoming increasingly vulnerable. NATO is expanding, and the Arctic is becoming more important.

» Closer Nordic cooperation on security, resilience and emergency preparedness could lead to the development of more common solutions within a Nordic and Nordic-allied framework.

The digitalisation of industry and operational technology places increased demands on security. In the war in Ukraine, for example, Russia seeks to systematically break down civilian infrastructure – electricity, water, food, transportation and broadband and mobile services – with physical and logical attacks. Many lessons can be drawn from the telecom industry in Ukraine. Security comes at a cost. Business and government are expected to safeguard critical functions such as oil and gas production, electricity, public sector activities and hospital operations with appropriate industry expertise. It's crucial to establish new industrial partnerships for the development of software and solutions to help secure industrial companies and critical infrastructure. Leveraging critical expertise and capacity across industries will open up opportunities for innovation and value creation in industrial cybersecurity.

Sharing information supports threat understanding, which provides a basis for systematic risk management. For more than ten years the Norwegian Police Security Service (PST)[3] and the Norwegian Intelligence Service (NIS)[4] have shared their threat assessments of current security challenges with the public. As do security services across the Nordic region. In the same spirit, Telenor Norway is sharing its Digital Security Report, which addresses the threats to our business and how we handled them. We also highlight areas that are of key importance for business and society alike, and that need to be addressed. In this report we share this insight with the wider Nordic community for the first time.

We see a need to further strengthen digital resilience in all the Nordic countries. Doing so requires systematic interaction. Other crucial elements are establishing better solutions for collaboration on classified topics and granting selected enterprises access to threat and security information.

Artificial intelligence (AI) is currently being widely debated in relation to security. Will this type of technology strengthen or weaken cybersecurity? Artificial intelligence can be used in both cyber attacks and cyber defence. The unexamined use of AI

1 https://www.etterretningstjenesten.no/publikasjoner/focus/contents/China
2 https://www.etterretningstjenesten.no/publikasjoner/focus/contents/Russia
3 https://pst.no/globalassets/2023/ntv/ntv_2023_eng_web.pdf
4 https://www.etterretningstjenesten.no/publikasjoner/focus

PHOTO: TELENOR

could have significant negative consequences; the sound use of AI therefore requires human engagement and intelligence.

A united Nordic region in NATO will provide opportunities. Closer Nordic cooperation on security, resilience and emergency preparedness could lead to the development of more common solutions within a Nordic and Nordic-allied framework. Coordinated legislation that allows the sharing of expertise, personnel, technical solutions and infrastructure across the Nordic region is necessary. Faster security clearance processes and better use of scarce personnel resources are as well. The bottom line is that the Nordic region can build more security and resilience if resources work better together; having the right policies in place would be a good first step on this journey. Finally, tapping into private companies as part of overall contingency planning ensures the full spectrum of knowledge and capabilities are brought to bear on these issues.

In a more turbulent world, Norwegian and Nordic companies must prepare to face uncertainty: There will be a greater risk of interruptions in deliveries, and shortages of critical components. A Nordic initiative to make better use of technical solutions and infrastructure – such as fibre and datacentres across Nordic countries – would strengthen national security by ensuring more resources closer to every Nordic country. It would also strengthen the resilience of the Nordic region as a whole and stimulate multinational technology suppliers to establish centres of expertise in the Nordic region.

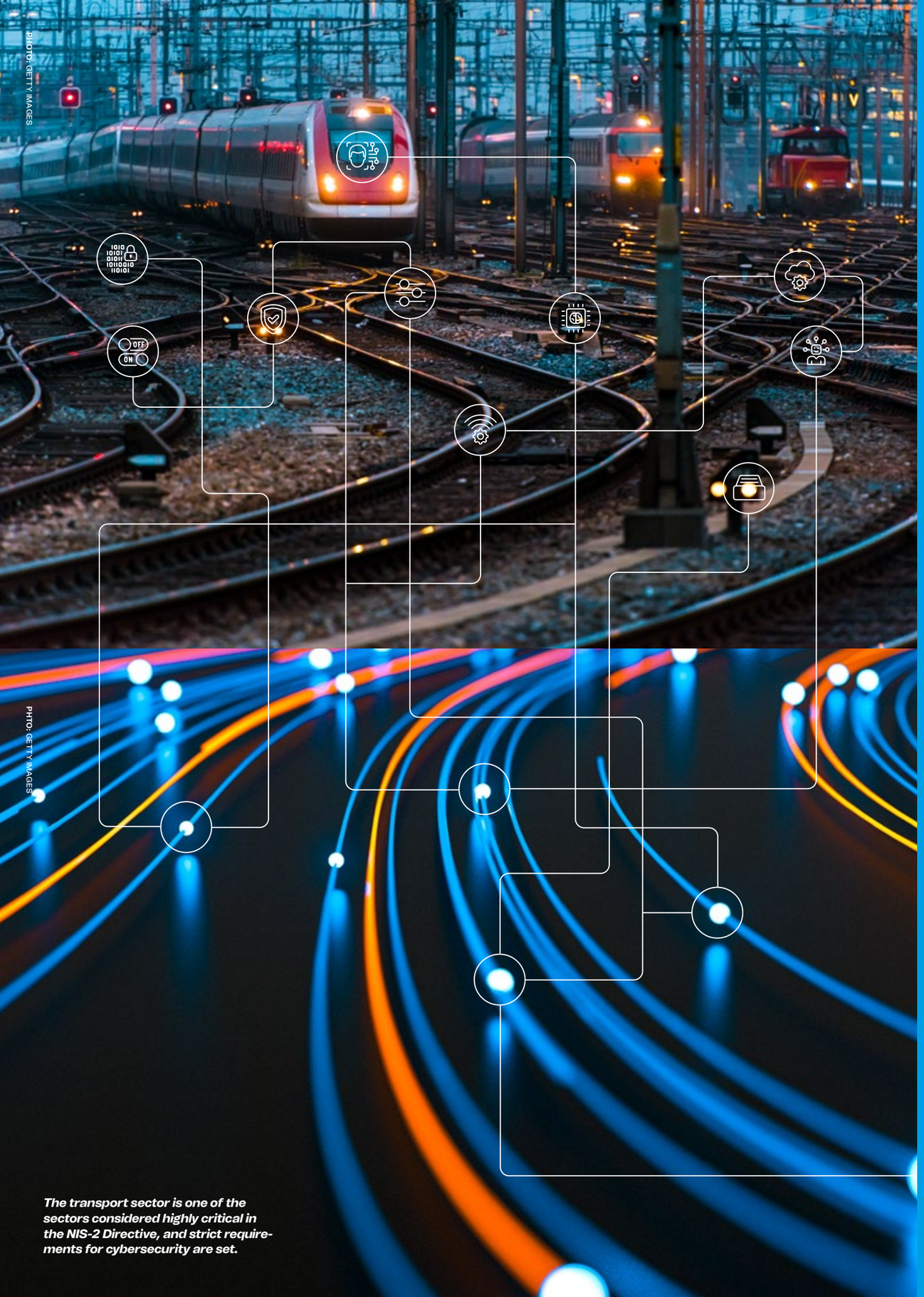
Finally, security is last but not least a leadership responsibility. It starts with recognising risk, and then ensuring that security and risk management are integrated throughout the organisation. Building a security culture requires time and systematic effort. This culture is crucial for how well we will succeed in simplifying, improving and renewing our own operations and supporting the digitalisation of society. Everything is connected: We must all be prepared.

We wish you an interesting and motivating read!

Jørgen C. Arentz Rostrup
Head of Telenor Nordics

Birgitte Engebretsen
CEO Telenor Norway

PHOTO: GETTY IMAGES



PHTO: GETTY IMAGES

The transport sector is one of the sectors considered highly critical in the NIS-2 Directive, and strict requirements for cybersecurity are set.

2

Industrial cybersecurity – innovation and value creation

The digitalisation of operational technology (OT) increases technology dependence and exposes vulnerabilities. As with all other digitalisation, digitalising OT calls for higher security requirements. In this article, the authors highlight the needs for cybersecurity in information technology-operational technology- (IT-OT) integrated systems, and discuss these needs in relation to established frameworks and regulations. They advocate shifting focus from the cost of securing OT to the value potential that investments in OT security bring.

INFORMATION TECHNOLOGY (IT) describes systems that manage information by collecting, processing, storing and transmitting it. Operational technology (OT), on the other hand, encompasses the devices and technology that interact with the physical world: both the physical machines themselves and the systems that control, monitor and interact with them.

OT presents unique security challenges for several reasons. OT has very high requirements for availability and operational continuity. The equipment lifecycles in OT are very long (sometimes decades), so an organisation may need to take outdated equipment into account in its cybersecurity planning. And the equipment may be from an era when OT was isolated or "air-gapped" for security purposes. Built-in security capabilities are often weak or non-existent.

IT and OT have gradually merged over time. In the digital transformation of industry – often referred to as "Industry 4.0" – they are integrated into cyber-physical systems (CPS). These systems have several characteristics that distinguish them from both pure IT and pure OT systems. These are intelligent systems where physical, network-based and database components interact. CPSs constitute core elements in industrial control systems (ICS) used to control processes in industries, e.g., manufacturing, product handling, and production and distribution.

OT cybersecurity – an investment in opportunities

Discussions about OT cybersecurity often emanate from the potential losses one risks by not investing in it. Sometimes previous incidents and the resulting costs are brought up, as well as work hours lost due to downtime, and similar metrics.

Unfortunately, scenarios such as these are why businesses usually consider cybersecurity as a necessary *cost* rather than *an investment and opportunity*. This is also one of the reasons for questions arising around the need to allocate resources to cybersecurity, especially ones not subject to industry-specific market actions or regulatory requirements.

Promoting OT cybersecurity should no longer be based on fear of undesirable events. It is time to focus on the opportunities and benefits of investing in OT cybersecurity. The discussion should be about how doing this can enable innovation, digital transformation, and value creation. OT cybersecurity is about more than just protecting data and systems from malicious acts. It's also about new approaches to running a business, creating value and delivering services in the digital age. Cybersecurity can help organisations:

- **Strengthen reputation, trust and loyalty** amongst customers, partners and stakeholders by ensuring privacy and security.
- **Adopt new technology solutions more quickly, efficiently and safely,** simultaneously enhancing operational efficiency and productivity while enabling flexibility to deal with changing market conditions and customer needs.
- **Promote innovation and creativity** by enabling safe experimentation, collaboration, product development and information sharing.
- **Achieve competitive advantage** and market share by offering differentiated and secure products and services.
- **Comply with regulatory requirements** and industry standards by adopting best practices and frameworks.

Cybersecurity – more than just technology

In addition to technological changes, IT-OT integration leads to organisational and behavioural changes that affect cybersecurity. For example, establishing trust between machines and humans might require new authentication mechanisms and associated training. Moreover, the complexity of IT-OT integration requires not only innovative solutions but also innovative perspectives.

What this means is that organisations cannot simply apply cybersecurity technologies and measures developed for pure IT systems to IT-OT integrated systems. It is also necessary to extend cybersecurity attributes beyond the conventional CIA triangle (confidentiality, integrity and availability) to include attributes like controllability, observability, and operability to reflect the requirements of industrial control systems.

AUTHORS:

Sokratis Katsikas, Centre Director, NORCICS

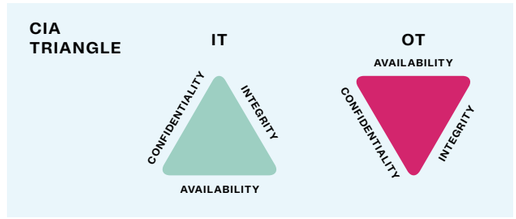
Vasileios Gkioulos, Work Package Leader, NORCICS

Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS) is one of NTNU's centers for research-based innovation.

Read more about NORCICS here: https://www.ntnu.edu/norcics

This article has been editorially adapted for publication in Digital Security 2023.

» For example, establishing trust between machines and humans might require new authentication mechanisms and associated training.



The challenges of managing cybersecurity for IT-OT integrated systems require a holistic, systematic approach to technology, people and processes that addresses cybersecurity at all stages of a product or service's lifecycle. Such an approach is set out by the *NIST Cybersecurity Framework (CSF)*[5]. NIST is the US National Institute of Standards and Technology.

Frameworks and Standards

NIST released its CSF for the first time in 2014 and updated it in April 2018. The next update is expected to be available in early 2024. The CSF is a voluntary framework of standards, guidelines and practices. The framework consists of three main components: *Core*, *Implementation Tiers* and *Profiles*.

The *Core component* provides a collection of desired cybersecurity activities and outcomes organised into five core functions: Identify, Protect, Detect, Respond, and Recover.

1. **The Identify function** aims to identify the resources that need protection
2. **The Protect function** aims to establish the protective measures to be implemented
3. **The Detect function** aims to establish the measures to be used to detect attacks
4. **The Respond function** aims to establish measures that can limit an attack if it occurs
5. **The Recover function** aims to establish measures that enable quick recovery if an attack succeeds

5 https://www.nist.gov/cyberframework

The *Implementation Tiers* provide a framework for how an organisation looks at cybersecurity risk, and evaluates the processes in place to manage that risk.

The *Profiles* are the organisation's unique adaptation of requirements and goals, risk appetite, and resources against the desired outcomes from the Core component.

Beyond frameworks and recommendations, *standards* provide valuable guidance regarding cybersecurity challenges. Several standards address cybersecurity for ICSs wholly or partly, but two stand out as generally accepted and sector-independent: NIST SP 800-82r2 guide and the ISA/IEC 62443 series of standards. (ISA is the International Society of Automation. IEC is the International Electrotechnical Commission.)

These standards establish best practices for security and provide a way to assess the security level. Both employ a holistic approach to the cybersecurity challenge across OT and IT, and »

«High criticality» sectors in NIS-2:

- Energy: Electricity, District heating and cooling, Oil, Gas, Hydrogen
- Transport: Air, Rail, Water, Road
- Banking
- Financial market infrastructures
- Healthcare
- Drinking water
- Waste water
- Digital infrastructure
- ICT service management (B2B)
- Public administration
- Space

«Critical» sectors in NIS-2:

- Postal and courier services
- Waste management
- Manufacture, production and distribution of chemicals
- Production, processing, and distribution of food
- Manufacturing
- Digital providers
- Research

OT cybersecurity is not a one-time investment nor a static state where something is "secure" or not. It is about being *sufficiently* secure.

encompass both safety in processes and cybersecurity. ISA/IEC standards are related to all industry sectors that use ICSs. However, the implementation of the guidelines provided by these standards is neither simple nor straightforward.

Regulation

Another significant factor influencing the implementation of OT cybersecurity solutions is regulatory compliance with, for example, the NIS2 Directive. This European Union (EU) directive extends and modernises the original NIS Directive. Both directives set requirements for security in network and information systems (NIS). In NIS2, new sectors are included, a clear size limit is introduced, and fines and other sanctions are increased. NIS2 has an expanded sector-focused approach, covering more sectors than before and setting a number of focus areas for which all included organisations must implement measures.

A shared responsibility

OT cybersecurity is not a one-time investment nor a static state where something is "secure" or not. It is about being *sufficiently* secure. This is a process that requires continuous monitoring, updating and improvement. It is also a shared responsibility that involves all stakeholders, from top management to employees, customers and partners. OT cybersecurity is a strategic resource that can support businesses in achieving their goals and visions in the digital age.

By investing in cybersecurity, businesses not only protect their assets and reputation but also open up new opportunities and potential for growth and transformation. Instead of viewing OT cybersecurity as an expense, businesses should instead recognise the opportunities for value creation and innovation that it provides. //

Areas of Action Set in NIS2:

a. Security policies and the security of information systems

b. Incident management (prevention, detection, response, recovery)

c. Business continuity through disaster preparedness and crisis management

d. Security in the supply chain, including security-related aspects concerning the relationship between each entity and its direct suppliers or service providers

e. Security in the procurement, development and maintenance of network and information systems, including vulnerability management and disclosure

f. Guidelines and procedures for assessing the effectiveness of cybersecurity risk management measures

g. Basic practices for cybersecurity hygiene and cybersecurity training

h. Guidelines and procedures for the use of cryptography and, when appropriate, encryption

i. Security of human resources, access control policies, and asset management

j. Use of multi-factor authentication or continuous authentication systems; secure voice, video, and text messaging communication; and secure communication systems for emergencies within the entity, when appropriate

PHOTO: GETTY IMAGES

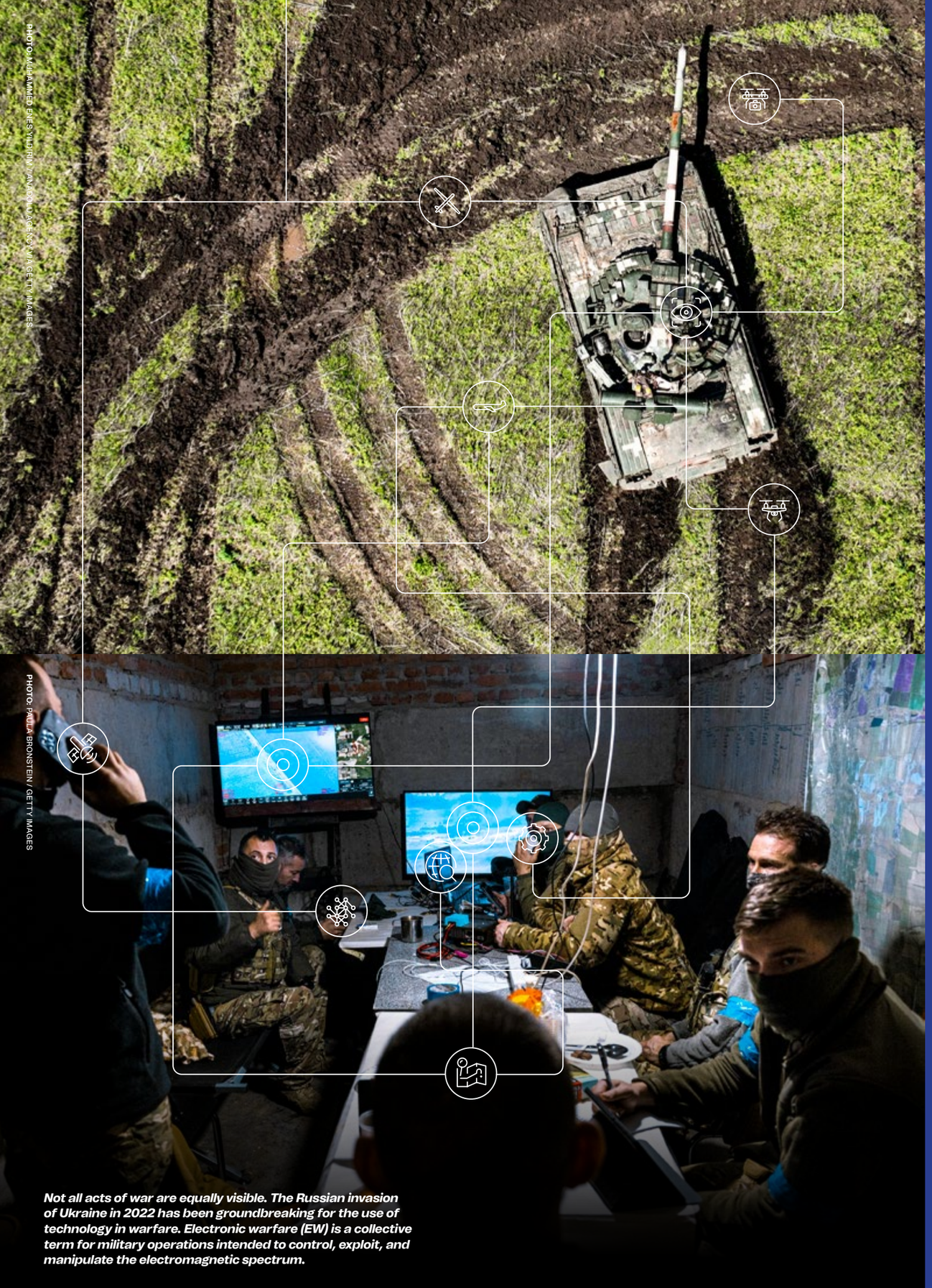


PHOTO: MUHAMMED HAJ SULEIMAN / ANADOLU AGENCY VIA GETTY IMAGES

PHOTO: PAULA BRONSTEIN / GETTY IMAGES

Not all acts of war are equally visible. The Russian invasion of Ukraine in 2022 has been groundbreaking for the use of technology in warfare. Electronic warfare (EW) is a collective term for military operations intended to control, exploit, and manipulate the electromagnetic spectrum.

