

NO 1 2023

# DIALOGUE

A JOURNAL FROM THE PETROLEUM SAFETY AUTHORITY NORWAY



**SECURITY**  
IN UNCERTAIN TIMES



## BE ALERT

The front cover and several of the full-page illustrations in this issue have been created by an image generator utilising artificial intelligence (AI).

Image generators, text robots and virtual “friends” have suddenly become common property on the web, a development which amazes, astonishes and annoys – and creates a certain unease.

In a survey for the Norwegian Communications Agency this April, 43 per cent of respondents expressed concern or great concern about the way the future is being shaped by AI. Another 25 per cent were not bothered at all.

You probably don’t need a technical education to spot factual errors either on this issue’s cover or in the other images which AI has generated for us.

A difference has always existed between human and artificial intelligence. But progress is rapid and a close eye needs to be kept on the technology, who is using it, and how it gets used.

Being alert is also a key requirement with societal safety and security, which are the themes in this issue.

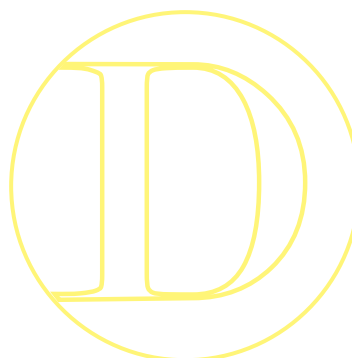
Russia’s invasion of Ukraine in 2022 has focused increased attention on threats facing the petroleum sector, energy security in Europe and the importance of safe operation on the NCS.

It has also heightened awareness of societal safety and security, which the PSA has long been working with. That responsibility nevertheless feels even weightier now.

This issue aims to explain what’s involved in these areas, identify some important as well as highly topical dilemmas and challenges, and provide some good advice.

### READ AND REFLECT!

Øyvind Midttun,  
Editor



## CONTENTS

---

Secure relationships	4
Facts: The PSA's role	9
Societal safety in a new era	10
Facts: Security Act	15
Threats to the petroleum sector	16
Facts: NSM, PST and NIS	21
Coping in troubled times	22
Facts: Guide to mental health	29
Tackling the threats	30
Calm under pressure	34
Standing firm against a storm	36
Facts: Increased infrastructure surveillance	41
Praise for oil and gas sector	42
Ransomware taught key lessons	44
Facts: Strengthened ICT security	50

A person wearing a full-body orange protective suit, a helmet with night vision goggles, and gloves is walking away from the camera on a wet, reflective street at night. The street is illuminated by bright, out-of-focus lights in the background, creating a hazy, atmospheric effect. The person's reflection is visible on the wet pavement.

BY EILEEN BRUNDTLAND

# SECURE RELATIONSHIPS





**Integrated risk understanding and strong barrier management are the basis for good safety and security in uncertain times, says Finn Carlsen, director of professional competence at the PSA.**

**T**he war in Ukraine is having serious consequences for energy supplies in Europe, and gas deliveries from Norway are more important than ever.

With the threat level changed for a long time to come, both industry and government must adapt their measures and priorities to a new reality.

This is part of the background for the PSA's main issue in 2023 – *For safe and stable energy progress – collectively and concurrently.*

It is important for the PSA that safety, including security against deliberate attacks, is taken care of in every phase of the petroleum industry, and that today's qualities and experience are maintained and adapted to the new energy industry.



As the supervisory authority, the PSA plays a key role in petroleum-industry safety. That responsibility also extends to security – including for ICT. (Illustration: Midjourney)

## KEY ROLE

The PSA plays a key role in the petroleum sector as the supervisory authority for safety. Its responsibilities also extend to physical and ICT security.

“So far, the industry has done a very good job with safety and security,” observes Carlsen.

He emphasises that an integrated approach must be taken to the risk picture in order for Norway to remain a stable gas supplier to Europe.

“The companies must view safety and security collectively. Maintenance work and turnarounds have to be implemented as planned.

“At the same time, they must have sufficient capacity and expertise to deal with unexpected events, including both unintended incidents and deliberate attacks.

“Last year’s drone sightings provide an

example of how the security picture can change quickly, and how we as an industry must be prepared for that.”

## BARRIERS

Carlsen gives particular emphasis to barrier systems, developed over a long time by Norway’s petroleum sector, as an important basis for risk management.

“The knowledge and capacity built up by the companies in terms of strengthening and maintaining barriers also contribute to work on security against deliberate attacks,” he says.

“That applies particularly to ICT security, which is attracting great attention both from the government and in the industry.

“We’re particularly concerned to ensure that industrial control systems are well-protected – that barriers around them are robust and tailored to the threat picture.”

## CENTRAL

He emphasises that employees also play a key role in security work. That became highly relevant last autumn, when employees on offshore facilities and at land plants contributed to good reporting of drone observations.

“Alert personnel are also extremely important in such issues as cyber security and access control,” Carlsen points out.

“The level of security in the petroleum industry is defined both by company systems and by the contribution of each individual. Companies must therefore continue to prioritise relevant and timely information to their own workers.”

## SHARING

Carlsen gives great weight to the sharing of information between companies, between employers and employees, between various government agencies

and between agencies and companies.

“The threat picture must be described, communicated and understood as the basis for establishing and tailoring measures.

“Collaboration between all the parties involved is crucial for preventing and containing deliberate attacks.” ★



Finn Carlsen, director of professional competence, PSA.  
(Photo: Anne Lise Norheim)



**FACTS:**







# THE PSA'S ROLE

A brief overview of the role played by the PSA in relation to societal safety, security and total defence in Norway is provided below.

## **SOCIETAL SAFETY**

Societal safety is concerned with society's ability to defend itself against and deal with incidents which threaten basic values and functions, and threaten life and health.

Such incidents could be unleashed by natural events, result from technical or human errors, or be a consequence of deliberate attacks – including cyber assaults.

The PSA is responsible for societal safety in the petroleum sector. That relates particularly to contributing to an understanding of the position and the risk picture.

## **SECURITY**

The PSA has the authority to conduct system-oriented and risk-based supervision of security. Audits of offshore facilities and onshore plants have been the key activity in this respect.

Offshore audits include the logistical chains for personnel and materials through heliports and supply bases.

Section 9-3 of the Petroleum Act requires licensees to initiate and maintain security measures to help avoid deliberate attacks on facilities and to have contingency plans at all times for dealing with such assaults.

The main issues addressed by the PSA's security audits involve technical, organisational and operational barriers (various types of security measures), security risk analyses and plans, governing documentation, expertise, and verification of the measures described.

Security work by the authority also involves close contact with other relevant government agencies, companies and employers/employees in the industry.

## **TOTAL DEFENCE**

In addition, the PSA contributes to Norway's total defence – a collective term for overall military and civilian preparedness in Norway. This incorporates mutual support and collaboration between the armed forces and civil society over prevention, preparedness planning and operational conditions.

Total defence aims to ensure that society can maintain a functioning national crisis leadership in all types of crises, deal with large numbers of injured people, secure supplies of food, water and energy, and maintain communication and transport systems.

BY ØVIND MIDTTUN

# Societal safety in a new era

## How society should best be organised to protect individuals and shared values is an issue which cuts across both science and politics – and one full of major dilemmas.

**A**fter the Berlin Wall fell and the Soviet Union collapsed in 1989-1991, the world appeared from a Norwegian perspective to be a fairly peaceful place.

Defence preparations were downgraded in relation to civil preparedness, and Norway rethought “old-style” security and safety work from the Cold War era.

Society nevertheless remained vulnerable, as shown by a number of incidents like as the New Year hurricane which struck western Norway in 1992 and the big east Norwegian floods in 1995.

Combined with ever-growing technological complexity, such events made it clear that the country was inadequately organised to cope with accidents and disasters. More needed to be learnt about meeting innate threats to civil society.

### **VULNERABILITY**

The concept of societal safety made its full entry to the public discourse through the findings of the vulnerability commission, published as Norwegian Official Reports (NOU) 2000:24.