3

Electronic communication in conflict and war

We have already witnessed multiple years of war in Europe since Russia invaded Ukraine in February 2022. Within this conflict, electronic communication is playing a crucial role in the functioning of both military systems and civil society. It comes as no surprise, then, that electronic communication and communication infrastructure are targets for disruptive and destructive operations, involving cyber, electromagnetic and kinetic attacks.

IN THIS CHAPTER, we will first take a closer look at combat operations in the electromagnetic spectrum. Then, Cathal McDaid, CTO at Enea AdaptiveMobile Security, summarises key experiences from the telecom industry in Ukraine, offering insight and reflection for preparedness work for other countries.

Combat operations in the electromagnetic spectrum

While electronic warfare, which is the manipulation of signals in the electromagnetic spectrum, is shrouded in secrecy, it has still been possible to observe its use, at least partially, during the war in Ukraine. This article examines its offensive aspects, especially jamming (see separate information box for terminology). Some types of electronic warfare (EW) have been clearly observable, like the jamming of GPS signals, while other types are subject to a much higher level of secrecy and can only be understood based on circumstantial evidence.

3G, 4G and 5G mobile communications quite obviously depend on radio signals, but it's less well-known that with each new generation of mobile communication, the frequency at which mobile systems operate increases. The consequence is that communication becomes more dependent on frequencies that are closer to certain types of radar as well as more dependent on precise time synchronisation with accurate time signals from navigation satellites. EW aimed at the higher frequencies used for military tactical communications and frequencies for certain types of radar is near the current frequency bands for telecommunications.

EW can also be directed at the radio segment in mobile phone systems and can directly affect telecommunications. The most recent updates indicate that Russian forces may be developing systems to engage in EW against communication satellites operating in low Earth orbit (LEO). Given the conditions described above, it is therefore appropriate for telecom operators to take a closer look at the overall EW picture in Ukraine.

Satellite navigation systems

The first application of EW, which has been confirmed and documented on numerous occasions, is jamming and sometimes spoofing of signals from satellite navigation systems. The most well-known system is the US-operated Global Positioning System (GPS), but there are two other systems with global coverage: the Russian-operated GLONASS and the EU-operated Galileo.

All three systems are based on signals transmitted by a set of satellites positioned about 20,000 km above the Earth's surface. Since the radio signals from these satellites are sent from such a distance, they are weak when they reach the receiver on the ground, making them relatively easy to jam. A ground-based jammer can cover a significant area, mostly only limited by the curvature of the Earth. The Russian capacity to jam GPS was well known before the invasion of Ukraine in February 2022, with incidents in eastern Ukraine having been observed in 2014 and in the border areas with Norway in 2017.

After the Russian invasion in February 2022, several GPS outages were recorded, likely carried out to support Russian attacks. GPS outages were also registered along large parts of the frontline through eastern and southern Ukraine. There are clear indications that, as the war has progressed, Ukrainian forces have also begun to conduct jamming operations, e.g. aimed at satellite navigation systems. It is likely that they actively jam frequencies in the Russian GLONASS system.

As Ukrainian forces began counterattacks with long-range artillery and missiles against airfields and supply areas, Russian GPS jamming occurred in several areas deep inside Russia. Most likely, this jamming was initiated by Russia to prevent GPS precision guidance of shells and missiles, as well as the steering of Ukrainian unmanned aerial vehicles (UAVs).

Close to the battlefield – tactical communication systems, radars and mobile phones

Coming back to the second application, the jamming of tactical communication systems near areas of ground combat has been observed and referred to in open sources multiple times. Such jamming has been directed at frequency bands used for military radio communication, such as VHF and UHF bands. In the same areas, mobile phone systems are also likely to be subjected to jamming.

In the initial attacks in February and March 2022, this jamming was not so effective, possibly due to the rapid movements and complex battlefield. Later, when the frontline became more static in the east and south of Ukraine from autumn 2022, local jamming against Ukrainian targets became more effective. There is not much information on Ukrainian jamming directed at Russian

» Every day it becomes clearer how well Ukraine has used electronic warfare to degrade enemy radio signals and radars and to disable drones and missiles. Electronic warfare capabilities, including but not limited to cyber, are increasingly relevant.

Josep Borrell, High Representative of the European Union for Foreign Affairs and Security Policy
in *Lessons from the war in Ukraine for the future of EU defence*

forces, but it is clear that Ukrainian forces are employing these techniques. Many of the areas along the frontline in the east and south are likely subjected to extensive jamming. This affects Ukrainian forces' ability to communicate, manoeuvre, and find and combat targets.

Observations of Russian jamming are supported by actual losses on the battlefield. Oryx, the Netherlands-based analysis group that counts losses on the battlefield, has identified 36 damaged or destroyed Russian EW systems. These various jamming systems can work against ground-based and airborne tactical communication systems, mobile phones, satellite navigation systems, high-speed data links and a range of radar frequency bands. Oryx's data contains little information on the loss of Ukrainian EW equipment, having only identified two systems as damaged or destroyed.

Is jamming directed against cruise missiles?

In terms of further applications, let us now explore more indirect and somewhat more uncertain identification of the use of jamming. Despite significant superiority, the Russian Air Force has not been able to establish air dominance over eastern and central parts of Ukraine. Russian forces have therefore relied on carrying out missile attacks against targets inside Ukrainian-controlled territory, using various types of low-flying cruise missiles.

Throughout the Russian campaign, the missiles have exhibited surprisingly low precision and limited capability to penetrate airspace. It's easy to attribute this to effective tactics from Ukrainian air defence units. Another likely factor is the use of EW against the missiles. The Russian cruise missiles use GLONASS to correct their course, as well as radar to adjust altitude and ultimately hit their target. Jamming against these missiles can be directed both against the three frequencies GLONASS operates on, as well as the higher frequencies for target-seeking radars. Since Ukrainian forces cannot know exactly which type of missiles are incoming, it will be necessary to jam a relatively broad spectrum of frequencies. »»

PHOTO: YAROSLAV KRECHKO VIA FACEBOOK

A Russian R-330ZH Zhitel in Donbas.

There are entire segments of the front where [Ukrainian drone operators] can't fly their drones since they are getting jammed by the Russian EW forces.

Samuel Bendett, an analyst and expert in unmanned and robotic military systems at the Center for Naval Analysis

Latest developments indicate Russia possibly developing the capability to jam LEO communication satellites

According to an article published in *The Washington Post* in April 2023, based on one of the classified documents leaked on the Discord chat platform in the so-called "Discord leaks", Russian space forces are believed to have used a ground-based system in an attempt to jam Starlink communication satellites as they passed over Ukraine. Originally, it was thought that this occurred over a 25-day period, but later estimates suggest that the jamming had been going on for a slightly longer period. *The Washington Post* attributes the activity to the use of a large system that operates from permanent installations located far outside Ukraine.

Conventional methods for jamming satellite communication signals involve using ground-based jammers near the ground transmitters/receivers. The impact is limited by the curvature of the Earth, local geographical conditions, and the position and power of the jamming resources employed. What's unique about the Russian system described by *The Washington Post* is that it jams from the ground up, towards the satellites themselves, using large parabolic antennas. These affect the Starlink satellites from two or three locations outside Ukraine.

Starlink communication satellites operate in LEO at altitude bands of 340-360 km (Gen. 1) and 525-535 km (Gen. 2), and move rapidly relative to the Earth's surface. Similar conditions apply to other operational civil communication systems in LEO, such as the Iridium satellite constellation. Military communication satellites also exist alongside these.

The method described by *The Washington Post* is plausible, provided that the parabolic antennas can be synchronised accurately enough to follow satellites at a distance of several hundred kilometres. This would require significant electromagnetic energy, and it would be desirable to have the largest possible parabolic antennas to concentrate the radio signals. Closer examination of the information reported in *The Washington Post* shows that several of the described locations are clearly identifiable and have newly built infrastructure. At some locations, larger movable parabolic antennas and unique communication infrastructure are visible. Other information indicates that a development contract was awarded in 2012 for a system with such capabilities. There is also information about construction projects at some of the locations in recent years, and the system is apparently designated "Tobol".

The parabolic antenna is considerably larger than the typical size employed for high-speed communication with satellites. This holds true even when compared to modern equipment for communication to and from satellites in geostationary orbit, 36,000 km above the Earth's surface. The fact that such large parabolic antennas are equipped with steering mechanisms/devices and motors to track moving satellites (for example, satellites in low or medium Earth orbit) is also unique. Parabolic antennas of this size are normally used towards geostationary satellites, which have a fixed position relative to the Earth's surface. The antennas therefore remain stationary during operation and don't require a large motor for swift repositioning.

When it comes to other types of large movable parabolic antennas, the Soviet and Russian space programmes have employed two distinct categories. Older systems from early in the Soviet space programme feature less precise steering and signal paths, necessitating the use of large parabolic antennas. In addition, the Soviet Union and Russia have run a program for deep space exploration, incorporating very large movable parabolic antennas. These serve the purposes of communication with spacecraft beyond high Earth orbit and radio-telescopic observation of deep space. These have a significantly different design from the parabolic antennas at the locations described above. Nothing suggests that the recently observed parabolic antennas are part of such space programmes. They are also installed in different locations from the ones used in the space programmes.

It has also been reported that the Tobol project included a unit consisting of mobile vehicles equipped with a large parabolic antenna. While pictures of a prototype exist, the information here is uncertain. Furthermore, the existence of a finalised version of such a vehicle remains unclear.

Overall, the information about the Tobol system, its functionality and operational testing is relatively uncertain. There is no available information on whether satellite communication was effectively jammed. However, the method is unique and plausible, and could represent a new category of threat to satellite

Starlink has resisted Russian cyberwar jamming & hacking attempts so far, but they're ramping up their efforts.

Elon Musk on Twitter May 11, 2022

PHOTO: GOOGLE MAPS 2023

communication in LEO. The locations differ from other ground stations used by the Russian space programme, commercial entities and the Russian defence forces, including intelligence and security services. If Tobol actually exists, the use of this system would constitute a new threat. Among other things, this could affect the use of satellite systems as backup communication solutions in the event of a fibre-optic communication failure. That is why we have included it in our assessment in this chapter, despite the limited information available.

What can the telecommunications industry conclude

In wartime situations or highly escalated conflicts, telecom operations will have to be conducted in a signal environment where active electronic warfare (EW) is a significant factor. Radio waves propagate freely through the air, and EW activities from either side can impact operations. EW is likely to occur in specific geographic areas, on specific frequencies, and can change rapidly. Areas near combat zones will likely be heavily affected. Defensive jamming, to counter the threat from air attacks, as well as jamming from airborne and maritime mobile platforms, can be carried out in areas further away from the combat zone.

There are 11 specific frequency ranges for GLONASS, Galileo and GPS. These and nearby frequencies are very likely to be jammed. The 11 frequency ranges are spread between 1176 MHz and 1602 MHz, none of which are very close to the frequency bands used for mobile telephony. However, jamming of these frequencies would affect the availability of satellite-based timing signals, with potentially serious and wide-ranging consequences.

Jamming of the X-band and Ku-band frequencies, used by cruise missile seeker radars, hits right in between the most common and very highest frequency bands for 5G. If broad-spectrum jamming against such missile radars is carried out, depending on the specific conditions, it could potentially affect communication between base stations and terminals (mobile phones and other user devices).

Jamming aimed at ground-based airspace surveillance radars, air defence systems, aircraft and airborne surveillance radars, artillery locating radars and ship radars (for surveillance, navigation and target acquisition) will affect a wide range of frequencies spread over several frequency bands. The use of such jamming will vary with the tactical situation and will change quickly, both in terms of coverage area and frequencies. Jamming here could come from both ground-based systems that are only moved periodically, as well as from airborne and maritime platforms.

The potential build-up of Russia's ground-based capability for jamming communication satellites in LEO creates some uncertainty regarding these satellites' reliability as backup capacity for bridging communication gaps in fibre connections. However, there is currently little and unclear information about this topic, meaning it is premature to draw conclusions about the development, scope, operational area and impact of such a complex system. //

Electronic warfare

Electronic warfare (EW) is a collective term for military operations aimed at controlling, exploiting and manipulating the electromagnetic spectrum, which includes various radio frequencies. Attacks through digital networks are not considered EW and are called cyber warfare or cyber operations, which is distinct from EW. EW can be divided into three types of operations: offensive, supportive and protective. In this chapter, we have focused on offensive operations.

About offensive electronic warfare

Principally, there are three ways to conduct offensive EW operations: jamming, spoofing and decoying. Jamming involves blocking signals, usually by sending more power to the receiver than the original signal. With modern signalling, it is also possible to use techniques that block specific control signals or specific sequences of a signal. For example, blocking the signal that controls the opening of the receiver can, in practice, lead to the same result without using extraordinarily high power.

Spoofing involves imitating a signal and making it appear as if it's legitimate. The most typical form of spoofing is to mimic the call sign of another transmitter. With modern digital signalling technology, it is possible to imitate a variety of signals. Decoying involves sending out stronger signals to get a receiver to lock onto a false transmission. This is typically deployed in the domain of EW focused on diverting radars. The use of a fake base station in a mobile network is, in principle, a form of decoying. Used against a radar, a decoying signal will appear as a real echo to the radar operator, while in reality, it is a transmitter providing a stronger signal than the radar echo from an aircraft or vessel.

PHOTO: AP PHOTO / SERGEI GRITS / NTB

Ukraine: Wartime telecoms

The 2022 invasion of Ukraine by Russia has been ground-breaking in many ways when it comes to technology. One of the least known, but potentially most important aspects, has been the wartime use of telecom networks and in particular, mobile telecom networks. Overlooked before the war - where most analysts (mistakenly) predicted that cyberwarfare would play a large part in the conflict - mobile networks have been shown to have massively impacted the course of the war.

This impact can be shown in three different ways:

One - The effect on morale and the international response. Functioning and secure Ukrainian mobile networks allowed early Ukrainian successes – such as repelled Russian forces and burnt-out Russian tanks in the early days of the invasion – to be shown to the Ukrainian public. A graphic example of this was President Zelensky sending a video from his phone in Kyiv the morning after the invasion, something that would not have been possible without functioning Ukrainian mobile networks. Potentially more important in the long run, these successes could be broadcast to Western public and decision-makers worldwide, accelerating material support from these countries.

Two - The impact on the Russian invasion forces. Ukraine was able to restrict the use of its mobile networks by Russian phones. This meant that when Russian forces ran into communication difficulties with military radio systems, they were forced to use the Ukrainian networks and Ukrainian phones as a backup system. This exposed Russian forces to location tracking, communications interception and other forms of attacks, reportedly leading to the deaths of several high-ranking Russian commanders.

Three - The execution of the war. This war has shown a new usage of mobile networks in the form of crowd-sourcing of intelligence. Civilians now report a wide variety of activity, such as reporting enemy troop movements, drone attacks and battle damage. These use different methods, ranging from simple text messages and messenger apps all the way up to Telegram channels to dedicated mobile apps that report the direction and sound of drones and cruise missiles in order to crowd-source location for physical interception.

AUTHOR:

Cathal McDaid,
CTO i ENEA
AdaptiveMobile

These successes have not happened by chance. At the beginning of the war some analysts struggled to understand as to why Russia permitted mobile networks to continue to operate, given the obvious benefits it gave Ukraine in defending itself. These analysts tended to completely ignore the fact that Ukraine could have a large say in how it defended itself and its infrastructure. Ukrainian mobile operators like Kyivstar outlined how they prepared for the conflict months in advance, by making decisions like:

- Construction of additional Network Control Centres
- Construction of "bunker" base stations in critical buildings
- Relocation of critical equipment away from exposed/vulnerable areas
- Increasing interconnection with the rest of the world
- Performing in-depth security analysis of possible vulnerabilities

All of these actions were performed before the conflict began. The importance of prior preparation cannot be underestimated. For example, on the night after the invasion, less than 24 hours after the war began, all three Ukrainian mobile operators – Vodafone Ukraine, lifecell and Kyivstar – blocked mobile numbers from Russia and Belarus registering on their network. We said earlier that this had a large impact on Russian forces as they could no longer communicate using their own mobile phones (Russian SIM cards were prohibited on Ukrainian networks) and had to use Ukrainian numbers/SIMs, which could be more easily tracked and intercepted. The uniqueness of this move cannot be overestimated – no country in the world has ever disabled an existing roaming relationship to not one but two of its neighbours and (in Ukraine's case) some of its largest markets. This type of action so soon after the invasion, and the fact it was coordinated by all three Ukrainian mobile operators, means it would have been planned beforehand as part of a set of options that the Ukrainian Government could ask the Ukrainian mobile community to implement. This move had a further protective effect in that it could reduce the attack surface over the signalling interconnect channel – an area that Russia exploited in Ukraine in 2014. This was only part of a whole set of actions that the Ukrainian mobile community took. Other actions included allocating additional frequency bands to the mobile operators for greater connectivity, stopping

» As the war continues, we are continuing to learn lessons. One of the more recent learnings in the war has been the importance of energy.

disconnection of accounts in case of no credit and blocking some outbound phone calls to Russia/Belarus, while intercepting and recording others.

There is one other action that the Ukrainian telecom community took after the war began that also had a massive impact on the course of the war, as well as never having been done to the same extent anywhere in the world. On 7 March 2022, the three main Ukrainian mobile operators implemented emergency roaming between each other in parts of the south and east, before extending it to other regions. This allowed a mobile phone from one network to use a different Ukrainian network if required. This move massively increased the resilience and usability of the mobile networks throughout Ukraine, especially in the conflict zones, and was used to ensure communications to places like Mariupol and the Zaporizhzhia nuclear power plant while they were under attack. Again, while the use of emergency roaming had been discussed in other countries, and had been implemented at a small scale in places like the Netherlands and the US, no country had ever implemented it with the scale and success that Ukraine did. One issue with implementing emergency roaming for the mobile operators was not the technology, but the logistics, especially when it comes to payment and planning. Billing of different mobile operators within a country does not normally happen, and there were no estimates on the network load that each operator might have to deal with if people could change the operator they could use. In the end, a decision was made to go ahead and implement emergency roaming due to its benefits, and to deal with any negative consequences later.

While the actions of the Ukrainian mobile operators had a definite impact on the war, Ukraine has not been alone in harnessing the power of mobile networks. From a slow start, Russia has started to adapt. After the war in the Donbas in 2014, two unlicensed mobile operators called Phoenix and Lugacom emerged in the Russian-backed separatist areas of Donetsk and Luhansk respectively, using captured mobile equipment from the incumbent Ukrainian mobile operators. These were set up by the separatist groups in the Donbas in order to control communications in the area. Several weeks after the 2022 invasion of Ukraine, Russia moved rapidly to expand Phoenix and Lugacom into the newly occupied regions of southern and eastern Ukraine. At the same time, an additional two new unlicensed mobile operators emerged in occupied Ukraine – called +7 Telecom and Mir Telecom. As a result, by summer 2022 four Russian-controlled unlicensed mobile operators were active in occupied Ukraine. The importance to Russia of having mobile communications in this region is shown by the fact they invested the resources to make sure not one but four mobile operators were deployed and active in a few months in the middle of a warzone. In comparison, it took occupied Crimea several years to have an equivalent number of unlicensed operators deployed, and this with no war occurring. Given the speed and number of mobile operators deployed, and the fact that they have been deployed to provide coverage in areas sometimes lacking other civilian infrastructure like water or electricity, we can safely say these Russian unlicensed networks clearly have military as well as civilian uses. They would give a second method of communications for Russian forces, and also allow a civilian occupation government to communicate and function. Emulating Ukraine, Russia has decreed that emergency roaming is to be put in place between the unlicensed Russian mobile operators, improving resilience by using the benefits of overlapping mobile operators.

As the war continues, we are continuing to learn lessons. One of the more recent learnings in the war has been the importance of energy. In winter 2022, large-scale Russian drone and missile attacks on Ukrainian energy infrastructure had a knock-on effect on mobile networks. In the worst period, around November/December 2022, about 40 percent of the Ukrainian power grid was affected, making the mobile networks vulnerable. This caused the Ukrainian mobile operators to look to both introduce generators for additional power as well as a crowdsharing appeal to connect to other generators, which eventually led to energy being supplied to 600+ base stations. Over time, with increased air defences, a reduction in drone usage and improved energy security, the Ukrainian mobile networks were able to handle the outages relatively successfully. Another learning has been the use of satellite networks. While the use of Starlink has been well publicised by frontline military units, satellite communications for backhaul use from celltowers has also been used via Starlink. There has also been testing of satellite to mobile communications as well. Not all changes have been positive, however. Due to population outflows, Ukraine has had a reduction of around 12 percent of active SIM cards, with four million outbound roamers. Other impacts are that 4G deployments within Ukraine have slowed down, with little progress on 5G. While the war has accelerated the deployment of security and resilience technologies and practices, the loss of paying subscribers and war damage to infrastructure will impact Ukrainian mobile operators when the war ends. That, however, is a problem for the future.

The impact of telecom networks has had a profound effect on the course of the war in Ukraine, and new cases and uses of mobile networks will continue to emerge. The many hard-won lessons gained from the experiences and actions of the Ukrainian telecom community should be studied and understood by anyone involved in preparing for national emergency or security events. //

PHOTO: GETTY IMAGES

Telephone fraud is a serious social problem that affects an increasing number of Norwegians. There are now so many fraud attempts that many hesitate to answer the phone if it rings from an unknown number. Fraud through the use of Norwegian telephone numbers is also on the rise

PHOTO: GETTY IMAGES

4

How they attack

In the digital realm, the pressure that attackers exert on potential victims is constant. Criminals' motives vary: They may want money, trade secrets or other intellectual property, or perhaps they seek the attention that comes with disrupting a company's operations on a large scale. In this chapter, we take a closer look at attackers' methods and share our own experiences.

THE PREVALENCE of scam attempts today makes people hesitant to answer the phone when they receive a call from an unknown number. In this way, scams affect people who are not even direct targets.

Wherever someone turns in the digital space, there is steady pressure from criminals trying to deceive. They do this by using channels such as SMS, phone calls, social media, direct messages, websites, and competitions, as well as fake online ads that appear on otherwise credible sites. It only takes a moment's inattention – perhaps when hungry, tired, or stressed – to click on a link one would otherwise avoid.

In economically uncertain times, we often see a surge in scam activities. When people are under financial pressure they are more likely to make poorer decisions, such as accepting offers or opportunities they would normally identify as too good to be true.

Those trends hold true in attacks against businesses. Phishing, CEO fraud and extortion attacks are among the most prevalent. In addition, we see distributed denial of service (DDoS) and other attacks that can partly be related to the war in Ukraine.

Hacking of private PBX (private branch exchange) systems is a well-known challenge that unfortunately is still relevant.

Remote access scams are on the rise

One type of scam, which is occurs quite frequently, involves calls that seem to originate from unknown Norwegian phone numbers. In these cases, the caller may impersonate a representative calling from a company like Amazon or some other large, well-known retailer or service provider.

These are criminals using programs designed to gain control of the target's mobile phone: This is known as a remote access scam.

If the person targeted answers the phone, he or she usually hears a pre-recorded message informing them of a product order placed in their name, for example an iPhone. The message will direct them to "press '1' to get in touch with customer service" or something similar. If they actually do so, they will instead be routed to a scammer.

Such phishing attacks usually come in waves: a surge of calls where the perpetrators pretend to represent, for example, Microsoft. Later, we could see a similar surge of calls allegedly from Amazon or from other different well-known companies.

No matter what company name the caller claims to represent, the approach is basically the same: The target receives a call and is presented with a problem. If it's not a "wrongly purchased iPhone" it might be a "virus detected on x, y, or z device" or some other problem.

In each case, the scammer offers to help if the recipient follows the instructions given by the scammer. The scammer's help is dependent on the victim downloading an app onto their mobile device or computer. The scammer often describes this program as a "security app" but, in reality, it's a tool that gives this criminal access to the victim's mobile device or computer.

The app *AnyDesk* has emerged as criminals' preferred tool, but programs such as *TeamViewer* have also been misused. These are legitimate apps available as free downloads via both Apple App Store and Google Play. The problem is that they are also very easy to misuse. All that criminals need do is to convince a target – any owner of a mobile device or computer – to give them access. Time and again victims do so despite warnings in these apps about the risk of scams.

These remote access apps enable others to both see what someone is doing on their screen and *remotely control* that person's Internet-connected device. If a person installs a remote access app and grants access to someone with malicious intentions, it is essentially the same as giving the criminal free scope to operate.

Once remote access has been granted, the possibilities of exploitation are many. Whatever the target sees on their own screen can also be seen by the perpetrator. If the victim logs into their online banking portal, the criminal can easily obtain the same information and access the account as well. Perpetrators can also capture one-time multi-factor authentication (MFA) codes sent via SMS, for example, and use those to hijack the victim's account.

CEO fraud – still a serious threat

For the seventh year in a row, Telenor experts have deemed CEO fraud to be the scam method with the greatest loss potential for our company and subsidiaries.

In a CEO fraud, the criminal pretends to be a leader – usually the Chief Executive or other C-level executive – in a company. When successful, they target employees (often someone with financial responsibility and authority) and make them carry out a transaction that "urgently" needs to be completed.

» Wherever someone turns in the digital space, there is steady pressure from criminals trying to deceive.

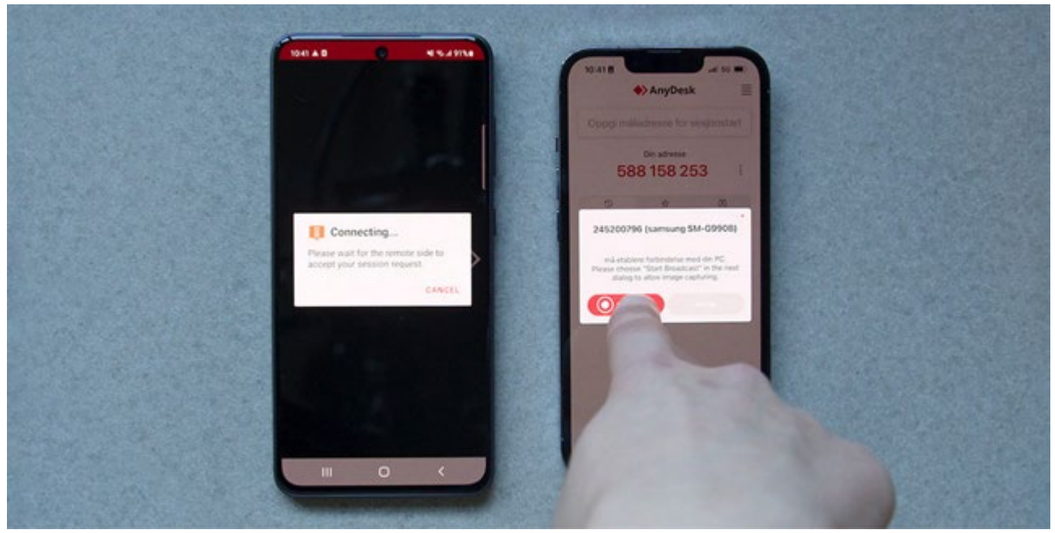


PHOTO: TELENOR

ASK YOU TO DOWNLOAD AN APP: As part of the scam, the criminals often ask you to download an app such as AnyDesk. If you do this, and give the criminals the access they need, they can see everything you do on your mobile – and in the worst case, take full control of it.

Criminals manipulate employees via email or text message and gather information they can use to create a false invoice, or otherwise trick the employee into making a payment. The criminals might instruct the employee to change an account number on an existing invoice to an account belonging to the criminals. Changes in payment information are also associated with the commonly used "business email compromise" (BEC) scam, in which the scammers gain access to an email account at the business or supplier.

Every year, we witness attempts to deceive employees at Telenor. In a recent attack, a sales director at Telenor Linx received an email marked *"URGENT"* signed by the CEO, which seemed to originate from the CEO's email account.

The sales director, busy taking his children to school at the time, quickly replied that he could be reached via phone. Soon after, the requester replied: *"I'm in an important meeting right now, and I cannot make calls. I need you to handle an urgent task for me carefully."*

The sales director replied that he could clear his calendar until 2:30 p.m. To this, the response was: *"Ok good. I want you to buy gift cards for certain customers. Can you do it in 25 minutes? Let me know so I can send you the names on the gift cards and the exact value of each. I will reimburse your money immediately after the meeting."*

Only after the children were dropped off at school did the sales director take a closer look at the emails he had received, and then all the warning lights flashed. The message contained a number of grammatical errors and the tone of voice seemed different than usual. He knew these were typical hallmarks of a scam attempt. He contacted the CEO's assistant and it was confirmed that the CEO had not sent the emails. Crisis averted.

In CEO frauds, criminals take advantage of the trust, respect, and sometimes, the fear that many employees have for senior officers. If the employee believes the CEO or a senior leader is actually behind a request, chances are that the employee will comply. The interaction might start with something as seemingly harmless as buying gift cards, but can escalate to involving much larger amounts once trust and communication are established.

In this case with the sales director, we cannot know for certain what the criminal was ultimately hoping to gain. Digital gift cards, as requested here, are known to be an easily tradable commodity on the Internet. The interaction might have ended with the gift cards. Still, it is quite possible that the first request would have been followed by other requests involving larger amounts.

Telenor's own findings in recent years indicate that organised criminals to a larger extent are using open sources like LinkedIn and Facebook to map out employees and companies in connection with CEO fraud.

They combine this information with other open-source information. Once all the pieces are in place, the criminals can carry out targeted CEO fraud attacks with high precision. The more time scammers spend on information gathering and preparation, the more complex and believable their stories become. Thus, the amounts requested in these scams typically tend to be much higher.

In 2023, Telenor's security department followed up on several inquiries from our own employees who received suspicious inquiries and contact requests via LinkedIn. LinkedIn did not at this time require verification to link a user account to a company. Criminals take advantage of this. For example, they can claim to work at Telenor and use this to their advantage in direct messages to other Telenor employees on the platform. »»

More than 40 Telenor retail stores attacked – how we unmasked the hacker

More than 40 Telenor stores received calls from the same number around the same time. This was a systematic attack, where criminals aimed to gain access to Telenor's data systems through phishing and social manipulation. Here's what happened and how we figured it all out.

It started with an employee at a Telenor store in Oslo receiving a call, at work, from someone he initially thought was a colleague. However, he quickly realised something was wrong and ended the call.

Around the same time, another employee at a different Telenor store in Oslo received a call from a Swedish phone number. The man on the other end of the line claimed to be calling from Telenor's IT support. He said he was calling about problems the staff had been experiencing with a printer in the store.

The caller sounded like a native Norwegian. The employee thought it odd that the person was calling from a Swedish number, yet at the same time, the call seemed genuine. Calls from support were not unusual, and the store had indeed been experiencing a problem with a printer. The employee, who happened to be alone at work when the call came through, deemed this a credible inquiry as he had previously reported to his boss that the printer near one of the cash registers was malfunctioning.

How the scam attempt unfolded: Fake website and AnyDesk

After introducing himself, the caller explained that the printer trouble was due to a network error. To fix the problem, he needed access to the store's systems and asked the employee to open the following website: Billett-Telenor.com.

The website looked identical to a Telenor site; however, it was fake.

The hacker directed the employee to log into the site with his usual username and password for Telenor's systems – which he didn't have, as the Telenor retail store operated its own network independently from Telenor's corporate system.

The hacker subsequently asked the employee to download AnyDesk. The employee was familiar with AnyDesk and knew it was a tool that allows remote control of one PC from another. But since the employee believed the caller was from Telenor, he thought it safe to allow access.

PHOTO: IT PRO X

Within a few minutes the Telenor representative started to grow suspicious.

First, the employee noticed the browser warning that the URL was insecure. Then, he discovered that someone had created a new remote desktop on the PC, hidden behind the browser. He started to wonder if the man from Telenor support was doing other than what he said he was doing. When the hacker asked him to leave AnyDesk running overnight, his suspicions were confirmed.

The employee realised he had been tricked. The store was under attack.

The employee later said his first thought was "Oh no! What have I done?!" He knew that businesses are sometimes hacked but couldn't imagine perpetrators being so professional.

Thinking quickly, he immediately uninstalled the application, deleted the file and turned off the PC. He called his operations manager and told him what had happened.

Aware of the attack before the phone rang

What the employee didn't know was that while he was talking to the scammer on the phone, Telenor had already actively been tracing the attacks against the Telenor stores. A dealer in Bergen had previously reported a phishing attempt where the scammers also pretended to be from Telenor's IT support.

"When we received the first tip, we immediately started an investigation to determine the extent of the matter," says Thorbjørn Busch, senior security advisor at Telenor.

The Swedish phone number turned out to be a real number connected to a Skype account.

Busch believes the use of a Swedish number may indicate that criminals are trying to find new methods to breach security. In 2022, Telenor introduced a

Thorbjørn Busch

PHOTO: TELENOR

block that prevents misuse of Norwegian landline numbers through "spoofing."

Many companies have connections to Sweden, so a Swedish number in itself does not invite distrust. But the call coming from Sweden meant that Telenor would need to pursue the criminals abroad, making it more challenging to investigate the attack.