Chaired by former prime minister Kåre Willoch, this study addressed ways of strengthening society's safety and emergency preparedness.

“Societal safety was originally a political term which needed to be given scientific content,” comments Professor Ole Andreas Hegland Engen in the department of safety, economics and planning at the University of Stavanger (UiS).

“Initially, it addressed the way safety and emergency preparedness should be organised when attention was concentrated on society's innate threats rather than state security.

“This meant achieving a more societal perspective on the risks faced – natural disasters, the climate and the environment –

with the technological dimension at centre stage.”

Engen notes that people had talked about total preparedness and such issues earlier, but that “societal safety” raised this discussion to a more administrative level.

A 2001 White Paper following the vulnerability commission's report defined the term as “society's ability to maintain important social functions and protect the life, health and basic needs of citizens under different types of stresses”.

Since then, this definition of the concept and its content have been adjusted and expanded in several stages under the impact of incidents such as accidents, disasters and attacks.

Societal security has thereby been extended to include aspects like security and terrorism – in other words, society's ability to protect itself against deliberate malicious assaults.

At the same time, it now encompasses the vulnerabilities created by technology, critical infrastructure and changes to climate and the environment.

The latest definition of the term is to be found in a White Paper on societal safety in an uncertain world, which was presented to the Storting (parliament) in 2020.

This says the concept is about: “society's ability to protect itself against and deal with incidents which threaten fundamental values and functions, and put life and health at risk. Such incidents can be triggered by natural forces, by technical or human errors, or by deliberate acts.”

### **DISCIPLINE**

The UiS has been a trendsetter in developing societal safety as an academic discipline, establishing study programmes from an early stage



and contributing to extensive learning.

“When this subject was established in the early 2000s, it was natural to draw on developments in industrial safety,” Engen says.

“That related primarily to the petroleum industry, with its knowledge of managing risk and technical safety, and not least the experience gained from the Norwegian regulatory model – which the PSA, of course, forms part of.

“This model differs from approaches taken in many other countries, including its emphasis on managing safety in the context of industrial democracy. Collaboration between employers and employees and mutual trust are important dimensions here.”

This way of thinking has undoubtedly affected societal safety in Norway, Engen says, with performance-based regulations, internal control, the individual responsibility of companies and the risk management principles as important elements.

“The question then, of course, is whether we can call this a separate discipline at all,” he points out. “Risk has long been a subject, with its own methods and theoretical basis, but societal safety still has a multidisciplinary character.

“That includes a dose of political science, a dash of sociology and a dollop of organisation theory. But we’re working to weld these together.”

## BALANCED

The benefits of a high level of security and good emergency preparedness always need to be balanced against other advantages and values.

In a 2021 book about perspectives on societal safety, Engen and his co-authors from the UiS highlight a number of dilemmas, paradoxes and challenges which can arise when seeking to make society safer.

These need to be given greater attention, they believe, with the balance between freedom and security as perhaps the most important of many issues.

“When the state takes responsibility for safeguarding citizens, it’s usually at the expense of

personal freedoms,” Engen notes, and says some of these rights are dropped to give people security.

“The state organises society in such a way that the freedoms and rights of its inhabitants are coordinated, restricted and managed.”

This is a classic discussion, he says, which also goes right to the heart of current problems related to security and protection against deliberate attacks.

“Every time we enter a period where security and security issues are put on the agenda, that discussion re-emerges to a greater or lesser extent and in differing contexts.

“Whenever a threat to society arises, the government will face the challenge that measures which might be needed to protect people don’t necessarily accord with the democratic values we like to expound.

“It’s clear that personal privacy, surveillance, possible controls on our online activities, and data storage – in other words, all the issues we discuss in connection with societal safety – will always be associated with such dilemmas.”

Introducing Norway’s Security Act and identifying objects worth safeguarding confront Norwegians with this type of problem – where the measures adopted can affect freedom of action.

## EXPANDING

“That brings us to what’s often called ‘securitisation,’” says Engen. “In other words, the authorities use security as an argument for extending their powers or passing laws.”

Value-laden terms such as “societal safety”, “security” and “safeguarding” both are or can be deployed politically to achieve specific goals, he notes.

“In political discussion, security- and value-related aspects may be weighty arguments for pushing other considerations aside. But actions always have consequences, and securitisation presents us with dilemmas. You can’t get away from that.”

## INTEGRATED

Societal safety encompasses both “safety” and “security”. Although conflicts exist between these two areas, Engen believes it is important to think and work with them in an integrated way.

While safety is about preventing mishaps and accidents which occur in legal activities, security deals with foiling deliberate attacks.

“A clear conflict between security and safety is presented by the transparency principle,” Engen says. “We can’t talk openly about the one in the same way we can with the other. The information flow has to be different.

“And the other key dimension is that when we protect ourselves in a security context, we’re safeguarding against a potentially willed and malicious action.”

By contrast, he observes, the issue in the safety area is to be organised in the best possible way to reduce risk. But interfaces do exist, of course.

“Safety can influence security. If the safety systems aren’t good enough, the way can be opened to malicious activity. So safety and security personnel must collaborate.

“These two areas traditionally involve different environments, professional traditions, risk thinking, legal frameworks and logics. But they must be harmonised to function optimally.”

## CHALLENGE

More extensive security measures also challenge the collaboration between employers, unions and government which has traditionally been very important in Norway’s industrial relations, Engen notes.

“What happens to that partnership when unions, for example, are no longer consulted over new security laws because the discussions involved are confidential? Some very fundamental traditions are being challenged here.”



Professor Ole Andreas Hegland Engen, UiS.  
(Photo: Marie von Krogh)

## CHANGED

Societal safety was developed at a fairly peaceful time from Norway’s viewpoint. That has now changed. Engen believes the subject is bound to find its place in a discussion which is inevitable in Norwegian society, where security issues will be a stronger element.

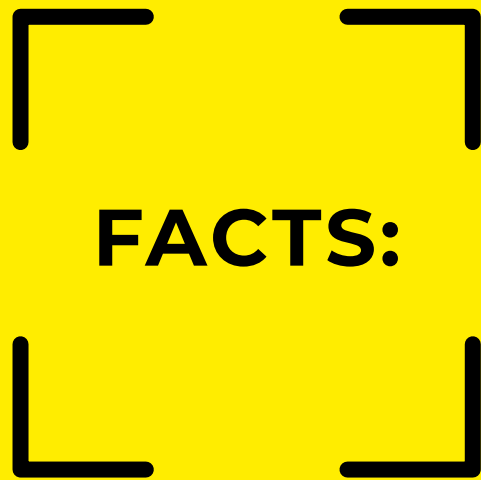
“We now face a new type of threat in the light of Putin’s Russia and what might follow,” he says. “We also face hybrid technological threats, and a climate crisis which will escalate.

“Climate, digitalisation and a new security policy position are aspects which societal safety must take seriously in a good and constructive way.

“Development of this discipline must also be clarified in relation to issues of state security – in other words, its operational, military and territorial components.

“How are we going to look after overall emergency preparedness while simultaneously maintaining our defence capability? That question actually unites state security with societal safety.” ★

*Sources: Engen et al (2021). Perspektiver på samfunnssikkerhet (2nd edn), Oslo, Cappelen Damm Akademisk.*



**FACTS:**



# SECURITY ACT

The purpose of the Norwegian Security Act is to help prevent, uncover and counter threats in the form of actions which could directly or indirectly harm national security interests.

This legislation builds on a risk-based approach and requires that undertakings subject to its provisions continuously assess the risk their assets are exposed to, and that the necessary measures are taken to achieve a satisfactory level of security.

Threats to Norwegian national security interests take various forms. The collective term employed in the Act is activities which threaten security.

Examples of these activities include intelligence-gathering by foreign states, sabotage, terrorism, serious crime which can harm national security interests, or preparations for such deeds.


This also encompasses insiders who, directly or indirectly, consciously or unconsciously, assist the success of such activities.

Work is under way to assess the extent to which parts of the petroleum industry should be classified as basic national functions and become subject to the Security Act.



BY ØYVIND MIDTTUN

# Threats to the petroleum sector



The annual threat and risk assessments from the Norwegian Intelligence Service (NIS), the Norwegian Police Security Service (PST) and the Norwegian National Security Authority (NSM) for 2023 all cover conditions relevant for Norway's petroleum activities.



Illustration: Midjourney

Information and assessments on foreign, security and defence policy are provided by the NIS to support Norway's civilian authorities.

Its *Focus 2023* report analyses the status of and expected developments in thematic and geographical areas which the service considers particularly relevant for Norwegian security and national interests. Topics covered include Russia, China, international terrorism and conflict areas.

Combined with the National Threat Assessment 2023 from the PST, the NIS report describes national and international conditions which influence the threat picture.

The PST's assessment concentrates on the intelligence threat, with particular emphasis on Russian and Chinese espionage. It also describes politically motivated violence – extremism and threats to people in authority.

Intelligence work can be pursued in a variety of ways, including network operations, recruitment of sources, and digital and physical sabotage.

Risk assessments and safety measures must be updated in line with changes to the hazards. The war in Ukraine has demonstrated that Norway has to be prepared for a broad range of threats.

## CYBER VULNERABILITIES

In its *Risk 2023* report, the NSM calls attention to how the petroleum sector should reduce vulnerabilities to make the job of threat agents more difficult.

Phishing attacks will still be the simplest and most widely used method for obtaining access to information about a person or an enterprise.

The NSM is constantly seeing human, technological and organisational vulnera-

bilities being exploited to assist malicious cyber operations directed at a number of Norwegian enterprises.

Digital threat agents also exploit such vulnerabilities as weak passwords, outdated software and lack of two-factor authentication to secure unlawful access to ICT systems.

Such attacks are not always aimed directly at networks belonging to enterprises. Individuals and third-party services on which enterprises depend may be exploited because they are regarded as easier to assault than the actual targets.

## INSIDER RISK

The Norwegian security services are devoting much attention to insider risk, which can arise at any point in an insider's period of employment.

This means background checks or security declarations are not an adequate means of avoiding such risk. These issues are dealt with in more detail in the PSA's report on managing insider risk (*Håndtering av innsiderisiko* - in Norwegian only).

Good situation and threat pictures at sectoral and national levels depend on a functioning chain which extends from alertness by the individual through reporting systems at companies to filing reports with the authorities.

Routines at enterprises for internal notification, combined with a system for onward reporting to the PSA, the power sector's computer emergency response team (KraftCERT), the PST or the NSM, make it easier for employees to report.

The PSA has entered into an agreement with KraftCERT, which discharges the operational role as the sectoral response team for the petroleum sector and receives reports of all cyber incidents in the industry. ★

### **WHAT MUST BE REPORTED?**

Suspicion of, attempts at or successful security incidents, both digital and physical.

### **WHAT MUST BE NOTIFIED TO THE PSA?**

Section 29 of the management regulations specifies the requirements for notifying and reporting hazards and accidents. These also apply to cyber and security incidents. The notification/reporting form can be found at <https://hendelser.ptil.no/?language=engelsk>.

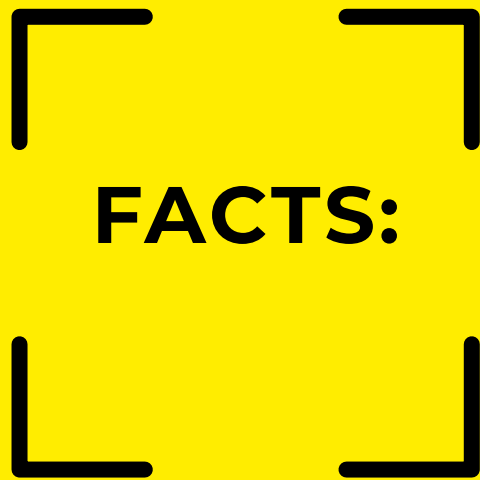
### **HOW CAN OTHER GOVERNMENT AGENCIES BE NOTIFIED?**

Cyber incidents: [cert@kraftcert.no](mailto:cert@kraftcert.no)

Activities and incidents which represent a security threat: [varsel@nsm.no](mailto:varsel@nsm.no) or the PST website at [www.pst.no/tips-oss](http://www.pst.no/tips-oss)  
It should be made clear whether the notification is a tip-off, accusation or request for assistance.

### **ADVICE AND GUIDANCE**

Get in touch with the business contacts in the relevant police district:  
<https://www.politiet.no/kontakt-politiet/naringslivskontakter/>  
(in Norwegian only)





## Norwegian National Security Authority (NSM)

The NSM is Norway's directorate for preventive national security. It gives advice on and carries out audits and other checks on both civilian and military sides related to the security of information, systems, objects and infrastructure of national significance.

A national responsibility for identifying serious cyber operations, warning about them and coordinating responses also rests with the NSM.

Through its annual Risk report, it presents its updated assessment of the risk picture for national security. This evaluates how vulnerabilities in Norwegian undertakings and social functions influence the risk picture in light of the threat picture described by the NIS and the PST.

The report also recommends measures for reducing the risk associated with activities regarded as a security threat.

## Norwegian Police Security Service (PST)

The PST is Norway's national domestic intelligence and security service, and is subordinate to the Ministry of Justice and Public Security. Its job is to prevent and investigate serious criminality directed against national security.

It identifies and assesses threats related to espionage, sabotage, the proliferation of weapons of mass destruction, terrorism and extremism. Its assessments contribute to shaping policy and supporting political decision processes.

The PST's annual threat assessment is part of its unclassified societal communication, where it reports on the expected development of the threat picture.

## Norwegian Intelligence Service (NIS)

The NIS is Norway's foreign intelligence agency. It reports to the Chief of Defence Norway, but covers both civilian and military matters.

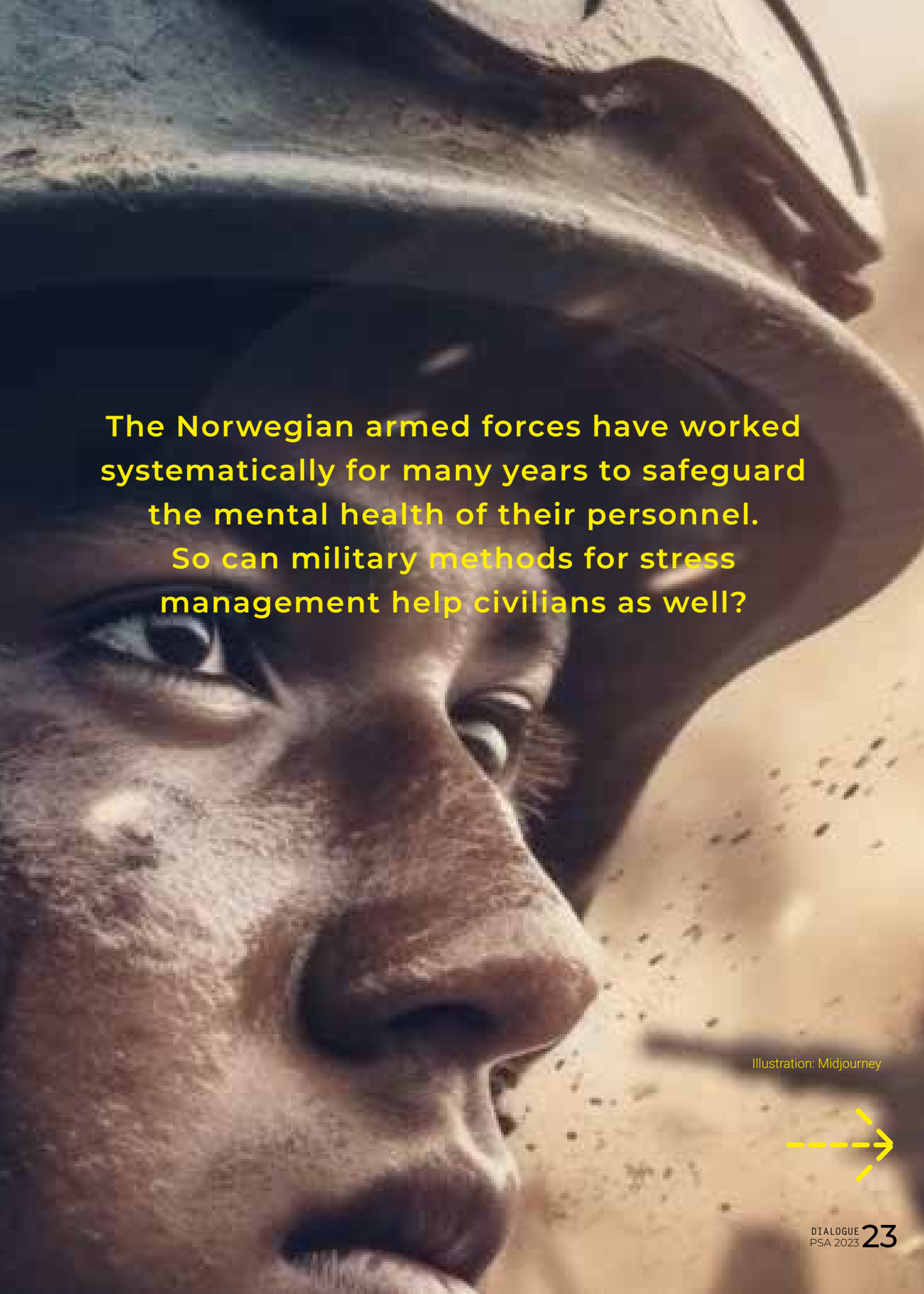
Its main job is to warn of external threats to Norway and priority Norwegian interests, support the armed forces and the defence alliances the country belongs to, and assist political decision processes with information of special interest for Norwegian foreign, security and defence policies.