After an extensive search in traffic data on the Swedish number, the security team quickly saw which other Telenor stores had already been subjected to the phishing attack. After talking to some of the dealers, the team suspected that the perpetrators were trying to gain access to Telenor's other data systems via the Telenor stores – something that, fortunately, is not possible, Busch explains.

In this case, their first goal was likely to collect usernames and passwords via the fake website. When that did not go well, Plan B was to gain access to company information via AnyDesk.

The goal may have been to gain control over mobile numbers

It is still uncertain what the ultimate goal of the attack was, but there is no doubt that criminals can exploit such access for various purposes, with financial gain usually as the main goal. The criminals might have been hoping to achieve a SIM-swap. A SIM-swap can be used to gain access to the victim's accounts – for example, email or crypto wallets – by tricking a phone carrier into sending reset passwords or two-step MFA verification codes to the scammer instead of the actual account holder.

"This is not just a threat to individuals, but also to businesses. Full access to employees' phone calls and texts can be utilised to access business intelligence, commit CEO fraud, or other types of attacks on the company," says Busch. One possible theory is that this particular perpetrator wanted access to customer lists, with the hope of gaining control over mobile numbers on those lists.

Transparency is crucial to uncover fraud

At the second Oslo location, before the employee and his manager could even report the incident to Telenor, Telenor security contacted them. They were relieved to know that the problem was already in the security team's hands. The case was handed over to the police, and although reports do not always lead to an arrest, they do provide the police with important information that may prove useful in other situations.

To be able to investigate such cases, Telenor is dependent on employees and managers reporting situations like these. When we ourselves manage to conduct a thorough investigation, chances that police eventually will make an arrest increase.

As to how the scammers could have known that the printer at the store was not working, unfortunately, that is a low-risk gamble no matter where they had called, says Busch, because printers are so prone to issues.

Spoofing – countermeasures and adaptive criminals
Telephone scams have become a serious social problem that unfortunately affects more and more people. Scammers who pretend to be bank representatives or police officers and take advantage of the trust we have in people in these professions. Their only purpose is to con people out of large amounts of money.

In recent years, we have seen an increase in cases where criminals have misused Norwegian phone numbers in scam attempts. What appears to be a call from a Norwegian phone number can actually be organised criminals operating from abroad. With simple measures, they are able to hide behind Norwegian landline numbers. Spoofing means that the original foreign phone number is replaced with a self-chosen Norwegian number.

After Telenor in 2021 introduced measures against spoofing of *mobile* numbers, we saw an increase in spoofing of Norwegian *landline* numbers. Landline numbers start with 2, 3, 5, 6, or 7 – and indicate a location, such as 21 80 21 80 for Oslo municipality or 75 55 50 00 for Bodø municipality. These are well-known number series with a high degree of credibility.

In addition to the calls that originate from abroad there has been an increase in scam calls conducted by Norwegian criminals over the past few years who come across as convincing with their polite and accommodating manners. The chances that someone will answer a call increase significantly if the number displayed on the screen is a Norwegian number, as opposed to a foreign or hidden one. Similarly, if the number belongs to a well-known company or public institution, people are even more likely to answer the call, and also more inclined to follow instructions.

In November 2022, several Norwegian telecom operators including Telenor joined forces and blocked criminals' ability to spoof Norwegian landline numbers. The initiative was the result of collaboration in the non-profit association *ITAKT*, which brings together Norwegian Internet and telecom operators to combat fraud and misuse of services and infrastructure. The blocking was implemented in line with recommendations from the National Communications Authority (NKOM) and guidelines set in Norwegian regulations for electronic communications and numbering.

This measure prevents spoofing of Norwegian landline numbers from abroad. If a call to a Norwegian number originates from abroad but displays a Norwegian landline number as the sender, it will be blocked and not reach Norwegian consumers.

What is spoofing?

Spoofing is a scam technique with false sender or origin information. The most common channels where spoofing occurs are email, text messages or phone calls where criminals forge a sender's identity to carry out scam attempts. The technique is often used as part of a broader social manipulation attack, but spoofing of the source address for IP traffic is also used in some types of denial-of-service (DoS) attacks.

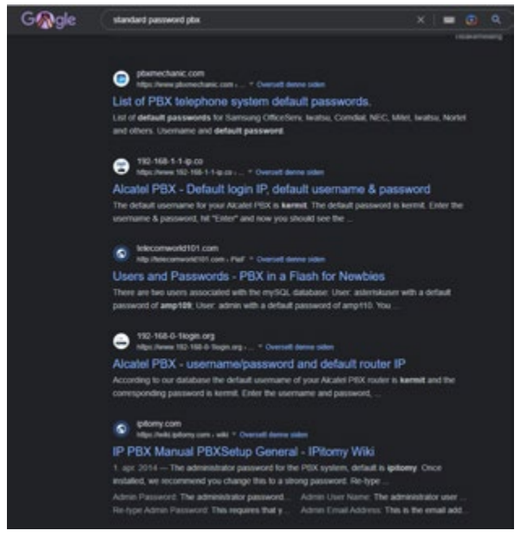
Even though landline numbers are less used by private individuals, they are still often used by businesses and public institutions such as the Norwegian Labour and Welfare Administration (NAV), the Tax Administration and the police. These agencies regularly experience their names and numbers being misused in scams. The block provides better protection against misuse for Norwegian businesses and public institutions..

Hacking of PBX systems – a continuous challenge
Telenor observes that business PBX systems are still subject to breaches. By exploiting weaknesses in the functions of the PBX, criminals can attempt scams. They can also use a PBX breach as a starting point for further cyberattacks, such as ransomware attacks.

PBX systems are delivered with standard usernames and passwords and are connected to the Internet. If the username and password are not changed and the PBX is not secured at installation, the business exposes itself to significant risk. This can be compared to leaving one's house with the door unlocked. Changing standard passwords and settings is fundamental security hygiene, as lists of standard usernames and passwords are available on the Internet.

If criminals gain control of a PBX system, they can start searching for open international premium rate numbers (IPRN). These types of numbers are also called "international revenue share numbers." Telecommunications carriers enter into agreements with other carriers for services like international calling. As such, the more minutes of calls to these IPRN numbers the criminals can generate from the PBX, the more money they can accumulate.

» Scammers who pretend to be bank representatives or police officers take advantage of the trust we have in people in these professions.



An overview of standard usernames and passwords can be found online.

Telenor has implemented measures to shut down access to IPRN numbers worldwide. Monitoring solutions have been used to identify this type of unwanted traffic in our network. The criminals typically use a script – referred to as a *dialer* – to automate searches for open premium rate numbers. They often have to make more than 1000 calls to various countries and numbers before they find open numbers. Telenor can often detect these attempts while in progress and start the process of shutting down this traffic before the scammers succeed. In this way we prevent further misuse. Our experience shows that by reporting the fraud to the police, we are able to stop payments related to such fraud in over 95% of cases.

This is why reporting fraud to the police is so important, even though Telenor can limit the financial damage by stopping further traffic. A report will also give the police a more comprehensive overview of this form of crime.

Premium rate numbers and *wangiri* fraud
Premium rate numbers are also used in so-called *wangiri* fraud. (*Wangiri* is Japanese for "one and cut.") Scammers make money from *wangiri* calls by calling a number, letting it ring once, then ending the call. The victim sees that he or she has missed a call, calls the number back, and is put on a very long and expensive hold. By blocking calls to and from premium rate numbers used in scams, Telenor also prevents *wangiri* attacks against our customers.

The majority of premium rate numbers come from various national number series that are not generally used in the country or they could be technical series earmarked for specific purposes.

If, for example, you receive a call from the British Atlantic island of Ascension, and you choose to return the call, it's unlikely that your call will actually be answered in Ascension. It's much more likely that your call will be forwarded to a premium rate provider. Once the call is connected, you will hear an automated voice message (IVR) designed to keep you on the line as long as possible. "Please hold the line – your call is important to us."

Unfortunately, there are also a few local operators willing to pay commissions to premium rate providers for traffic to numbers in their networks. Here, it can be anything from individual numbers to entire series. Telenor blocks all such numbers as soon as they are identified.

Several companies offer services that, in practice, facilitate scamming. They provide necessary tools and services such as IVR servers, search tools and test numbers. They also supply numbers to criminals either directly or via other companies. Telepremium is an example of such a provider (https://telepremium.net/how-it-works/).

Some of these companies also offer a downloadable phone app to check out which numbers are currently available. Contact with these companies is often only possible via Skype. They seldom operate with a physical address or company name.

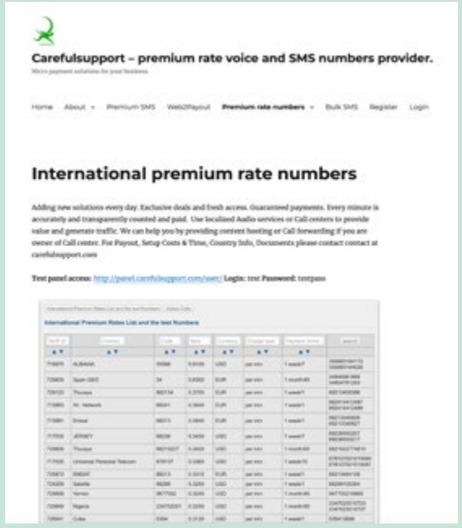
Wangiri fraud and hacking of PBX systems are unfortunately just two examples of how scammers make money on premium rate numbers. There are others; any method that tricks the victim into calling the number and keeping them on the line for some time generates revenue for the scammers. Unfortunately, guidance and suggestions for different methods are also readily available online.

One of Telenor's priorities is ensuring that traffic to and from such premium rate series is blocked and remains blocked. This is important.

Hacktivists carry out targeted and direct DDoS attacks
Over the past year, the number of DDoS attacks recorded through Telenor's systems has remained steady, with an average of around nine registered attacks per day. Most of the attacks target individuals and are relatively short-lived.

The majority of these attacks involve sending a large volume of data traffic to cripple the Internet connection of the target. Much of this traffic is generated by exploiting randomly misconfigured servers on the Internet to reflect and amplify traffic hitting the target. Since the traffic used in the attack originates from a misconfigured server, the attacker's actual IP address is effectively hidden.

Search for premium rate numbers

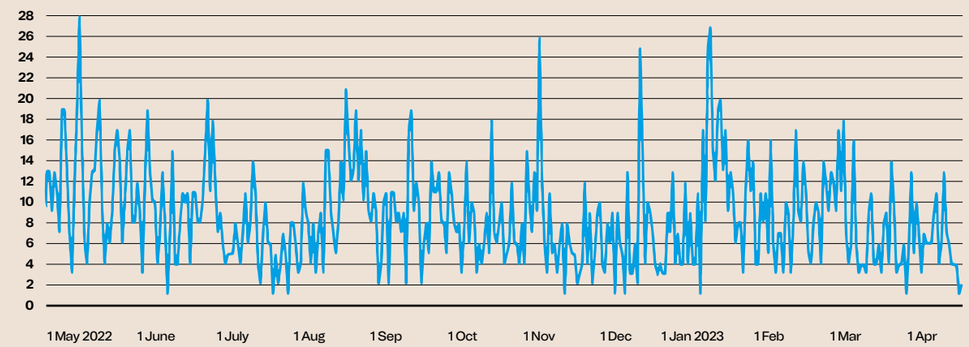


Carefulsupport.com; An example of a company that offers a dedicated test panel.

Excerpt from instructions for installation and use of mobile app from Carefulsupport.com

Attacks per day

DDoS attacks per day over the last year (April 2022 – April 2023)



Telenor and other major Internet service providers (ISPs) have systems that can effectively detect and stop these types of attacks. The systems monitor traffic on Telenor's routers that border other ISPs. This traffic comes from legitimate services but in far greater quantities than what is normal. Examples of services that are often misused include NTP (Network Time Protocol), DNS (Domain Name System), and LDAP (Lightweight Directory Access Protocol).

Following Russia's invasion of Ukraine, many hacktivist groups have emerged, both on the Russian and Ukrainian sides. On the Russian side, KillNet and NoName057 have been particularly active. These groups have also been mentioned in Norwegian media in connection with DDoS attacks. Over the past year, entities such as the Norwegian Labor Inspectorate, BankID, Altinn, NRK, Schibsted, the Norwegian Labour and Welfare Administration (NAV), and the Norwegian National Security Authority (NSM) have been targeted.

The groups constantly change their targets and countries of attack, depending on what is reported by the media. For instance, Noname057 attacked Norwegian targets on March 2, 2023, following the Norwegian government's announcement of a multi-billion kroner financial support package to Ukraine.

Both Killnet and Noname057 coordinate their actions and discuss potential targets for attacks in chat groups on the messaging service Telegram. The latter uses a DDoS tool written in Python called DDosia, which is available for download through links shared in Telegram groups. Members register via a Telegram bot and are assigned a unique ID which they submit into the tool. The tool is installed on members' own machines, on hacked servers, or on rented virtual machines in the cloud. Those who contribute the most to the attacks can gain fame and, in some cases, small amounts of cryptocurrency transferred to their account as a reward for their effort.

In most cases, websites are attacked directly, with fully connected TCP connections. This means that the connections are encrypted, making it difficult to discern from network traffic what is happening and what the attack traffic consists of. Before the attacks start, hacktivist groups thoroughly check their targets and find features on the websites of each target that typically burden the web server and underlying systems as much as possible. This is often combined with sessions that never disconnect, known as Slowloris attacks. When the attack targets the application layer, the attacked server can become overloaded without the network connection being filled with traffic.

The attack traffic consists of seemingly normal connections from regular users. Therefore, it is difficult to detect when a company is under attack using standard traffic analysis. These types of attacks are often only discovered when web servers under attack do not respond at all or respond very slowly. Sometimes, an increase in traffic is not even visible by analysing traffic graphs against the web server, but the attack can be recognised by looking at the number of queries or the resources being requested.

Since it is difficult to distinguish attack traffic from useful traffic at the network layer, this type of attack is often stopped using geographic IP filters. If a Norwegian website is under attack, for example, all incoming connections from outside the Nordic countries can be blocked. This type of blocking is obviously less suitable if the users of the website are geographically very dispersed.

To block DDoS attacks of this type, it is best to have access to the actual queries made against the web server. After analysing these, unwanted queries can be blocked directly on the web server, or preferably via a system before the server, like a proxy or a WAF (web application firewall).

Through logs and statistics, one can identify which resources on the server are being misused during the attack and block these. Systems that receive traffic from regular users should also be configured to prevent Slowloris attacks. This can be done, for example, by limiting the number of open network connections per client and how long they can be kept open, etc.

It is important to have an agreement in place with your ISP before an actual attack occurs to be able to stop DDoS attacks. Also, ensure that the web server's architecture has been thoroughly reviewed and that it is easy to access logs and block requests used in attacks.

Phishing – techniques and measures

For years, phishing emails have been one of the most commonly used methods for gaining illegal access inside an organisation. Having access to usernames and passwords of one or more employees in a company enables a hacker to misuse several services, among these, cloud-based services used by the company. According to the organisation Anti Phishing Work Group (APWG), 2022 was a record year for phishing, with more than 4.7 million attack campaigns worldwide. Since 2019, the number of such attacks has increased by over 150% per year.

Many companies train their employees to recognise phishing attempts and not click on suspicious links in emails. However, distinguishing genuine links from phishing proves difficult. Several companies use external providers for many of their internal services. This means that employees often must click on links to sites outside the organisation's internal domains, making it harder for employees to differentiate between legitimate and illegitimate links.

It is often difficult even for cybersecurity experts to determine what is a legitimate email or a scam. If a phishing test is conducted against a larger company, there will always be at least one

employee who is tricked into giving away sensitive information such as usernames and passwords. Thus, attackers will achieve what they wanted.

To avoid attacks, several organisations in recent years have implemented various forms of multi-factor authentication (MFA). In addition to a regular password, users must enter a one-time code to log in. Attackers are increasingly circumventing this extra layer of security by also asking for the one-time code. The code can be manually entered on the mimicked service, or a proxy can be set up, enabling attackers to log in. In this way, unauthorised individuals can gain access to the victim's session key, thereby posing as the legitimate account owner.

An example of a commercially available service (PaaS, phishing as a service) that offers this functionality is "Greatness," as reported by Cisco Talos in May 2023. Greatness provides a complete phishing package with ready-made emails, phishing pages, proxy functionality and a control panel ready for use against services like Microsoft 365.

Authentication mechanisms resistant to phishing are required to secure against advanced attacks powered by malicious services like this.

Physical security keys, such as YubiKeys, are an example of an authentication method not vulnerable to phishing. A physical key is linked to the user's account and communicates via USB or Bluetooth with the device being used to log in. The key must be physically stolen to be used by unauthorised individuals for logging in.

Google introduced this type of security for its employees in 2017 and has not experienced successful phishing attacks since then. However, there is a significant barrier to adopting security keys. They must be distributed to users and registered, and they are also easier to lose, which would lock the user out until they obtain a new key.

A new technology offers security nearly as good as physical security keys, but without their drawbacks. This technology is known as passkeys and is based on the same standard as physical security keys. One such product is "WebAuthn," developed by the Fast Identity Online (FIDO) security alliance.

Microsoft, Apple and Google now offer passkeys for logging in. Passkeys from these providers can also be used to authenticate the user further with other service providers.

A passkey consists of a private and a public key generated locally by the operating system of the device the user employs. The public key is shared with the service the user logs into. At login, the private key is unlocked locally on the machine; for example, by the user authenticating with facial recognition, fingerprint, or a PIN code. (Biometric information is not shared with the service the user is logging into.)

If adopting a new device, a new key can be generated on the new device by authenticating via an existing device, such as a mobile phone. The mobile phone will contact the new device via Bluetooth or NFC (near field communication) to verify that the user has physical control over the new device. Providers can also choose to synchronise passkeys between devices that the user is logged in on, as Apple does, for example, via Keychain.

Passkeys make phishing attacks impossible to execute. The address of the website the user is attempting to log into is exchanged encrypted with the service provider as part of the login process. In a phishing attempt, this address would be incorrect, and the login would be rejected. Unlike passwords, passkeys are also impossible to guess and consist of a long string of random data, in contrast to classics like "Password123!"