In its annual Focus assessment, the NIS provides its analysis of the current position and expected developments in thematic and geographical areas which it considers particularly relevant for Norway's security and national interests.



BY EILEEN BRUNDTLAND

# COPING IN TROUBLED TIMES



**The Norwegian armed forces have worked systematically for many years to safeguard the mental health of their personnel.**  
**So can military methods for stress management help civilians as well?**

Illustration: Midjourney



**C**ommander Jon Fauskanger Bjåstad, a clinical psychologist, knows a lot about how uncertain times affect people mentally and what they need to do when war and crises dominate the news.

Employed by the institute of military psychiatry in the Norwegian Armed Forces Joint Medical Service, he works out of a building at Stavanger's Madlaleiren naval base with a simple red cross over the door.

Bjåstad and his colleagues in the institute produced a mental health guide for Norwegian troops soon after Russia invaded Ukraine in February 2022. This was based on the principles



Clinical psychologist Jon Fauskanger Bjåstad.  
(Photo: Gunlaug Leirvik)

for managing stress in the various operations of the armed forces.

"Put briefly, it's about being aware of how you're consuming news stories and reminding yourself that you're doing an important job," he says.

"You also have to learn to recognise how your thoughts affect your feelings, and make sure

that you draw on your social support network." And the guide then advises the reader to seek help if they need it.

"When we published this, we didn't know how worried people were or how the war would develop," Bjåstad observes. "And it remains relevant now, so we're still referring to it. None of the ideas are new, but we know the advice works."

### ACCEPTABLE

Asked what is important in managing to keep stress at an acceptable level, he identifies two key aspects – individual measures and action at the system level.

"In the first case, the individual learns how to cope with stress. The other concentrates on the working environment and a culture of openness.

"We know that a good working environment, good managers, a functioning health services and structures like a buddy system have a preventive effect."

Having someone you can turn to with your concerns is important, Bjåstad observes. "We also know that pressure builds up if you have worries at home while on assignment. Such cumulative stress is an important factor when things get too much."

He draws parallels here with the petroleum sector. "Offshore workers are also away from their family frequently and for long periods, live cheek by jowl with others, have limited freedom of movement – and therefore depend on a good working environment."

### DIALOGUE

So a good and open dialogue plays a key role in identifying whether people are worried, Bjåstad says. Conducting a survey might then make sense.

"Perhaps job reviews should include a question on how the employee assesses the risks of their job? Even though most people may not be particularly worried, it could be necessary to identify the group who're not sharing their anxiety and stress."

He has long experience of visiting troops on foreign postings. Everyone there is called in for mandatory psychological reviews, where the threshold for talking about difficulties is lowered.

"We don't ask those with problems to put up their hand," Bjåstad says. "We talk with everyone. That systematises things and creates a relationship which makes it easier for people to return later if they feel the need."

"The same type of follow-up discussions are also held when the troops are on their way home, in addition to another talk a year later."

## FEARFUL

He finds it understandable that many people have felt more fearful since the Ukraine war began. At the same time, it is important to tell yourself that Norway faces no direct threat today.

"We humans differ in the way we perceive risk," Bjåstad notes. "Some of us are more at the mercy of our feelings than others. Emotional risk assessment is much quicker than applying logic and probability."

"Feelings stirred up by circumstances are prioritised first, while cold reasoning comes into play later. That's something to think about these days, when we're constantly surrounded by media images which trigger the emotion-driven brain."

An important piece of advice therefore deals with facts and how people should read and relate to information coming from different media sources.

"I think it's sensible to be conscious of where and when we read the news, because we can be overwhelmed by sensory impressions and their quantity."

"We humans are designed so that our brains seek out threats and risk. So it can be useful to stop checking the news as soon as you get up and just before going to bed, when your mental defences are a little weaker than if you're fully awake."

## VIGILANCE

Striking a balance between increasing your vigilance while staying calm can also be demanding.

"We want troops who're out on an operation to be wound up. They must be alert to possible threats," says Bjåstad. "They're trained and drilled in that."

"At the same time, we're concerned to ensure that they wind down once they're home. That's important for avoiding problems like post-traumatic stress symptoms."

This division between alertness and relaxation is equally important in other sectors, he notes.

"If you're constantly on edge, you'll eventually reach a point where alertness imposes such a strong stress reaction that you no longer function. Then you're not paying adequate attention to security."

## WORRYING

A number of techniques are available for reducing stress. Learning to recognise when you are sapping energy through unnecessary worrying is crucial.

That is when good habits are important – such as starting an activity or allocating time to worry



at the end of the day. Stress can easily become embedded in the body, so such things as learning breathing techniques or relaxation exercises can be useful.

“And it’s important to remember that not all stress is bad. After all, we generally need a bit of it in order to get ourselves moving.”

Reminding yourself about the meaningful aspects of your job also makes sense. Norway’s oil industry, for example, has a more important role than ever in ensuring energy supplies and welfare for Europeans.

“When we’re involved in something that gives meaning to our lives, we can cope with a higher level of uncertainty,” Bjåstad observes.

## **NORMAL**

Good information also has an important function. The Norwegian armed forces devote a lot of work to preparing their troops for dealing with reactions which they should regard as normal.

“When they’ve been told how they may respond in different circumstances, soldiers become less concerned about what we consider

‘normal’ behaviour,” Bjåstad explains.

“We often conduct group conversations on this subject, because people can easily get worried about their reactions. That’s why knowing what’s normal is important – it teaches people there’s a wide range of ways to respond.

“A number of different reactions are normal after you’ve been in a tight spot. Knowing that this applies to you and others is perhaps easier to accept than thinking you’re the only one.

“That’s how information can assist in reducing stress, because it helps you to appreciate that others also share the same responses – and that it’s normal.” ★

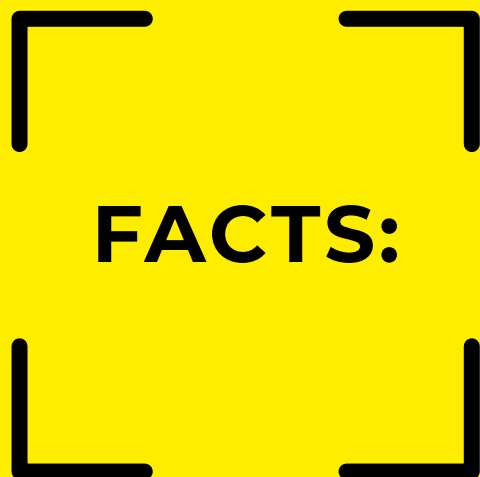
*Go to page 29 for  
an extract from the  
armed forces guide to  
mental health.*







Striking a balance between being more vigilant and keeping calm can be demanding. But it is nevertheless important, not only in the armed forces but also in other sectors. (Illustration: Midjourney)



**FACTS:**



## **Extract from the guide for service personnel produced by Commander Bjåstad and colleagues for the Norwegian armed forces.**

### **The war in Ukraine is making an impression on all of us. What's sensible to do at this time to protect your own mental health?**

The war now under way in Ukraine is exposing all of us to news about and images of hostile action hurting innocent people. Some may feel more worried, and others not. Both responses are normal. A number of things could be sensible to do in order to protect your own mental health in such circumstances.

Stick to the facts. We all have a need for information, and that's understandable. But try to be critical of sources (particularly on social media) when keeping informed about the war. Generally use large news channels such as public broadcaster NRK and sources like Forsvaret.no (the armed forces website).

Preferably limit how often you read news stories to a few times during the day and avoid this activity at bedtime or when you wake up. Maintain sound "screen hygiene" by taking good breaks from watching.

Some people using social media as a news source – which could involve exposure to a lot of video material, for example – may experience more distress than when relying on traditional media, which are subject to editing and fact-checking.

Although Norway does not face a direct military threat, media exposure could contribute to some Norwegians overestimating the threat picture for us and cause unnecessary concern. People should stick to information based on facts rather than rumour. Remember that we have our own personnel in the armed forces who assess the security position in Norway and give us good information.

Remember that you do an important job. The armed forces have an important role to play in ensuring security for our country and our population, where you


represent a significant part and function. That part is important even in circumstances where the threat to Norway has not been increased.

Assess your own thoughts. We all conduct a continuous "internal conversation" with ourselves through our thoughts. Our brain is created to protect us, so it's therefore normal that it concentrates attention on possible threats. Appreciating that we might have a tendency to exaggerate the probability of something dangerous happening while simultaneously underestimating our own ability to cope, could be important. So try to evaluate how likely what you're thinking is. The way we view the Ukraine war could influence our feelings, our physical reactions and our actions. Subjecting our own thoughts to a conscious assessment may have a positive effect on our feelings. If you're very worried, it could be useful to read more about some helpful techniques which we've listed in a separate document.

Keep in touch with your social contacts. Social relationships give us opportunities for fellowship, where we can share our thoughts and ways of dealing with things. Go on doing your usual leisure activities and maintain social contacts with others. Do something nice for other people and help to give them a feeling of fellowship.

Seek help if you need it – don't sit on your own with big worries. Anxiety is a normal and natural reaction to uncertainty. But if you experience troublesome reactions which get in the way of your daily life/service performance, it's important to seek help. This can be found in the civilian sphere, through your superior officer or directly through a military hospital.

Source: The Norwegian Armed Forces



BY EILEEN BRUNDTLAND

# Tackling the threats



## Norway's position as a gas supplier to Europe gives safety and security a special place. And Jannicke Nilsson's job in Equinor has never been more important.

**A**s the group's executive vice president for safety, security and sustainability (SSU), she works closely with today's demanding threat picture.

"The inhuman conditions we encounter via the news from Ukraine naturally affects me both as a human being and as a manager with my area of responsibility," Nilsson comments.

The war in Ukraine has had serious consequences for energy supply in Europe, where Norway was the clear leader for natural gas deliveries during 2022. This has increased the security policy value of Norwegian petroleum activities, and the demands Equinor faces as the largest producer in that industry.

"This conflict is very serious and dramatic. At the same time, it underlines the significance of Equinor as a reliable supplier of energy to Europe."

### INCREASED THREAT

In March 2022, soon after Russia invaded its neighbour, the Norwegian Police Security Service (PST) sounded the alarm over an increased threat to Norway's petroleum sector. And blowing up two Baltic gas pipelines brought the war even closer.

"The sabotage of the Nord Stream pipelines showed how far somebody was willing to go," says Nilsson. "It underlined the seriousness of the position and that the need to take action has become even greater."

Threat assessments by the Norwegian security authorities provide an important basis for Equinor's security work, she makes clear.



The security-policy value of Norway's petroleum industry is growing – but that also increases the demands on Equinor as the sector's largest operator. (Illustration: Midjourney)



“We also look beyond Norway to ask such questions as what’s happening in the cyber area, where are wars being fought around the world, and where is change happening.

“Based on various information sources, we then produce our own threat evaluations. These are very important for the risk assessments which form the basis for our business.

“The gas supply chain to Europe is a highly significant part of this right now because of the value it creates.”

At the same time, Nilsson makes it clear that protecting people trumps everything – both environmental and financial value. “It must be safe to work in and for us,” she emphasises.

## EXPERIENCE

Equinor learnt a lot from its experience with the terrorist attack on Algeria’s In Amenas gas field in 2013, when 40 people were killed – including five of its own employees.

In the wake of that incident, the group’s security work was reviewed both internally and externally, and a number of measures were implemented.

These included promoting security to the corporate management level and dividing it into three areas – physical, ICT and personnel.

“A lot’s happened since In Amenas,” reports Nilsson. “We’ve adopted a far more integrated approach to security work, where we now see these three areas merging to a greater extent.

“At the same time, our work is risk-based. We make our biggest commitment where we believe the threat to be greatest. Deliberate attacks, for example, were defined as one of the principal risks for us as a company long before the Ukraine war.”

This risk-based approach is inherited from many decades of systematic safety work in the group, and Nilsson sees a number of benefits deriving from the experiences this has provided.

“Transferring lessons learnt from safety to security is relatively simple, and we apply

many of the same principles in both areas,” she observes.

“The bulk of our work is devoted to what we can do before something happens. In addition, we have good plans for when a response is needed.

“That’s particularly important now with cybersecurity, where we see a steady increase in attacks around the world. We can’t assume this will never happen to us.

“So we must be ready to do all we can to avoid an assault. At the same time, we have to know what we’re going to do if something happens.”

The group also works a lot on physical security of the subsea infrastructure on the NCS. Several thousand kilometres of pipelines, along with power, internet and communication cables, form an extensive network on the seabed.

This must be protected, and a good deal of technological development is now being pursued in this area.

## EXPANDING

However, the biggest security challenge facing Equinor is a steadily expanding attack surface, which reflects growing complexity and an expansion in the players involved.

“We’ve become a broader energy company, which means that we work with several value



Jannicke Nilsson, executive vice president for safety, security and sustainability at Equinor. (Photo: Equinor)



chains and a larger number of suppliers and sub-suppliers,” Nilsson says.

“At the same time, we’re becoming increasingly digitalised and are thereby acquiring more connections to our networks.”

She finds that all Equinor’s suppliers are working well on security, whether this involves cyber, physical or personnel risk.

“I think everyone who works in this industry is aware that we’re an exposed sector now.

“We set specific requirements for security when entering into contracts, depending on which positions and areas the supplier will be working in.

“The most important consideration is nevertheless working together and sharing information so that we build expertise collectively.”

## **INSIDER RISK**

Insider risk has been highlighted as a threat by the authorities on a number of occasions, and it has received greater attention in recent years.

“We have a trust-based culture, and aim to keep it,” Nilsson says. “At the same time, we must be conscious that players may exist who want to extract information from us as a company.

“Detailed assessments are conducted when making new appointments. However, the vast majority are already working for us. So it’s important to identify which positions here could be the most interesting for other players to access.

“We also work systematically on expertise-building among managers, so that they’re observant and can conduct clarifying conversations from an early stage.”

## **SHARING**

“Our base values — open, collaborative, caring and courageous — underpin everything we do, including how we work on security,” she adds.