One of the biggest challenges with the solution is authentication if the user cannot log in, such as when they have lost their mobile phone. In such cases, the user must authenticate through an alternative method, such as another logged-in device, one-time codes printed on paper, a physical security key, pre-determined contacts who can confirm the user's identity, an SMS message, or by contacting customer service. These backup solutions must be designed to minimise the risk of users being permanently locked out, while ensuring that unauthorised individuals do not gain access to accounts by posing as the owner.

Going forward, passkeys will become more common for logins. Perhaps the dream of a password-free life without phishing attacks or password reuse will eventually become a reality. //

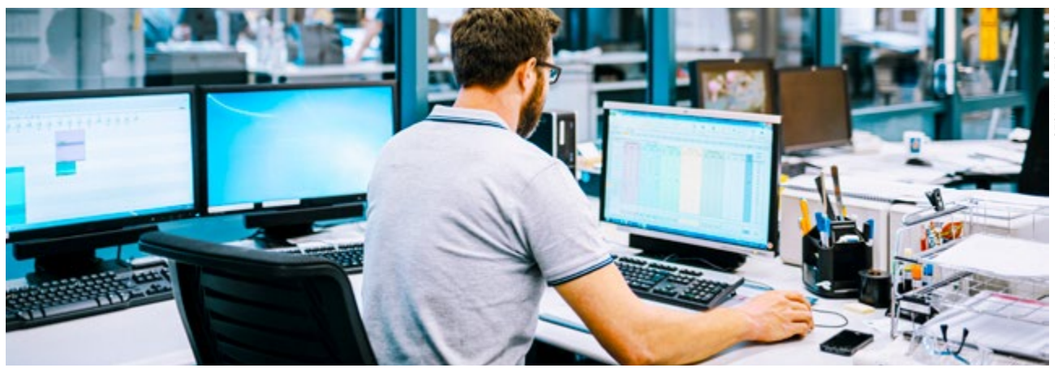


PHOTO: GETTY IMAGES

Perhaps the dream of a password-free life without phishing attacks or password reuse will eventually become a reality.

KraftCERT: from the power sector's perspective

KraftCERT is a sector-specific response environment for the power sector working to prevent, detect and manage incidents in this sector.

Actors will continuously work to develop capabilities for destructive/disruptive attacks. The leak by the Russian company NTC Vulkan, which is a supplier to Russian authorities, clearly shows that Russian actors maintain a toolkit for cyberattacks. This toolkit can be used by threat actors, primarily state or mission-driven, for a fee. The toolkits also include tools for disruptive/destructive attacks.

The tools that NTC Vulkan has developed for attack purposes are well-planned. Several of them are modular, and some have also been demonstrated as functional. There can be several reasons why a threat actor might want to demonstrate a capability or tool, either to showcase tools to potential customers or to support state actors' claims about capabilities. However, even though certain capabilities are demonstrated, all actors, whether state or commercial, will not want to show their full capability. Instead, they want everyone to know that this is not their full capability.

Information from NTC Vulkan and the code for attack tools like PIPEDREAM are examples of leaks that are highly undesirable for threat actors, as their true capabilities are revealed to a great extent. Threat actors do not want others to have time to develop countermeasures. Conversely, all potential targets of attacks desire access to such information to prepare countermeasures.

The latest leaks demonstrate that threat actors are largely underestimated and are far more mature and professional in malware development than previous analyses have shown.

Long-term strategic planning of attacks against OT

Attacking control systems is complex and requires more planning than attacks on conventional IT systems. However, attacks like Stuxnet and Trisis have shown that it is entirely possible. Even though the planning of such attacks takes time, the rate of change in OT is not high enough to necessarily pose a significant obstacle for threat actors.

In connection with Russia's attack on Ukraine in 2022, malware named "Industroyer2" was used. There is little doubt that the attacker had a significant amount of information about the target before the attack took place. The fact that planning takes time and that it must be custom-made for the target means that OT-targeted attacks are costly.

Other factors that make attacks costly are targets that are well-protected, such as the ones protecting high value systems, or those with strict regulatory requirements. The targets that are more difficult to access will be most interesting for advanced actors who have high competence, ample time and are willing to pay more for access and zero-day vulnerabilities. (An undiscovered weakness in an app or operating system is called a zero-day vulnerability; no security patch exists for it because the software creator is unaware of it and has therefore had zero days to mitigate it.)

In such cases, threat actors will avoid exploring the open market for access, but will instead contact suppliers they trust. An access traded in a private forum will not appear on lists of known information leaks and will therefore remain hidden from the target.

To carry out successful attacks on control systems, detailed information about the systems is needed, including location. The owners of this type of information often underestimate how valuable it is, and in any case, information that is not documented as particularly sensitive may be poorly protected. It's not just the owners who are targeted; it may be their suppliers as well. This was evident in incidents at Sargent & Lundy, which was storing documentation on 900 power stations it constructed for customers when it was hacked in late 2022, and Black & McDonald, a Canadian government contractor which was presumably hacked for its military, power and transport documentation.

HelseCERT: From the health sector's perspective

HelseCERT is the national centre for cybersecurity in the health and care sector. The centre aims to increase the health sector's ability to detect, prevent and handle serious cyberattacks.

Attacks against the health sector
The security environment has changed significantly over the past few years. We see an increased intelligence threat, a sharp increase in activity from hacktivists and an ever-growing distance from Russia.

What has changed less is how threat actors attack. We have seen for a long time that known vulnerabilities, weak passwords and lack of multi-factor authentication are actively used to attack organisations. Attackers quickly start looking for vulnerable systems after information about vulnerabilities becomes publicly known. We continuously see attempts to guess usernames and passwords, and passwords that have gone astray are used to carry out attacks. Here we illustrate this with three different data breaches that occurred in the health sector in 2023.

Data breach 1 – vulnerable server online
A system with a vulnerable server was compromised by at least two different threat actors, both associated with ransomware attacks. The system was exposed on the Internet and had a publicly known vulnerability. The first attacker was stopped by antivirus software and gave up. The second was not stopped and managed to gain administrator access, moving on to several servers, including domain controllers, file servers, database servers and more. The vulnerability was exploited shortly after it became publicly known. The attack was discovered after about three weeks. The organisation's IT systems were taken offline for about two days when the attack was detected, and much time and resources were spent on analysis and cleanup afterward.

Data breach 2 – unauthorised access to VPN solution
A weak password on a VPN solution allowed the attacker to log into a lab environment by guessing usernames and passwords. The attacker connected to a VPN tunnel for about five minutes. Through this tunnel, they could access several systems further inside the organisation. Analysis of log data does not suggest that the attacker did more than confirm access. It is assumed that the attacker planned to return later.

Data breach 3 – password guessing and a vulnerable server
A ransomware group is assumed to be behind this data breach. The attacker started with brute force activity (password guessing) against a server. They used about 400 generic usernames and various passwords to guess the correct ones. They made between 50-500 login attempts each day over several weeks before hitting a valid username and password combination and logging into the system. After logging in, they exploited a known vulnerability, for which a patch had not been installed, to install a program that allowed them to remotely control the server. The attack was discovered by a third party who noticed suspicious traffic from the compromised server. Quick incident response stopped the attack with no major consequences.

» Attackers make between 50-500 login attempts each day over several weeks before hitting a valid username and password combination and logging into the system.

PHOTO: GETTY IMAGES

PHOTO: GETTY IMAGES

PHOTO: GETTY IMAGES

On the one hand, malicious participants can use AI and machine learning to identify vulnerabilities in businesses they wish to attack. On the other hand, businesses can use AI to identify potential threats and prevent cyberattacks.

5

Will artificial intelligence strengthen or weaken cybersecurity?

In this article, the authors examine how artificial intelligence (AI) can be used in both cyberattacks and for cybersecurity defence. They emphasise that human considerations will be critical for the responsible and effective use of AI, while also pointing out that even the well-intentioned use of AI can have negative consequences for society.

The age of connected devices

5G offers a wide range of connectivity options and supports various devices – from data-intensive smartphones to basic sensors and high-precision devices requiring ultra-reliability and low-latency connections. With the introduction of 5G, we are witnessing a massive increase in the number of connected devices. According to Statista, "the global number of Internet of Things (IoT) devices is expected to almost double from 15.1 billion in 2020 to more than 29 billion IoT devices in 2030." These devices will provide useful and innovative applications and services that enrich people's lives but also bring new cybersecurity threats.

The cybersecurity threat landscape has changed dramatically due to the vast and rapidly growing attack surface with billions of connected devices and the huge amount of data they generate. Traditional cybersecurity mechanisms and filtering of incoming data for potential threats at the network perimeter are no longer sufficient. This requires new cybersecurity measures, and the use of AI is a natural first choice. Unfortunately, AI is not just reserved for actors with good intentions; malicious actors and hostile nations have already made use of AI to conduct multiple destructive cyberattacks while bypassing traditional cybersecurity defences. Let's first look at how AI can be used in cyberattacks, and then explore how it can be leveraged for cybersecurity defence.

AI in the wrong hands – use of AI in cyberattacks

Identifying vulnerabilities in the victim's systems

Malicious actors can gather vast amounts of data from cybersecurity logs, digital media and other relevant information sources, and then use artificial intelligence/machine learning (AI/ML) to identify vulnerabilities in the organisations they intend to attack. Attackers can perform automated external scanning of a wide range of arbitrary networks to identify weaknesses in network structures and configurations.

Avoiding detection

Attackers can use AI/ML to ensure that their scanning is below the "radar level" and avoids creating anomalies that can be detected by the victim's security system. Malware can be developed to dynamically change behaviour and thus avoid detection by security

AUTHORS:

Thanh van Do, Telenor/Oslo Metropolitan University

Bruno Dzogovic, Telenor/Oslo Metropolitan University

This article has been editorially adapted for publication in Digital Security 2023.

systems, using Generative Adversarial Networks (GANs) or reinforcement learning.

GANs are a form of generative modelling consisting of a pair of neural learning networks; one generator network and one discriminator network. The generator network learns to produce increasingly better results by repeatedly attempting to trick the discriminator network into believing that the generated results are real or, in the case of malware generation, harmless.

Scam letters and spear phishing

Phishing attacks aim to deceive individuals into revealing sensitive information or performing harmful actions using fraudulent techniques. AI can be exploited by threat actors to create highly convincing and personalised scam letters. Using natural language processing (NLP) and ML algorithms, AI can help generate messages that are very good imitations of genuine communication. This makes it extremely difficult for people to distinguish between real and fake messages.

Deepfake attacks

Deepfakes, a combination of "deep learning" and "fake", are data that have been fabricated and digitally manipulated to replace one person's presence, in text, audio, image or video, with that of another in a convincing way. Combining deepfake videos with a Generative Pre-trained Transformer (GPT), e.g. a large language model (LLM) like ChatGPT, can create "virtual people" in just a few clicks.

Deepfake attacks can generate compromising or misleading content, impersonate well-known individuals or spread disinformation, which can lead to reputational damage, financial loss or social unrest.

Attacks against machine learning systems

Adversarial machine learning attacks aim to deceive or confuse a machine learning system, resulting in wrongful predictions and decisions. Such attacks are generally divided into two main categories: misclassification of input data or data poisoning, which involves the injection of incorrect data. Misclassification of input data is the more common variant, where attackers hide malicious content in the filters of a machine learning algorithm, with the goal of causing misclassi-

» Deepfake attacks can generate compromising or misleading content, impersonate well-known individuals or spread disinformation.

fication of a specific dataset. Data poisoning involves altering the machine learning process by introducing incorrect data into a dataset, making the outputs less accurate or wrong.

AI in cybersecurity

Anomaly detection

A promising current application of AI and ML methods in cybersecurity is the detection of behavioural patterns and anomalies related to IoT devices. With their specific characteristics and instructions, an IoT device connected to a network can be expected to have a unique but identifiable pattern when transmitting data; either through a fixed amount of data, through a fixed transmission frequency (e.g., a limited number of times it connects to the network to send data), or by other recognisable behaviour related to the device type. A "disruption" in this recognisable pattern can be perceived as an anomaly and may indicate a potential threat not just to the device in question, but also to the telecom operator it is connected to.

Telenor Research, in collaboration with OsloMet (Oslo Metropolitan University), has worked to better understand these types of traffic data-driven patterns and anomaly detection in 5G networks. This work aims to develop guidelines for identifying potential threats using IoT devices, such as flooding or distributed denial-of-service (DDoS) attacks, by analysing control and data planes and understanding the behaviour of

AUTHORS:

Bernardo Flores, Oslo Metropolitan University

Van Thuan Do, Oslo Metropolitan University

Boning Feng, Oslo Metropolitan University

connected IoT devices to establish what can be called a device profile. This profiling consists of a series of unique characteristics of a specific IoT device, based on its past behaviour when connected to a mobile network, so it is possible to distinguish, for example in an IoT smart home context, between a surveillance camera and a temperature sensor. AI/ML platforms use these device profiles as thresholds when analysing traffic in a mobile network. If something falls within a device pattern spectrum but does not match the specified threshold, it will be considered an anomaly, requiring further investigation by the telecom operator's cybersecurity team.

Generating IoCs (Indicators of Compromise)

If a potential threat is indeed identified based on the detected anomalies, AI/ML-based Indicators of Compromise (IoCs) can be extracted and shared with partners within the cybersecurity community through threat exchange platforms, provided an appropriate modelling framework is used. Frameworks such as CMTMF, designed for the telecom industry, help to understand the full impact of an attack that has used connected IoT devices as a medium. Such tools can help strengthen intrusion or anomaly detection systems (I/A DS), as the sharing of data from previous attacks can make future detection more effective.

AI-based I/A DS that are designed with a focus on device-driven behavioural principles, but also with other tools to recognise various types of attacks, help prevent and limit cyberattacks to a certain extent. However, attackers aiming to exploit IoT solutions are becoming more familiar with how these systems work and have found successful and undetected ways to carry out their attacks.

This can be the case with an adversarial attack. Here, by manipulating IoT devices in an isolated manner through short bursts of data, attackers can cause intrusion detection systems (IDS) to view each isolated incident as a mere anomaly. It then becomes too late to prevent such an attack when all the infected devices are used in coordination. »»

Another focus area in the use of AI and ML within cybersecurity is the design of dynamic honeypots - a “trap” designed to lure malicious actors and isolate harmful activity from critical infrastructure.

Cybersecurity teams at telecom operators and other owners of critical infrastructure are also becoming more aware of this form of attack and are optimising their IDS and AI models to be more resilient. In most cases, there have been improvements. However, even though AI will be a tool to increase efficiency in cybersecurity, especially in handling routine work and less threatening attacks, dedicated cybersecurity teams will still be needed to support more critical and complex decisions. This is partly because the tools and models learn from past experiences and training from these very professionals. Moreover, not all established damage limitation practices will continue to be as effective as attacks (and attackers) evolve their methods.

Dynamic honeypots

Another focus area in the use of AI and ML within cybersecurity is the design of dynamic honeypots. A honeypot is a “trap” designed to lure malicious actors and isolate harmful activity from critical infrastructure. Honeypots can be real and simulated computers, services, networks, user accounts and data objects – often combined in a way that mimics an entire infrastructure. However, attackers using AI for adversarial attacks can, over time, gain sufficient information about the defence systems and identify honeypot networks, thereby attempting to avoid them in subsequent attacks. The introduction of AI-based dynamic honeypots aims to counter this through automatically reconfigurable traps to handle AI-driven adversarial attacks, based on the attacker's behaviour.

The impact of AI on society

Threats to privacy

The emergence of billions of connected devices continuously monitoring people’s activities everywhere has led to massive amounts of data being generated and collected. However, this data in itself does not pose a threat to privacy without the enormous data processing power of AI/ML.

AI/ML algorithms, including facial recognition, can identify, analyse and predict a person's movements by synthesising data from a variety of sources, such as social media posts, geotagged photos, surveillance camera footage, and so on. This ability of AI/ML can be misused by dishonest actors, criminal organisations and dictatorial authorities to monitor citizens, thus posing a threat to privacy, the right to anonymity and personal freedom.

Social manipulation through AI algorithms

One of the greatest dangers of AI/ML is social manipulation, as companies, politicians and public figures use social media to promote their strategies and political views, to gain popularity or gather votes. Social networks are flooded with content based on AI algorithms selected by themselves, often failing to protect users from harmful and misleading media content. The situation is exacerbated with the emergence of deepfakes, which enable the spread of fake news and propaganda. No one knows what is true or false anymore.

Discrimination and unfair results

Through analyses based on complex models and an immense amount of data, predictive AI/ML reaches conclusions that may not be explainable to humans. The conclusions are also not always 100% accurate, which can be fatal in areas like healthcare and other fields where greater transparency is necessary. Furthermore, biases can arise from AI/ML algorithms, where the results produced are prejudiced due to incorrect assumptions, incomplete datasets, or datasets from human decisions that reflect human biases. This can, for example, lead to discrimination based on race, gender, age, religion and more.

Managing the risks of AI/ML

AI/ML is a double-edged sword that can bring both great value and serious harm to society, necessitating an understanding of both the opportunities and limitations that AI/ML offers. More research is needed, and it is crucial to focus on privacy, freedom, fairness and ethical issues. Finally, there should be authorities that can regulate the use of AI/ML and ensure its fair use. This is exactly what both the EU and the US are working on; defining regulations to prevent the misuse of AI/ML while enabling its potentially huge contribution to society.

Conclusion

The intention and goal of AI are to benefit humanity, but if it achieves this goal in a destructive (yet efficient) way, it will negatively impact society. AI algorithms must be built to align with humans' overarching goals.

AI algorithms are driven by data. As more and more data is collected about every single minute of every person's day, our privacy is at risk. If businesses and governments decide to make decisions based on the information they collect about us, as China does with its social credit system, it can lead to social oppression.