“It’s important for us to be open about as much as possible, even though we naturally keep some details relating to security issues confidential.”

A great need for information has been felt over the past year, both by employees and by their next of kin.

“When the war started, we established a strategic project team to see how we could best work across the group,” Nilsson explains. “Fixed meetings with both safety delegates and unions were established to ensure information flowed as openly as possible.

“We’ve received comments about where we need to be more open and areas where we must expand the information we share. Our emphasis is on informing employees, so they have the facts to pass on to their families.”

Collaboration both internally in Equinor and with government agencies has also been strengthened over the past year.

“We’ve collaborated well with the PSA over a long time,” Nilsson says, and explains that this cooperation has now extended to the ministries, the intelligence service, the PST, the Norwegian National Security Authority (NSM), the police and the armed forces.

“It’s also important that we involve suppliers and other players, such as Gassco, so that we’re working together around the whole value chain.”

## **NEVER GOOD ENOUGH**

Nilsson is pleased that the systematic work done over a long time has equipped the group better to assess which areas are the most important to work on.

But she also points out that conditions are constantly developing. That poses big demands for new expertise both in the industry and on the authorities.

“Our most important priority is to look after those who work in and for Equinor. We must then continue to work systematically and collaborate — and not forget that what was good enough last week won’t be good enough in the next one.” ★

# CALM UNDER PRESSURE

Greater attention than ever is being given to security and safety in the Norwegian petroleum sector. Two unions have given their views on the way workers in the industry are experiencing this.

“If I’d been asked six months ago about the security position, I’d undoubtedly have said that many people feel a bit fearful about working offshore,” says Henrik Solvorn Fjeldsbø.

A national officer in the Norwegian Union of Industry and Energy Workers (IE) and a member of the Safety Forum, he relates such fears to drone observations and the Ukraine war at the time.

But conditions have grown calmer, he says, and adds that the position today is not entirely negative.

“Norway’s the biggest gas supplier to a Europe in crisis. That’s made us more conscious that we work in a special, socially useful industry.

“The political wind and popular support for maintaining the oil and gas industry have also shifted. We find many people are more positive to our industry today, and more see that the green shift isn’t simply a matter of shutting down this sector.”

## CHALLENGING

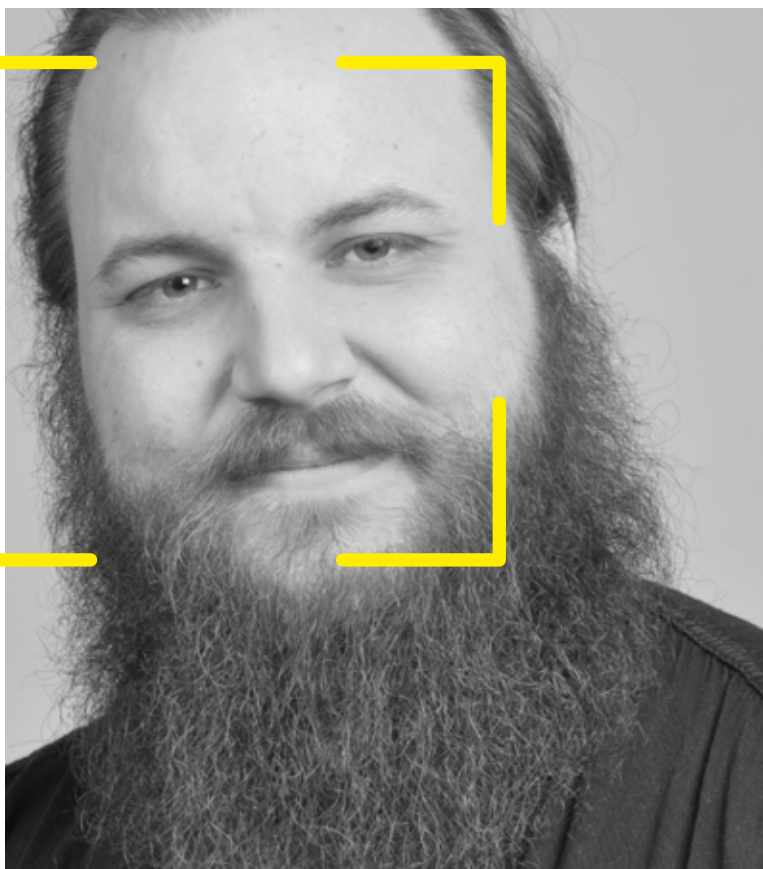
But Fjeldsbø makes it clear that needing clearance to access much of the information related to security presents a challenge to

tripartite collaboration between employers, unions and government.

He has personally experienced these parties getting input from different sources. Even when everyone has the same information, moreover, discussing it openly in joint meetings is impossible.

“We must dare to question which risks must be open, and what lessons we’re now able to draw if we can’t freely debate the challenges,” he says.

“Tripartite collaboration is based on openness, trust and dialogue, and on jointly finding the best solutions.



Henrik Solvorn Fjeldsbø,  
a national officer at IE.  
(Photo: Gunlaug Leirvik)

Peter B Sabel, one of Tekna's shop stewards. (Photo: Gunlaug Leirvik)



"When so much of the information is confidential, it restricts the way we work. We don't get all the good contributions which could have been provided."

But he admits the position is unique.

"We've never been involved in anything similar. The question therefore is what processes we now need to share more information if we later find ourselves in similar circumstances."

## THREATS

Peter B Sabel, a shop steward for the Norwegian Society of Graduate Technical and Scientific Professionals (Tekna) in Equinor and a Safety Forum member, notes that the industry has experienced threats before.

These included demonstrations and campaigns by various groups, but he admits that the position which emerged in 2022 nevertheless falls into a different category.

"Some workers undoubtedly felt uncomfortable when the land-based plants were shielded by armed personnel from the Home Guard. However, my impression is that this settled down and the extra security became part of the new normal."

In the wake of the drone incidents and the sabotage of the Nord Stream pipelines, many

questions were put by members to Tekna's shop stewards.

"The companies took the need for information seriously, and the questions rapidly tailed off," says Sabel. "Our impression is that most employees understand the need for security measures."

"Senior union officers have found there has been regular, good and open dialogue throughout the period – as open as possible, where security is concerned. We try to communicate this on to other shop stewards and our members."

## FUNCTIONED WELL

Security, particularly for ICT, has attracted much attention in the industry for a time, and Sabel feels that tripartite collaboration has functioned well.

"A Safety Forum work group on digitalisation, HSE and tripartite collaboration delivered a very good report last year, including a number of recommendations for further improvement."

"Some people are undoubtedly more affected physically and mentally by the position than others, and it's important that they're properly looked after. But our experience is that this has generally gone well."★

An underwater photograph of a large, rusted metal pipe lying on the seabed. The pipe is heavily corroded and covered in marine growth. A yellow rectangular frame highlights a section of the pipe. Sunlight filters down from the surface, creating a dramatic, blue-green atmosphere.

BY OLAV HOVE

# STANDING FIRM AGAINST A STORM

An energy crisis in Europe and gas pipeline sabotage were among the developments which meant that Linda Nordbø's first year as Gassco's head of communication was not what she had expected.



**W**hen she joined the gas pipeline operator in the autumn of 2021, Nordbø had a clear vision of how the job would contrast with many years of deadline-driven.

She took on a role which looked more family-friendly for a mother of small children, and envisaged being largely able to manage her own daily life.

It would have been difficult for her to be more wrong.

Gassco is based in Karmøy north of Stavanger, at the heart of a region which absolutely deserves to be called beautiful, but where terms such as “weather-beaten” spring easily to mind.

Nor does the company’s office building at Bygnes cry out for attention in an open landscape, where the sea and the elements create a dramatic backdrop.

“That’s actually a good picture of what we’re meant to be like,” says Randi Viksund, head of staffs and support for Gassco. “However fierce the storms outside, it’ll be calm, concentrated and relatively anonymous here.”

She was responsible for unintentionally giving Nordbø false hopes about the content and scope of her new job, emphasising that the company had always attracted little notice.