One thing is certain: The future will definitely involve AI. Whether it is on our side or not, depends on us! It's time to use our own “natural intelligence”! //

PHOTO: GETTY IMAGES

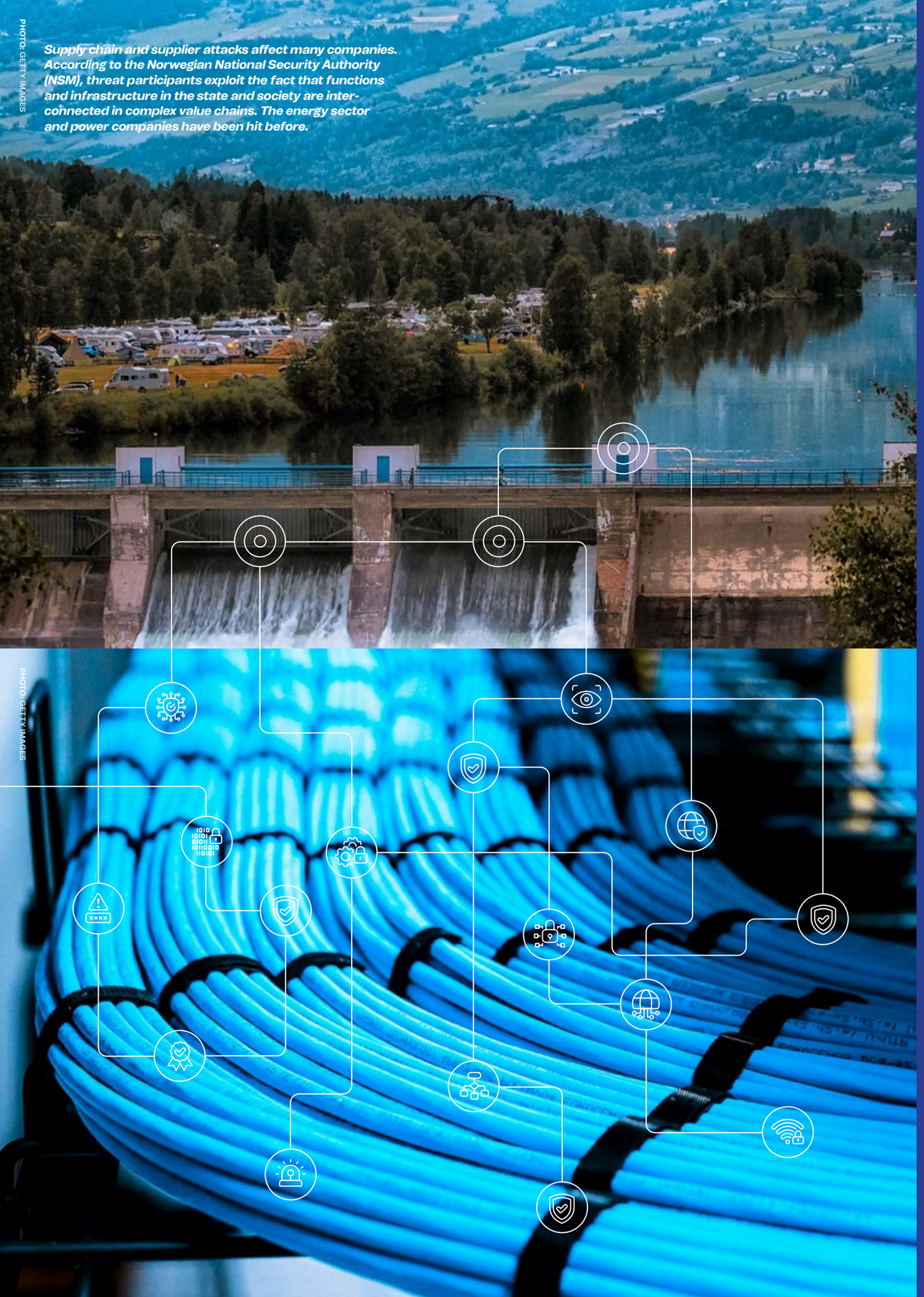


PHOTO: GETTY IMAGES

Supply chain and supplier attacks affect many companies. According to the Norwegian National Security Authority (NSM), threat participants exploit the fact that functions and infrastructure in the state and society are inter-connected in complex value chains. The energy sector and power companies have been hit before.

PHOTO: GETTY IMAGES

6

When nights are getting longer – part III

We pick up the threads from Digital Security 2020 and 2021 and take a closer look at risks related to software supply chains and continuity risks in supply chains.

IN *DIGITAL SECURITY 2020*[6] we first addressed supply chain risk in the article When the nights get long[7]. The article focused on security in the supplier interface, requirements setting, and how to create incentives and collaboration for security in deliveries, the supplier organisation, and down the underlying supply chain. In *Digital Security 2021*[8], we delved into software supply chain risk, and how best to defend against malicious attacks that would threaten a company's ability to conduct operations and serve its customers.

Everyone would wish, of course, that by now the topic of security in supply chains would have resolved itself. But alas, it is still highly relevant.

So now, in 2023 – after a 1-year hiatus from focusing on this topic in this publication – we once again address risks related to software supply chains and how the software bill of materials (SBOM) can contribute to handling them. Additionally, we look into continuity risks in supply chains, an issue also highlighted by the Defence and Total Preparedness Commissions in Norway.

Software Supply Chain

Threat actors are increasingly focusing on indirect attack vectors such as delivery and supplier chain attacks. Within software supply chain attacks, several sources report a dramatic increase. Sonatype, for example, reports a 633% increase over the past year in its latest edition of *State of the Software Supply Chain*[9]. Some of the explanation may lie in a fact Veracode highlights in its *State of Software Security* report[10]: Based on Veracode's observations, "79% of the time, once a library is included, it never gets updated."

Select Recent Attacks

Among major attacks of late, we can particularly take note of and learn from the following:

Okta

The identity and authorisation service Okta, Inc. was in the crosshairs of no less than three supply chain attacks in 2022.

In January, a subcontractor for call centre and customer service, Sitel, was compromised by the extortion group Lapsu$, which demonstrated its access by displaying screenshots of Okta's internal systems. Investigations revealed that customer data belonging to 366 businesses, approximately 2.5% of Okta's customers, was compromised. The entry point was through a third-party company, Sykes, recently acquired by Sitel.

In August, the IP telephony company Twilio was compromised – a service Okta used for sending one-time codes to its customers. A "minor number" of phone numbers and one-time codes were affected.

These first two incidents point towards the need for requirements for, and verification of, security in suppliers. It also highlights the need for security reviews as part of due diligence in acquisitions.

Finally, in December, parts of Okta's source code were exposed to unauthorised individuals when their GitHub account was compromised. Whether this last incident is definitively classified as a supply chain attack is not clear; there is speculation that the access was facilitated through one of the two previous incidents. Okta's statement that "Okta does not rely on the confidentiality of its source code for the security of its services" is somewhat reassuring: that's how it should be. However, access to source code is still useful to adversaries looking for exploitable vulnerabilities.

GitHub

In April, GitHub was hit by a type of attack that has gained significant momentum in recent years: theft of various forms of authentication and access tokens.

This could involve information in cookies and short-lived access tokens, or longer-lived keys and session IDs. In the specific case, attackers successfully obtained OAuth access tokens – a form of identifying token used to provide access over a configurable period of time without requiring re-authentication – issued to third-party integrators *Heroku* and *Travis CI*. With the stolen OAuth tokens, attackers gained access to organisations using *Heroku Dashboard* and *Travis CI* products.

GitHub's investigations revealed that the attackers systematically searched downloaded content for additional keys and tokens that could provide even more access. In this way, the attackers obtained, among other things, an AWS API key. This then granted them access to *GitHub's Node Package Manager (npm)* production environment. Fortunately, without the ability to modify any npm packages, they could only download code.

There are several points to note here. First, theft of API keys and similar tokens often results from inadequate application security or weak handling of secrets (tokens, keys, etc.) in applications, development, build, and test environments.

Second, the cleanup and removal of old permissions that are no longer in use is another often- overlooked point, both in professional application development and use, as well as when we as individuals authorise third-party services and apps for access to our accounts on social media. It is reasonable to assume that in some organisations where *Heroku and Travis CI* tools were once authorised for access, the organisations no longer actively used these products.

6 Telenor Digital Sikkerhet 2020: https://www.telenor.no/binaries/om/digital-sikkerhet/Telenor_Digital_Sikkerhet_2020_1.pdf

7 This is a non-translatable pun on the dual meaning of the Norwegian word "nettene", which can mean both "nights" and "networks". It is the title of a popular Christmas carol, but in this context doubles up as a pointer to the fact that supply networks have gotten to be very long/wide.

8 Telenor Digital Sikkerhet 2021: https://www.telenor.no/binaries/om/digital-sikkerhet/digitalsikkerhet2021.pdf

9 https://www.sonatype.com/state-of-the-software-supply-chain/about-the-report

10 https://info.veracode.com/report-state-of-software-security-2023.html

» Theft of API keys and similar tokens often results from inadequate application security or weak handling of secrets (tokens, keys, etc.) in applications, development, build, and test environments.

Finally, the handling and follow-up measures taken have been commendable, from all parties involved.

GitHub, regardless of the incident, developed a service that scans code for secrets before it is uploaded to distribution channels.
From a supply chain perspective, it is worth highlighting notification and action: GitHub was quick to notify all affected users, and both Heroku and Travis CI notified their customers and implemented revocation and reissuance of tokens and keys for their services. The latter is not an easy decision, as it affects their services and customers, but it is the right decision to minimise damage and security risks.

Fishpig

For those who may not have heard of FishPig before, it is software for integration between the extremely popular publishing platform *WordPress* and the very widely used e-commerce software *Magento*. FishPig is used in over 200,000 online stores.

Attackers compromised FishPig's distribution servers, i.e. the servers from which customers retrieve software and updates. They uploaded modified versions of the software that, when downloaded and installed, infected customers' systems with the *Rekoobe* trojan, providing attackers with a backdoor into customers' systems. The damage potential was significant, as these are online stores with payment functions. *Magento*-based online stores have been a favoured target for financially motivated threat actors for years, leading to significant losses in some cases.

There may be reason to question the security monitoring at FishPig, as attackers had access for about 12 weeks before the then ongoing supply chain attack was uncovered.

From a supply chain perspective, this type of attack is challenging for customers because attackers succeeded in including their code in seemingly authentic software. Mechanisms for automatic updates – generally recommended from a security standpoint – also limit the possibilities for actions such as test-running the update in security-instrumented test and sandbox environments before installation in production. In any case, measures such as test-running the update would be excessively resource-intensive for many of the affected customers.

While these attacks are challenging, better planning might have helped. *Rekoobe* is a known malware family, and *endpoint detection and response (EDR)* tools on Linux servers can be an effective tactic to detect its presence and behaviour. It is also crucial to subscribe to and respond to alerts from suppliers.

After the incident, FishPig provided exemplary guidance to affected customers, such as tools that enable even customers with limited expertise to clean up a compromised online store.

3CX

In March 2023, it was revealed that software from the IP telephony company 3CX had been compromised. The exact duration is unclear, but the first reports of observed anomalies among user organisations – initially assumed to be false positives – emerged March 22.
The legitimate software of 3CX, used by over 600,000 companies and more than 12 million daily end-users, turned out to have been supplemented with malicious code for DLL *sideloading*. In simple terms, this involves inclusion of instructions in the software installation routine to fetch additional code libraries (DLL) from an external source.

The 3CX attack harkens back to the well-known SolarWinds attack, and really all the way back to the attacks by "APT 1" on *managed service providers* (MSPs). One thing common to APT1, SolarWinds, and a portfolio of intermediate campaigns is the ability and willingness to use supply chain attacks (which have a very broad, visible impact) to take adversarial action on only a few select targets. This modus operandi, along with the absence of economic gain, points towards intelligence-motivated actors.

From a supply chain perspective, we note that the 3CX attack was actually made possible through another *software supply chain* attack on a company called Trading Technologies and their software for securities (futures) trading, *X_Trader*. Several security analysts and media outlets describe this as the first time one software supply chain attack has led to another.

The infected version of *X_Trader* was simply downloaded and installed by an employee at 3CX. There is broad consensus among analysis companies that the *X_Trader* campaign and the subsequent attack through 3CX's software are connected to the North Korean *"Lazarus Group"*.

The *X_Trader* campaign targeted several other companies, including at least two power companies in the USA and Europe. »

The broad secondary campaign through 3CX, targeting the energy sector, and compromising software for securities trading all raise questions about whether the attacker's motivation was primarily economic or geopolitical. Even with strong attribution, it can be challenging to conclude, as *Lazarus Group* appears to be motivated by both.

Recursive Dependencies – A Persistent Challenge

We also observe that the organisation of some open-source ecosystems presents security challenges and opportunities for attackers, particularly in the way development handles *dependencies*. In this case, *dependencies* refers to code or software modules that another software project relies on and, therefore, is dynamically fetched and included. In some ecosystems, such as *npm*, these recursive dependency structures can be very deep.

Several attack concepts take advantage of this, as well as other aspects of how open-source development and distribution is organised:

Malicious dependencies – Event-stream incident[11], 2018
In August 2018, a developer with the screen name "Antonio Macias" published the *flatMap-stream* parser library on *npm*. He contacted the developer responsible for the widely used parser library *event-stream* and suggested including the *flatMap-stream* parser library as a *dependency* to the *event-stream* parser library. That September, the next version of *event-stream* was released, dynamically incorporating *flatMap-stream* code. In October, the codebase of *flatMap-stream* was updated with malicious code. From that point on, all new installations of event-stream continued to automatically pull in *flatMap-stream*, thus also including the malicious code into event-stream.

Event-stream is a popular package and itself a *dependency* in at least 3,931 other packages. However, the real target of the attack was a single software project: the highly popular bitcoin wallet *Copay*. The introduced code in *flatMap-stream* was effective only within *Copay*, enabling the theft of bitcoins and private keys.

Dependency confusion – Alex Birsan, 2021
In Digital Security 2021, we discussed how security researcher Alex Birsan demonstrated "dependency confusion" attacks[12] early in the year:

"An additional factor contributing to reducing time and cost is the dynamic use of third-party libraries like Node, JQuery, and Chartbeat. Dynamically included libraries are either downloaded when the application is built or when it runs in a browser. On one hand, such libraries often contribute to more secure code, as they frequently help programmers 'do things right,' while on the other hand, they increase the risk of compromise through the supply chain. This was aptly demonstrated in February when a security researcher described how he had exploited this type of dynamic download by publishing packages with conceptual 'malware' to various public frameworks (npm, RubyGems, and PyPI) with the same or nearly the same names as several major technology companies used for their internal modules."

The consequence was that automatic build tools at the affected companies loaded Birsan's publicly published software components with the same names, instead of components from the company's private internal codebase. This behaviour basically allows for anyone gaining knowledge of internal package names, to replace private code with their arbitrary code. .

Npm Manifest Confusion attack[13], 2022
npm packages have a so-called "manifest file," which contains metadata about the code package and lists dependencies on other packages. Former GitHub employee Darcy Clarke has uncovered that there are no mechanisms comparing the published manifest file with the one included in the tar-compressed downloadable code package.
Many software security tools evaluated software packages only on the basis of the information in the standalone manifest file. Build tools, however, orchestrate the build process based on the version included in the tar-compressed package. This provides an opportunity for a publisher or attacker to include malicious or known vulnerable code in the included manifest file, and thus in the built software, while the standalone published manifest file may not mention it and security tools thus not detect it.

Repojacking, 2023
Security company Aqua Security published information[14] in the summer of 2023 from a study of 1.25 million code projects on GitHub. They found that nearly 37,000 of the projects were vulnerable to a technique known as repojacking. The technique is simple and involves threat actors registering code projects with project or usernames that are no longer in use. This could be due to the user account being cancelled or the project changing its name. Projects having an affected project as a dependency may be unaware of the change and may thus continue trying to fetch the project's code from the original user account or project name. This gap allows threat actors to publish code that others automatically fetch and use in their projects, simply by re-registering the old name. Aqua Security has only scanned a small sample and claim the actual attack surface to likely be several million code projects – not just the nearly 37,000 identified.

11 https://snyk.io/blog/a-post-mortem-of-the-malicious-event-stream-backdoor/
12 https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610
13 https://www.bleepingcomputer.com/news/security/npm-ecosystem-at-risk-from-manifest-confusion-attacks/
14 https://blog.aquasec.com/github-dataset-research-reveals-millions-potentially-vulnerable-to-repojacking

PHOTO: ANDREJ VASILENKO / THE NEW YORK TIMES / NTB

Taiwan's representative office in Vilnius, Lithuania.

What Do Norwegian Authorities Say?

Norwegian authorities, through reports from PST (Police Security Service), NSM (National Security Authority), and the Intelligence Service, have addressed various forms of threats and attacks through supply chains. We particularly note the following.

PST: National Threat Assessment 2023
«In January 2022, Lithuania experienced a comprehensive and complex reaction from the Chinese authorities when the country allowed Taiwan to open a representative office in Vilnius. Following the incident, Lithuania faced an influence campaign and several digital network operations. Additionally, the country was subjected to extensive supply chain pressure, service interruptions, and other formal and informal sanctions. Meanwhile, companies in Lithuania had difficulties obtaining Chinese parts and components. Chinese authorities also exerted pressure on businesses in other European countries to limit their trade with companies from Lithuania.»

«Over the past year, PST has observed that several state intelligence services or threat actors operating on their behalf have carried out so-called value chain attacks. These are network operations targeting weak and more peripheral points in a company's value chain, such as subcontractors. Companies with robust data security systems and procedures are vulnerable if their subcontractors do not have equivalent security measures. PST expects more network operations of this kind in 2023.»

«State actors employ a broad range of methods to bypass control mechanisms and secure access to technology and knowledge from Norwegian businesses. Tools such as fake documentation, complicated corporate structures, straw and front companies, and supply chains will also be utilised.»

Intelligence Service: Focus 2023
«Collaboration also creates vulnerability. Dependencies in supply chains are exposed, opening the door to extortion.»

NSM (National Security Authority): Risk 2023
«Even if a business has good physical and digital security, threat actors can exploit subcontractors with much weaker security to gain access to their true targets. This means we also need to secure ourselves well on the flanks.»

Several U.S. agencies and bureaus have distinguished themselves in advocating for the need for transparency in software deliveries and supply chains, emphasising the use of SBOMs.

«Our security is no stronger than the weakest link in the supply chain.»

«Long and complex supply chains still pose a vulnerability that threat actors know how to exploit. In recent years, we have seen many examples of supply chain attacks against providers of ICT services with very large customer bases having extensive consequences.

Outside the digital realm, we also observe threat actors exploiting supply chains to gain access to their true targets. When the goal is to impact a major enterprise, it requires fewer resources to attack a less secure subcontractor or individuals.»

NSM (National Security Authority): Security Advisory
«Threat actors exploit the fact that functions and infrastructure in the state and society are interconnected in complex value chains. Incidents seemingly directed at values in one part of a value chain may, in reality, be constructed to target an actual goal elsewhere in the chain.»

«Insufficient oversight of supply chains and the absence of security requirements for suppliers in acquisitions and projects open up the possibility for threat actors to use procurement processes as a means to access values. Consequently, threat actors can impact the business through suppliers and subcontractors.»

Software Bill of Materials

Software bill of materials (SBOM) is a specification of all the components in a software package. This is now a widely recognised term, but the journey to this point has been long, and there is still some way to go..

SBOM milestones
Among the milestones achieved so far, it is worth highlighting:

- October 2015: The SWID Tags standard from *NIST* published as ISO/IEC 19770-2:2015.
- March 2018: Version 1.0 of *CycloneDX*, an SBOM standard from OWASP.
- December 2020: ISO publishes "The ISO International Standard for open source license compliance" (ISO/IEC 5230:2020 – Information technology — OpenChain Specification), with requirements for a process for handling SBOM for delivered software.
- 2020/2021: The U.S. *National Telecommunications and Information Administration* (NTIA) publishes significant work from its *Software Component Transparency initiative* related to SBOM.
- February 2021: President Biden signs *Executive Order* 14017 on *America's Supply Chain*, requiring SBOM for federal acquisitions.
- May 2021: President Biden signs *Executive Order* 14028 on *Improving the Nation's Cybersecurity*, requiring, among other things, security testing and vulnerability management, and emphasising the role of SBOM.
- July 2021: NIST publishes its *Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software Under Executive Order (EO) 14028.*
- August 2021: The open SBOM framework SPDX, from the *Linux Foundation*, is published as the standard ISO/IEC 5962:2021.
- April 2023: Version 1.0 of the Supply-Chain Levels for Software Artifacts (SLSA) framework is published by the Open Source Security Foundation.

Despite several contributions being endorsed through the international standardisation organisations ISO and IEC, this list is dominated by United States elements, primarily for two reasons. Firstly, the technology industry and its actors, both on the non-profit and commercial side, are largely based in the U.S. Secondly, there is significant market influence when the U.S. federal sector begins to impose requirements on all its technology suppliers, leading to the operationalisation of directives and certifications, such as EO 14017 and 14028.

These measures, detailed through various directives and certifications not outlined here, have a global impact by compelling relevant suppliers to comply to be eligible for a supplier role going forward. This includes aspects like securing their software development environments, understanding their software supply chains, and being able to document their software deliveries through SBOMs.

A more prominent role in professional advice
Several U.S. agencies and bureaus have distinguished themselves in advocating for the need for transparency in software deliveries and supply chains, emphasising the use of SBOMs. Comprehensive introductory and training materials are available, particularly from the National Telecommunications and Information Administration (NTIA)[15] and notably the highly productive Cybersecurity and Infrastructure Security Agency (CISA)[16]. The latter, for instance, states:

«A «software bill of materials» (SBOM) has emerged as a key building block in software security and software supply chain risk management. A SBOM is a nested inventory, a list of ingredients that make up software components. The SBOM work has advanced since 2018 as a collaborative community effort, driven by National Telecommunications and Information Administration's (NTIA) multistakeholder process.

CISA will advance the SBOM work by facilitating community engagement, development, and progress, with a focus on scaling and operationalization, as well as tools, new technologies, and new use cases. This website will also be a nexus for the broader set of SBOM resources across the digital ecosystem and around the world.

An SBOM-related concept is the Vulnerability Exploitability eXchange (VEX). A VEX document is an attestation, a form of a security advisory that indicates whether a product or products are affected by a known vulnerability or vulnerabilities.»

15 https://ntia.gov/page/software-bill-materials
16 https://www.cisa.gov/sbom

In Europe as well, SBOM has gained increased attention from the authorities, including statements from ENISA, which in its Threat Landscape 2022 declares:

«It is almost certain that adversaries will further abuse this lack of visibility into dependencies, as well as the increased complexity and the trust organisations put into their suppliers, to gain a foothold within organisations. We need to highlight initiatives such as the Software Bill of Materials (SBOM) that aim at making such things more transparent and auditable. Gaining visibility into the web of third-party relationships and dependencies is a must. »

ENISA similarly emphasises this in *Good Practices for Supply Chain Cybersecurity, linking it – like CISA – to vulnerability management:*

«The handling of vulnerabilities has two aspects; one aspect is the monitoring of vulnerabilities which leads to an analysis on the vulnerabilities identified up to a patch delivered and deployed. The other aspect is the publishing of advisories, i.e. the vulnerability notifications. A vulnerability notification has the objective to warn product users of critical vulnerabilities and might recommend alternative mitigation measures to minimise the likelihood of an exposure. Tools that support the operators as well as the developers towards this direction are the software bill of materials and Vulnerability Exploitability eXchange concepts, and the Common Security Advisory Framework.»

A selection of relevant specifications and frameworks

CSAF: Common Security Advisory Framework (CSAF)[17] is a specification from OASIS for the exchange of structured machine-readable security advisories. The transition to unified machine-readable structures for security advisories, rather than prose text that needs to be crafted and consumed by humans, is crucial for automation—both in terms of generation and, especially, in terms of receiving, processing, and further utilising the information in vulnerability management.

VEX: Vulnerability Exploitability eXchange (VEX) is a structured format for vulnerability information, specifically focused on communicating whether software is vulnerable to a particular vulnerability and providing recommendations for handling it. VEX is an information profile in CSAF, but VEX messages can also be part of other specified information structures, such as CycloneDX.

CycloneDX: OWASP CycloneDX[18] is a comprehensive bill of materials (BOM) standard that not only specifies a structure for software bill of materials (SBOM) but also includes:

- Software-as-a-service bill of materials (SaaSBOM)
- Hardware bill of materials (HBOM)
- Operations bill of materials (OBOM)
- Vulnerability disclosure reports (VDR)
- CycloneDX also has a profile for Vulnerability Exploitability eXchange (VEX)

SPDX: Software Packaged Data Exchange[19] is an open standard for the SBOM format, supported by a consortium of stakeholders from the technology industry. It is now also formally standardised as ISO/IEC 5962:2021.

SWID: Software Identification (SWID) Tags is a format for describing a software object and originates from software asset inventory and management since 2012 when it was first specified as an ISO standard. The latest applicable formal standard is ISO/IEC 19770-2:2015. The format is part of specifications by, among others, the Trusted Computing Group (TCG) and the Internet Engineering Task Force (IETF). A SWID tag can also be part of a CycloneDX SBOM.

SLSA: Supply-chain levels for software artifacts[20] is a security framework for software manufacturing and distribution. The framework includes guidelines, checklists and controls to counteract illegitimate influence, primarily on the integrity of the software, at all stages from production to use. Where SBOM can be compared to the ingredient list on food items, SLSA can be likened to guidelines for the safe manufacturing, distribution, and storage of food. To clarify, the framework encompasses manufacturing, not development, as SLSA does not address the quality of the code being written as it relates to security, but instead focuses on what happens afterward. The framework is useful for both manufacturers and consumers by providing guidance and measuring good security practices, respectively.

17 https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.html
18 https://cyclonedx.org
19 https://spdx.dev
20 https://sisa.dev

Continued scepticism – the chicken and the egg
While SBOM, along with VEX and CSAF, is promoted by both security professionals in general and influential authorities in particular, there is still some scepticism. Many critics doubt the value of SBOM, as many of the recipients do not have processes and tools in place to leverage the information. The structured information must be received and integrated into the organisation's processes and systems, including asset inventory and vulnerability management, to provide real value. Transfer and processing must also have tool support that facilitates a high degree of automation, as the information is dynamic and updated frequently.

It is legitimate to question the current value of requiring SBOM for all delivered software, especially since many organisations face significant challenges with basic processes and tools in knowing what they have (inventory) and managing vulnerabilities and vulnerability information (referred to collectively as vulnerability management). Vulnerability information, too, must be produced, distributed, and consumed in machine-readable formats that enable automation.

This is, to some extent, a classic "chicken and the egg" problem; no one invests in tools to handle information that does not exist, and few see the need to demand or provide information that few have the capability to effectively leverage.

However, many security experts agree that control over what you have and the vulnerabilities it contains is a prerequisite for adequate digital security. We must start somewhere, and just like the chicken and the egg, there is actually an answer[21].

Tool support must also be in place at software producers to generate SBOM and VEX data in a resource-efficient and agile manner, and this tool support may also take time to implement. Therefore, there is no reason to wait to state demands, and to meet them. Without requirements, nothing happens, and we will have a long wait for both chickens and eggs.

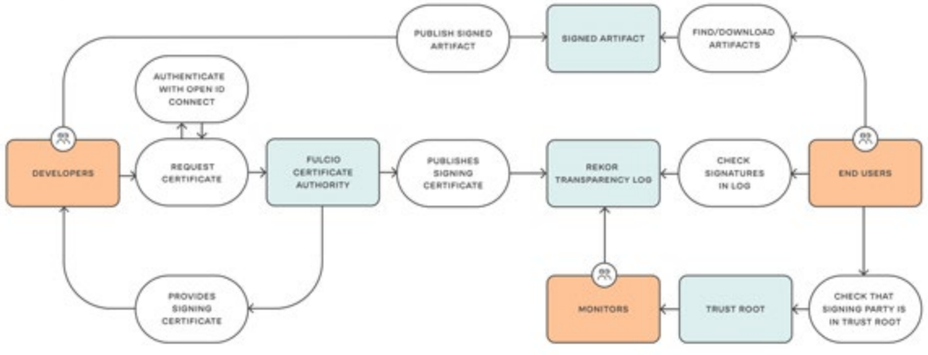
There must first be information to process, even though the tools and processes to manage it optimally and garner maximum value from it are still lacking in many organisations, and similarly remain to be introduced at many software producers. We cannot afford to remain in the status quo.

Today's situation in software management and software security is dire, and current practices do not work and do not scale. We imperatively need to transition to a high degree of automation in the exchange and use of software and vulnerability information.

Ensuring authenticity in open source code – several initiatives on the horizon
Although code signing and publishing checksums that can be verified upon download are far from new, comprehensive and standardised solutions for scalable signing and traceable authenticity for open-source code have been lacking. This has led to much use of open-source components in software projects either relying on trust on insufficient grounds or depending on retrospective control using third-party tools searching for "known bad." Signing and traceable authenticity for open-source components, libraries, images, and more have therefore gained increasing attention. One such framework is *Sigstore*[22], backed by Google, Redhat, Linux Foundation, Chainguard, and Purdue University.

Another approach to stay ahead, rather than searching for and uncovering malicious influence after the fact, is to use third parties who perform security vetting of popular open-source code and republish it in their own distribution channels. One such service that has gained much attention since its launch in 2022 is

The sigstore ecosystem



SOURCE: HTTPS://SIGSTORE.DEV/HOW-IT-WORKS

21 https://www.science.org.au/curious/earth-environment/which-came-first-chicken-or-egg
22 https://www.sigstore.dev

PHOTO: AFP PHOTO / SATELLITE IMAGE ©2021 MAXAR TECHNOLOGIES / NTB

The container ship Ever Given ran aground in the Suez Canal, spring 2021.

Google Assured Open Source Software[23]. While Sigstore ensures verifiable and traceable origin and authenticity, Google Assured Open Source Software goes considerably further, including:

- Build process and documentation in accordance with SLSA-2
- Comprehensive SBOM for each package, with additional information such as vulnerability information, in SPDX and VEX formats
- Fuzzing[24] and vulnerability testing
- Distribution from infrastructure operated and secured by Google

Continuity and Availability Risks in Supply Chains

Several events, to some extent coinciding, have posed significant challenges in supply continuity in recent years, highlighting a different type of supply chain risk: supply continuity and availability disruptions.

The societal impact of the Covid-19 pandemic, a ship stuck in the Suez Canal[25], increased geopolitical tension with conflicts on various fronts, including trade, and the outbreak of war in Europe have each influenced supply continuity in their own way, and underscored how dependent the world has become on supply continuity, and thus vulnerable to such events.

The Pursuit of Efficiency
Since its origin in Japan in the 1950s and 60s, just-in-time production has spread widely as the preferred method for resource- and capital-efficiency optimised manufacturing. The concept, along with the necessary just-in-time logistics, permeates throughout the entire value chain and has, from the 1970s to the 1990s, gained global prevalence across industries.

In short, nothing is produced or delivered to the next link in the supply chain until there is a concrete need, order, or forecasted need for it. There are few or no buffers; all processes are optimised, and inventory is considered "waste" (cf. Lean/Kaizen).

This approach creates a significant need for coordination and vulnerability to consequences in case of disruptions in one part of the supply chain. Both of which only worsens as each link in the supply chain becomes ever more specialised, leading to more suppliers, and supply chains become deeper and broader. This has driven a different dimension of risk in supply chains: supply continuity risk. Including this as a "security risk" might inspire many interesting discussions over semantics and professional terminology, but it is undoubtedly a risk dimension that, since the last time we addressed suppliers and supply chains in Digital Security, has repeatedly manifested itself and gained increased attention. In the context of an increasingly tense geopolitical situation, control over the supply of critical goods and materials has been weaponised.

23 https://cloud.google.com/assured-open-source-software
24 Fuzz testing or "fuzzing" aims to find potentially exploitable coding errors and security issues in software or networks by exposing them to large amounts of random and unexpected input data.
25 https://en.wikipedia.org/wiki/Ever_Given

The Supply Chain – Part of Continuity and Resilience

In Digital Security 2022[26], largely based on the experiences of disruptions in supply chains and acute needs that arose in Ukraine in the weeks and months following the invasion, we argued that Norway should consider establishing buffer stocks of standard information and communication technologies (ICT) components. However, this is only one proposal within – broadly speaking – one industry. It is in part addressed to Norwegian authorities, based on our reflection that this is a form of essential national resource.

For businesses in general, including actors in critical sectors with fundamental national functions, an assessment of supply continuity risk and measures to address it must be part of each organisation's plans for continuity and resilience.

This opens a Pandora's box of information needs:

- Do we have an overview of our critical resources, and do we know who the critical suppliers are?
- Have we taken into account that the loss of some resources that may seem less critical in their nature can still cause continuity disruptions to the organisation?
- Do we know who the critical sub-suppliers to the suppliers are, and how far down the chain can we gain and maintain visibility?

It also motivates innovative thinking regarding potential risk-reducing measures:

- Given foreseeable scenarios in an ever more unpredictable world with heightened geopolitical tensions, could it make sense to actually tie up more capital in stockpiling critical resources?
  - Can we collaborate with someone on this? Perhaps even competitors? Can industry associations play a role in coordinating joint efforts?
  - Can we achieve such collaboration among competitors without breaching competition and anti-cartel laws and regulations?

- Should we diversify the supply chain and spread supply continuity risk by establishing multiple alternative suppliers for the same critical resources?
  - Do we then know that the suppliers do not ultimately rely on the same critical input factors/sub-suppliers? (Thus nullifying most of the risk mitigation effect.)
  - Could the increase in security risk associated with broadening the supply chain, in which more suppliers and sub-suppliers become vectors for supply chain attacks against us, actually be greater than the reduction in supply continuity risk?

From Telenor Digital Security 2022:

It should be considered whether national emergency stockpiles for standard/"Commercial Off-the-Shelf" ICT components should be established. Prioritised product categories and products will require further analysis, but both basic network equipment, servers, and end-user equipment will be relevant. The emergency stockpiles can serve as a national buffer with continuous turnover. The arrangement must be binding for "member companies" to ensure that product categories are not kept in stock for a long time and become outdated. The companies we are referring to here are primarily public and private owners of critical infrastructure supporting essential societal functions.

Highlighted by the commissions

Both the Defence Commission and the Total Preparedness Commission emphasise in their assessments, both generally and within specific sectors, the importance of preparedness and resilience. The vulnerability created by long and complex supply chains is thoroughly discussed, with clear conclusions about the need for strengthening and measures — primarily initiated by, but certainly not exclusively in the context of — government agencies.

It is also noted that many critical components are produced by very few geographically concentrated actors or are dependent on input factors (minerals, etc.) where active sources are geographically concentrated. The vulnerability resulting from super-efficient just-in-time supply chains is also highlighted. Among the commissions' measures, we find: strengthened self-sufficiency, buffers, and emergency stockpiles, supplier diversity for having multiple options, and strict guidelines regarding which countries of origin we should dare to expose ourselves to or become dependent on for supplies.

From the report of the Total Preparedness Commission (NOU 2023:17), we would like to highlight, among other things:

«There is a need for greater resilience regarding the storage of critical input factors and increased self-preparedness. We have experienced a long period of globalisation and increasingly efficient but complex international supply chains. This has provided us with inexpensive trade goods. At the same time, our own stockpiles have been reduced, and in certain areas, we have become dependent on countries and regions with which we do not share common interests.»

«China continues to challenge the Western community in several ways. The country seeks to control strategic infrastructure, resources, and value chains.»

«The pandemic and the war in Ukraine have exposed vulnerabilities related to access to expertise and materials. It is not guaranteed that specialised expertise and spare parts are always available from abroad.»