Viksund told the newcomer that she was joining a workplace where people were always left in peace to fulfil Gassco’s mandate to deliver gas stably and safely to Europe.

Then came the storm.

Russia’s invasion of Ukraine pitched Europe into an energy crisis and greatly strengthened the spotlight turned on the Norwegian petroleum industry.

“We already felt that something was brewing in late 2021,” Viksund says. “Energy-market tensions and the constant cuts in Russian gas deliveries indicated that bad weather was coming.”

## TRANSITION

Nordbø initially got off to a fine start in her new job, even though she noted rising interest in Gassco’s role as the capacity picture changed.

But it was not until the explosions on the Nord Stream 1 and 2 gas pipelines in the Baltic during September 2022 that life really became hectic for her.

The day the incident occurred, she had flown to Oslo to try on her wedding dress. “My plane had just landed when the news came, and I quickly grasped that this was serious. During the first few hours, my phone rang incessantly. I simply had to turn back.”

While Nordbø was getting to grips with the flood of calls from home and abroad, Viksund and the rest of Gassco’s senior management were concentrated on the big picture.

“My first thought was that these weren’t our pipelines,” Viksund recalls. “But, of course, we understood that this would also have substantial consequences for us.

“So we had to prioritise, and were quickly asking ourselves what was important now and what our job should be.”

It was decided that the control room which forms the heart of the company would be safeguarded. No visitors were to be allowed, and attention would concentrate on day-to-day tasks.

This facility manages gas exports through the pipelines from Norway. Many processes are required to deliver gas in the right quantities and with the correct specifications.

That calls in turn for an overview of and knowledge about the physical preconditions for gas transport in real time. Various gas streams must be blended to achieve the right quality, and the volumes available need to be known.

“It’s complex, and demands concentration and calm,” Viksund explains. “That’s why the control room had to be protected.”

The next step was to inform the employees



and help them to feel secure, she says. In a chaotic initial phase after the pipeline blasts, this became an important success criterion.

With 20 years of experience in the company, she knows its organisation well. But conditions now were entirely unfamiliar. They had admittedly drilled a lot on similar scenarios, but this was no exercise.

"In my view, we handled the first phase extremely well, and that wasn't a matter of chance," Viksund says. "We'd trained for such eventualities, and were therefore prepared."

### REASSURING

"The calm in the control room has fascinated me from the start," says Nordbø. "Seeing this remain intact after the Nord Stream incidents was reassuring. I tried to maintain the same unflappability in my meeting with the media."

Numerous and steadily increasing enquiries flooded into her four-strong communication department. Priority had to be given to calls from Norway and the markets which receive its gas.

During this initial period, Nordbø found that very many queries were about capacity – could Norwegian deliveries increase so much that the scale of the energy crisis was contained?

"The questions were pretty similar from everyone who got in touch," she says. "They received by and large the same response. We shared facts and tried to help maintain calm."

As the days passed, however, Nordbø noticed a difference between the Norwegian and foreign press.

"The foreigners were concerned with security of supply, while journalists in Norway concen-

trated on capacity and security. They asked few questions about gas."

### RESPONSIBLE

Gassco currently has just over 350 employees, and is responsible as operator for safe and efficient gas transport from the NCS. It also has an overall responsibility for operating and developing a network of pipelines more than 8 800 kilometres long.

More and more questions about this transport infrastructure and its security were eventually put to Nordbø and her department.

"We noticed that enquiries from Norwegian media shifted from capacity to security – what are we doing to safeguard the infrastructure and are our routines good enough?" she recalls.

Everyone got the same answer, which seemed reasonably well received. But she noticed that questions began to shift towards Norway's sharing culture, and whether it made sense to be so open.

"We were often asked about the maps of the pipeline systems being freely available, for example, and whether the trust-based system was perhaps too naive in emergency conditions."

### TRUST

Viksund is convinced that the Norwegian model is the reason why these circumstances were handled so well. "This reflected the openness and trust between us, the companies and the government.

"I felt on a number of occasions how privileged I was to be in such a system. Greater solidarity and pride were created when a big potential existed to increase discord and division.

"That fact that you can pick up a phone and quickly reach key personnel in the companies, either offshore or at the land plants, is incredibly important in such circumstances.

"The same applies to the government. Close contacts were maintained and conversations were always constructive."

### CONFIDENTIAL

The media also asked a number of questions which could not be answered because the details were confidential. Many wanted to



Linda Nordbø, head of communication at Gassco.  
(Photo: Morten Gjerstad)

know how the pipeline system was protected, for example. Even in such cases, Viksund says, openness was a key.

“We took the line where security was concerned that we couldn’t go into details, but that our level of preparedness had been increased, extra measures were taken, and we were collaborating closely with the companies and government.

“That response was met with understanding. Apart from the great attention they paid, the press gave us good working conditions.”

## EDUCATIONAL

Both she and Nordbø agree that the time before and after the Nord Stream incident has been challenging but educational. “First and foremost, it was good to see that we were actually rigged for this,” says Nordbø.

The high level of attention demanded a lot from the whole company, and her department had to maintain close contacts with other parts of Gassco to give sufficiently precise answers.

“It’s the same in all such organisations, of course, but we were in a position here where the external desire for information was almost insatiable,” she says. “That demanded a lot from us all, but I think we handled it well.”

Viksund is happy with the questions they asked internally during the first phase – the decision to concentrate on the core assignments, with everything else secondary.

She nevertheless believes that the commitment from all employees has been extraordinary, without creating too much in the way of wear and tear.

“We acquired a kind of enhanced sense that we all had an important job, and that a huge amount depended on us watching our step and doing our job. That gave the organisation a boost.”

## FALLEN

Well into 2023, the workload has declined somewhat for Gassco’s communication team. Fewer calls are received and, even if daily life has not quite returned to normal, Viksund believes it is heading that way.

“That’s absolutely the case. But it’s important



Randi Viksund is Gassco’s head of staffs and support.  
(Photo: Gassco)

to remember that, if you have good routines in normal circumstances, they’ll also function in a crisis.

“This, at any rate, is something we’ve learnt. And it helps that we drill often and work to visualise various scenarios.”

The level of attention devoted to Gassco has increased, and much of it has been of the right kind.

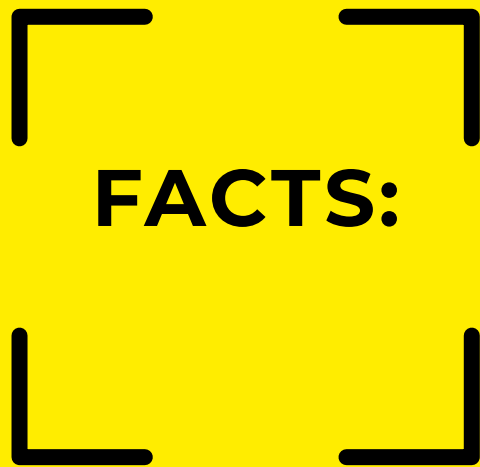
“We’ve received a lot of praise for our calm and openness,” says Viksund, and notes that this was highlighted when Gassco won the Norwegian Petroleum Society’s industry prize for 2022.

Nordbø admits that her first year in the job was not what she had expected. “We often talk about that around the kitchen table at home.

“And even if it’s not quite as busy at work any longer, I feel that Gassco is more on the radar and in people’s awareness now – for better or worse.

“On the one hand, the attention can be both time-consuming and wearying. On the other, it’s also an opportunity to tell the world who we are and what we do – that we can be relied on, and are able to stand firm against a storm.” ★

*Want to hear Linda Nordbø talk about her first year in Gassco and how daily life changed for the whole company? Listen to the PSA’s podcast Å være klar for det uventede (On being ready for the unexpected, in Norwegian only). Search for the PSA on your preferred podcast platform.*



**FACTS:**



## Increased infrastructure surveillance

Russia's invasion of Ukraine has concentrated greater attention on the threat picture for the petroleum sector, energy security in Europe and the importance of secure operation on the NCS.