«Societal functions are becoming increasingly dependent on long and complex digital value chains, making it more challenging to control all involved actors and subcontractors. Dependencies in multiple links increase the risk of vulnerabilities being exploited, digital services becoming unavailable, unauthorised access to sensitive content, and content being altered in a way that makes it uncertain what is genuine or false.»

«The close connection between digital systems and long digital value chains with often unknown dependencies on a large number of actors further complicates the work of digital security.»

«The Commission believes that digital services have become so crucial for maintaining critical societal functions that authorities must take greater responsibility for security across value chains and across all sectors of society.»

«To reduce digital vulnerabilities nationally in critical infrastructure, it has become increasingly important to determine which countries one does not want materials from or other forms of dependence. The Commission believes that going forward, Norwegian authorities must, to an even greater extent, set conditions and provide advice regarding which countries, technologies, and services are considered a risk to national security.» //

26 Telenor Digital sikkerhet 2022: https://www.telenor.no/binaries/om/digital-sikkerhet/2022/Digital_sikkerhet_2022.pdf

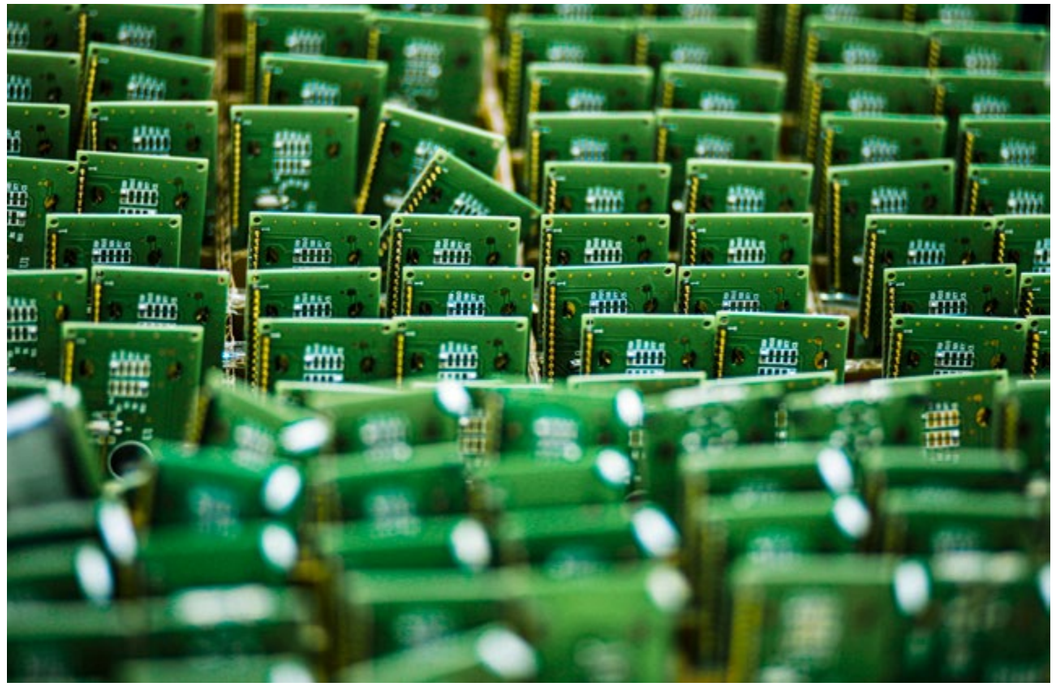


PHOTO: GETTY IMAGES

PHOTO: GUNNAR RIDDERSTRØM / UNSPLASH

PHOTO: GETTY IMAGES

A large proportion of all data traffic in Norway goes through Telenor's services and infrastructure. This gives us a significant social responsibility and means that we must provide stable and secure services in peace, conflict, crisis, and war.

7

It is more serious now

The global community wonders each day what tomorrow will bring. Russia's invasion of Ukraine entails a lasting change in the security situation in our region. Increasing geopolitical tension confronts owners of critical infrastructure with an increasingly complex landscape of threats and risks. The times we live in have never been more dynamic. The world is in a place where the destinies of individuals, nations and regions shift almost by the hour. Global changes will affect our choices for how we manage risk, protect our industries and national infrastructures, and work with authorities in the markets where we operate.

As we survey the present and ponder the future, certain truths emerge: Private companies must be part of overall contingency planning. More common solutions must be developed in a Nordic and Nordic-allied framework.
We have to be prepared.

Everything has to work
A modern infrastructure requires a solid and secure foundation, where vulnerability is reduced to a minimum. The premise of the digital foundation in 2023 is that everything has to work, all the time. Succeeding in this will be a decisive factor for how well we succeed in simplifying, improving and renewing our own operations and supporting the digitalisation of society.

The changed security situation affects the choices we make. Over the past 10-12 years, Telenor has built a holistic security organisation in Telenor Norway to safeguard and protect ourselves and our customers, and to help fulfil our social responsibilities. We work systematically in three areas: security, robustness and emergency preparedness to build, operate and develop as robust and secure a digital infrastructure as possible. We have increased vigilance in both the digital and physical domains, a lower threshold for reporting incidents, and even closer cooperation with the authorities, such as the National Security Authority (NSM) and the Norwegian Communications Authority (Nkom).

Meeting the technological and geostrategic shift
Over the past year, we have received a number of important reports that form the impetus for strengthened work on security and emergency preparedness. The Defence Commission (Forsvarskommisjonen) has made several recommendations to strengthen the capacity for cross-sectoral situational awareness and crisis management: that a national security strategy (NSS) be developed, that the Office of the Prime Minister (SMK) be given more staff power, and that the role of the crisis council (Kriserådet) be expanded.

The Total Preparedness Commission (Totalberedskapskommisjonen) has proposed a more robust emergency preparedness system, adapted to the challenges of our time. The report describes an improved emergency preparedness system with resilience to all forms of danger, across the crisis spectrum, and for as long as the situation lasts. The Commission summarises its main recommendations in ten points. A number of them concern Telenor's operations, in particular: closer integration of the business sector into the national emergency preparedness structure, expanded Nordic emergency preparedness cooperation, and intensified work on infrastructure and cyber security. These are all of strategic importance for our business.

The sum of changes in global power relations, increased regional instability, fragmentation of the international system and a higher willingness to take risks and use force against other states mark a new security policy situation. In the years to come, Europe will have to take far greater responsibility for its own security. The same applies to Norway, as a rich and vulnerable small state with an open democratic society, an outward-looking economy in a geopolitically vulnerable area.
from NOU 2023: 14 The Defence Commission of 2021 - chapter 17.1 A new era

27 https://www.regjeringen.no/en/dokumenter/meld.-st.-9-20222023/id2950130/

Telenor's role as emergency preparedness actor
Telenor in Norway owns and manages infrastructure critical to society, and ensures safe and stable deliveries of digital services on fixed, mobile and broadband. This includes delivering voice, data and SMS as National Critical Funtions (GNFs) , which are critical for the functioning of Norwegian society. A large proportion of all data traffic in Norway passes through our services and infrastructure. This gives us a significant social responsibility and means that we must deliver stable and secure services in peace, conflict, crisis and war. We recognise that we are a target for advanced threat actors. Our business is subject to the Security Act.

For private companies such as Telenor, it has been important to emphasise that governance and cooperation must be formalised in order to achieve a more effective total defence in these areas, where private enterprises and companies are more systematically involved. Private enterprises in oil and gas, power, food, and electronic communications are important elements for maintaining societal security and state security because they own critical infrastructure. They have a natural role in total defence to provide insight and expertise about the functions they maintain and the dependencies they have to others. The fact that the Security Act is not fully implemented in all sectors is an obstacle to this.

New opportunities with the entire Nordic region in NATO
We have a long tradition of working closely together in the Nordic region. With Sweden and Finland in NATO, everything is in place for strengthening and furthering Nordic cooperation in the digital domain. Such cooperation is important to ensure robust and secure infrastructure in times of crisis and war. The experiences from Ukraine, where the international community and industry partners have participated, shows the importance of international cooperation to sustain digital services and infrastructure. It is incumbent on private companies in the Nordic region to develop this cooperation to its potential.

It is a positive sign that the Norwegian Ministry of Justice and Public Security has announced that «*The government will map strategically important infrastructure in order to identify which allies and close partners we are most dependent on in order to secure national control, and will establish a close, binding and predictable collaboration with them*»[27]. At the same time, there is a need for a greater degree of cooperation across national borders. The security situation we face today is different and requires new strategies and choices. Closer Nordic cooperation could contribute to a more rapid effect if Nordic industrial partners can mobilise innovative power within frameworks based on strategic cooperation agreements.

We have taken note of the initiative for more binding cooperation and integration between the Nordic countries in the defence sector, and consider it natural that this should be seen in connection with similar processes on the civilian side. In our opinion, it is now very important that the electronic communications industry be given the latitude to share technical solutions and infrastructure

In their input to the Commission, several players in the Norwegian electronic communications sector have emphasised that they define the entire Nordic region as their home market. Within the framework of proper security, Telenor believes that autonomy must be understood in a Nordic context. In the changed security situation, reference is made to the initiative on more binding cooperation and integration between the Nordic countries in the defence field. In this connection, a desire is expressed for a Nordic initiative within the sector to use scarce personnel resources between Nordic neighbours and use technical solutions and infrastructure such as fibre and data centres across countries in the Nordic region. This will strengthen national security of supply with more resources close to Norway, and it will strengthen the Nordic region as a whole and stimulate the multinational technology suppliers to establish centres of expertise in the Nordic region.
from the Total Emergency Preparedness Commission's NOU 2023: 17 - Now it's serious

across the Nordic region, within the framework of proper security, for increased resilience and robustness.

Telenor has particularly noted that the Total Preparedness Commission recommends that *"Norwegian authorities, in connection with the Finnish and Swedish NATO membership, take the initiative for cooperation on cyber security and increased preparedness in the Nordic region"*. In Telenor's view, a Nordic initiative is needed to make better use of technical solutions and infrastructure such as fibre and data centres across Nordic countries and to make better use of the limited human resources with expertise in this domain. This will strengthen national security of supply with more resources close to Norway and the Nordic region as a whole, and stimulate the multinational technology suppliers to establish centres of expertise in the Nordic region. Such cooperation will require changes and harmonisation of national regulations. This work should be initiated immediately.

Closer integration of business and industry
It is positive to see increasing recognition of the business sector as an emergency preparedness actor and emergency preparedness resource. From a preparedness perspective, this is crucial, as the Total Preparedness Commission has emphasised that "the business sector is more closely linked to the emergency preparedness and crisis management systems from the central level to the regional and local levels".

Telenor is a recognised Total Defence actor. It is not in ministries or directorates that National Critical Funtions (GNFs) will be affected, it will be in public and private, civil and military enterprises. Such actors with a critical function must therefore be better integrated into Total Defence in order to provide the insight and expertise needed to be better prepared to work together in conflict, crisis and war. This will require formalisation and considerable further work to have an effect.

Based on the commissions' reports, the Government and the Parliament (Storting) have an exceptionally good basis for clarifying frameworks, roles and expectations for critical enterprises in the private sector. Such a strengthening of emergency preparedness capacity should be driven by a need for innovation, transformation and sustainable value creation. A more strategic approach to the development and protection of competence and technology in critical communications should be given priority.

Strengthen the ability to handle digital incidents
Telenor takes note of the government's ambition for Norway to stage a coordinated response to national incident management. In Telenor's view, there is a need for strengthened cross-sectoral cooperation that brings together all domains, and where both public and private actors participate. In our view, the sector principle and associated fragmented coordination fall short in this regard.

Telenor took note of the Office of the Auditor General's investigation of the authorities' coordination of work on cyber security in the civil sector; Document 3:7 (2022-2023). The Office of the Auditor General confirms that "weak coordination of roles, responsibilities and requirements makes the work on cyber security demanding for the agencies", that cross-sectoral incident management has not been "adequately facilitated", and that there is "a need for more training in cross-sectoral handling of incidents at the national level". Telenor shares these assessments.

Training and exercise
Telenor has previously advocated for exercises across sectors where we test collaboration, interaction, leadership and coordination that may be relevant to handling actual incidents. In this context, the importance of practicing real-world scenarios must be emphasised.

In Telenor's view, increased use of exercises could contribute to strengthened cross-sectoral cooperation and leadership at strategic, operational and tactical levels. Good shared situational awareness, not just information sharing, will also put everyone »»

The role of the Crisis Council (Kriserådet) should be expanded to strengthen the capacity for cross-sectoral situational awareness and crisis management across sectors. The number of members should be expanded to include a broad-based civil service group with representatives from all key emergency preparedness actors, the business sector and the regional level. This will both strengthen the analysis work and pave the way for better and broader basis for decision-making for the Government. The Central Total Defence Forum (Sentralt Totalforsvarsforum) should be developed into a national Total Defence and Emergency Preparedness Council with strengthened authority as advisor to the Government, with regard to prevention, preparedness and national crisis management. This council should have a flexible format that can be adapted and expanded, and that includes selected commercial enterprises and social partners.
from NOU 2023: 14 The Defence Commission of 2021 - chapter 17.2.2 New requirements for governance, management and resource use

Exercise “Bukkesprang”

Since 2017, Telenor Norway has organised "Exercise Bukkesprang", Norway's largest and cross-sectoral "live fire" exercise in digital incident management. In collaboration with the Norwegian Cyber Defence Force (Cyberforsvaret) and the Norwegian National Security Authority (NSM), Telenor gathers Norway participants from key players in the public civilian, military and private sectors at Fornebu, where we practice in dedicated infrastructure with technical traces of simulated threat actors of a highly realistic nature. During a week-long exercise, we gain experience, knowledge exchange and networking across sectors. The overall objective of the exercise is to strengthen the total defence of Norway. The exercise is unique in a Norwegian context, and an important contribution to total digital preparedness.

» with emergency preparedness responsibility in a better position to understand events in context and to capture the totality of hybrid operations. Exercises are also a good arena for building knowledge of each other's capabilities and working methods, as well as developing networks and relationships between key personnel at critical emergency preparedness actors.

Information sharing and platform for collaboration
Strengthened cooperation between the Norwegian security authorities, the Armed Forces, the police and other natural partners in the civilian sector is crucial for achieving more robust and safe emergency preparedness cooperation in Norway. Cooperation today lacks certain basic input factors and is too fragmented. In some areas, it is still more voluntary than binding.

Among other things, businesses do not have sufficient access to up-to-date threat and security information. In addition, many enterprises, as highlighted in NSM's advisory report A Resilient Norway (Sikkerhetsfaglig råd 2023), lack solutions for classified interaction. This is particularly serious when it comes to businesses that are part of Total Defence.

A particular challenge is that there are currently no commercial data centres or public cloud platforms adapted for enterprises subject to the Security Act. An increasing number of enterprises will have a need for cloud platforms and data centres for designated systems processing information worthy of protection (skjermingsverdig informasjon). It is therefore important that the authorities in various relevant processes, such as choice of concept for a national cloud solution (Nasjonal sky) or regulation of data centres, contribute to this goal being realised.

Data centres and cloud services for sensitive information, functions and infrastructure of importance to national security interests should be established in Norway. Computing power must be secured through distributed cloud services in regional and local data centres in Norway and contingency agreements with close allies in the event of a crisis.
from – A Resilient Norway (Sikkerhetsfaglig råd 2023), National Security Authority 2023

Harmonised security legislation
Telenor noted that the Norwegian Government has submitted a proposal for a law on cyber security, and that key objectives of this are to hold businesses accountable, ensure implementation of national advice and recommendations, and facilitate the introduction of the EU's Network and Information Security or NIS Directive. Telenor's position is that the more providers of socially important services in key areas are obliged to implement security measures and warn of serious digital incidents, the more resilient our open and digital society becomes. This can contribute to a better coordinated response across sectors.

Competence and industry cooperation
Telenor is experiencing an increasing challenge with access to expertise in the technology and security field. There is a large deficit of such specialist expertise in Norway today. Not least, we experience challenges in the availability of personnel with the right security clearance. We believe that closer Nordic cooperation on this issue is necessary. Closer coordination will make it possible for more efficient utilisation of the competence base in public and private enterprises across Nordic countries.

In addition to national measures such as increased educational capacity in relevant disciplines, Telenor believes there is a need to strengthen the overall work of facilitating better technology utilisation and industrial cooperation. It provides an opportunity to draw on the technological knowledge that Norwegian, Nordic and international industry and business have to offer.

Telecom is an international industry with multinational suppliers, and from the supplier side, priority will generally be given to markets of a certain size. Nordic cooperation, with a more harmonised approach to security legislation and clearance processes, could contribute to growing to the necessary scale. Doing so might entice multinational technology suppliers to establish centres of expertise in the Nordic region. In addition to contributing to the region's digital resilience, this could also strengthen Nordic competitiveness.

A security policy foundation
Close technical cooperation between companies and organisations across national borders requires a security policy foundation. This entails harmonisation of security legislation and cooperation between national regulators at a completely different level than what we see today. With increasing pressure on talent and expertise, and concentration of the supplier market with ever longer supply chains, the individual Nordic countries are by themselves too small. Closer security cooperation across the Nordic region will enable us to realise completely different conditions for effective, secure and robust total defence.

There is a need for closer Nordic cooperation on security, resilience and emergency preparedness. A more harmonised legislation allowing the sharing of technical solutions and infrastructure across the Nordic region is necessary. Security is best built together. //

Telenor’s ask to government is to strengthen security cooperation:

- On the clearance and authorisation of Nordic nationals with a common Nordic regimen for security clearance
- To operationalise requirements for national autonomy to enable cross-border use of personnel and to share technical solutions and infrastructure for increased robustness and resilience
- To quickly establish better solutions for classified interaction and provide better access to threat and security information for selected enterprises
- To better safeguard emergency preparedness and national security requirements in public procurement

Telenor

Snarøyveien 30
N-1360 Fornebu
Norway

www.telenor.no

Read the report online:

https://www.telenor.com/about/our-companies/nordics/digitalsecurity/2023/

telenor