Norway makes an important contribution to the current position by maintaining a high production of oil and gas through continued great regularity in the delivery chain.

The government has initiated measures to enhance preparedness related to petroleum infrastructure, land plants and facilities on the NCS, and has identified control over petroleum production on the NCS and gas transport by pipeline to Europe as basic national functions.

Following the attack on the Nord Stream 1 and 2 pipelines in the Baltic during September 2022, agreement has been reached by Nato on increased surveillance in the North Sea and a strengthening of work to protect critical infrastructure – including oil and gas pipelines.

Security for such installations has been increased across several domains. Sharing of information and intelligence has also been strengthened.

Both the government and the companies contribute to barriers which protect infrastructure and gas transport against deliberate attacks.

## Norway's gas transport system

Transport capacity in the Norwegian pipeline network is currently some 117 billion standard cubic metres (scm) of dry gas per annum.

Integrated in the system are three land plants – Kårstø, Kollsnes and Nyhamna – which receive rich gas from the fields and send on dry gas to receiving terminals abroad.

The latter include two each in Germany and the UK, one apiece in Belgium and France, and one at Nybro in Denmark which delivers gas to the Danish and Polish markets.

Most of the system is owned through the Gassled partnership, with Gassco as the neutral and independent operator.

*Source: Gassco*

BY EILEEN BRUNDTLAND

# Praise for oil and gas sector



"Don't forget that this could be a means of creating even more uncertainty," says Armed Forces head Eirik Kristoffersen. "Should any doubts arise about our ability to deliver secure energy supplies to Europe, it would also create difficulties for the European countries." (Photo: Norwegian Armed Forces)

**Eirik Kristoffersen, head of Norway's armed forces, has commended the petroleum industry for its good work on safety and security at a time when threats are greater than for many decades.**

**H**e said collaboration between the armed forces, the government and companies in the petroleum industry had been very good following Russia's invasion of Ukraine in February 2022.

"Norway's oil sector is very good at safety. This expertise can also be applied to security," Kristoffersen observed in an interview during the PSA's Top Executive Conference on 25 October 2022.

**NO DIRECT THREAT NOW**

Kristoffersen also made it clear that Norway faces no imminent threat of a military attack at present.

"The whole of Europe is more dependent on Norwegian energy and gas, and wants to escape dependence on Russian energy," he emphasised. "That means Norway is relatively much more important for Europe and thereby for Russia  
"Don't forget that this could be a means of

creating even more uncertainty. Should any doubts arise about our ability to deliver secure energy supplies to Europe, it would also create difficulties for the European countries."

**NOT NAIVE**

Kristoffersen emphasised that Norway has never been naive and unreservedly trusted Russia, but had monitored it in both intelligence and security terms.

"Putin has completely lost his status as someone we can trust – if we've ever done that," Kristoffersen observed. "But building a relationship with Russia when the war is over will nevertheless be important.

"Norway won't be finished with Russia. We're its neighbour. We have a common frontier in the far north. And we have a tradition of finding solutions for fishing and resource management."★

*See the full interview  
with Eirik Kristoffersen  
at [psa.no/forsvarssjef](https://psa.no/forsvarssjef).*

BY OLAV HOVE

# Ransomware taught key lessons





Senior managers at Hydro were awakened early on 19 March 2019 with the news that the Norwegian industrial group appeared to have been the victim of a major cyber attack. Nobody knew its scope or potential consequences, only that it was serious.



Hydro had to get out pen and paper to tell employees not to turn on their PCs. "One of the first things we did was to post a warning at our main entrance," explains Halvor Molland. "But it had to be handwritten, because nobody could access a printer any more."

(Photo: Terje Pedersen/NTB)

**T**his ransomware incident affected 32 000 employees and activities in 40 countries. The question is how a company should respond to a crippling event, which shuts down most of its systems. Where do you start?

"One of the first things we did was to post a warning at our main entrance," explains Halvor Molland, senior vice president for group communication. "But it had to be handwritten, because nobody could access a printer any more."

He was among the executives alerted that night, and has since repeatedly told the story of what happened. And, according to him, he often starts with that notice. It has become a symbol to many of how extensive the attack was.

## REPORT

"The next thing we did was to report the incident to the police – via text message, because the internet was inaccessible," Molland explains. "We didn't have much hope that they could crack the case, but it was the right move."

Asked how the group notified 32 000 employees in 40 countries in these circumstances, he says it involved a combination of what they had been drilled to do and exercising creativity.

Hydro had practised dealing with a cyber attack, detailed plans were available, and the organisation was trained to mobilise quickly.

"But we hadn't envisaged something of this

scope," he admits. Creative solutions for spreading the word included establishing WhatsApp groups and a dedicated news app for employees.

## PRIORITY

Chief information security officer Torstein Gimnes Are was another of the Hydro executives awakened that night. His first priority was to secure an overview – which was not straightforward.

"When you suffer a cyber attack, it often aims to isolate, restrict and shut down," he explains. "But we saw here that most of our business areas in every country we're in had been hit."

"It quickly became clear that we faced a massive assault which would have major consequences for our systems."

Hydro has a common IT platform used by all its business areas. And the immediate response was precisely to shut down all network links and servers. When people came to work, they had to start up manual routines where the platform was unavailable.

"Chaos reigned, but we began work at once on building up a secure infrastructure," says Are. "This was based on a backup system which is independent of our IT platform."

That job took weeks and months. During the initial phase, the group was left without an IT system – which had varying consequences.

Since production was not directly connected to the group's IT platform, most of its factories could go on working. With no support systems,



19.03.2019

### Hydro Network.

ices to the Hydro  
eives connected

Phone/Tablet etc.)

ORBS  
HYDRO ER  
UNDER CYBER-  
ANGREP.

IKKE KOBLE  
PC TIL NETTVEKK  
INNTIL NY  
BESKJED

ORBS

however, it was difficult to continue for long.

“They had no access to customer lists or order books, for example,” Are explains.

#### **PREPAREDNESS**

Hydro’s hydropower facilities are subject to Norway’s emergency preparedness regulations, which require such systems to be separate from a company’s IT platform.

They thereby escaped becoming part of the attack, unlike the factories. But exceptions also existed for the latter, with Hydro’s plant at Lichtervelde in Belgium largely unaffected.

However, that reflected the sales manager’s scepticism about the IT system. Every Monday morning, he therefore printed out all the orders and put them in a ring binder.

“He became a hero, because the factory was more or less unaffected by the attack and could operate as normal,” reports Molland.

In the rest of Hydro’s production network, people were forced to empty wastepaper baskets and containers in search of possible customer data which might have been printed out.

“Most parts of the group faced the equivalent of tossing all computers and mobiles out of the





Torstein Gimnes Are (left) and Halvor Molland at Hydro.  
(Photo: Morten Gjerstad)

window and trying to keep going for six-eight weeks,” says Molland.

The Hydro management resolved at once to admit what had happened. Early on the morning of the attack, the group issued a stock market statement and a press release about the position.

“We always try to be open,” Molland explains. “I’d say that’s part of our culture. But there are clearly a number of things we can’t say for competitive reasons and the like.

“And here we were also in a position where not everything could be revealed for security reasons.”

Everyone working to restore the Hydro platform knew that the attackers still had access to the same system, and were probably following the media coverage.

So a number of things could not be shared with the outside world, Molland explains. “It was demanding, but we were as open as we could be at any given time.”

## NO SURRENDER

The virus attack on Hydro was intended to force it to pay a ransom in order to regain control over

of system. But surrendering to this demand was never an option.

“Even if we’d paid, the attackers would still have had access to our system,” explains Are. “So that was always out of the question.”

He reports that the ransomware virus entered the system after an employee opened an attachment to an e-mail from somebody he knew well and had been expecting to hear from.

“In other words, there was no point in blaming anyone for this.”

The question then is what you can actually do when e-mails you think are completely secure turn out to contain a virus. Is it impossible to defend against a cyber attack?

“It could seem that way, of course,” says Are. “And it’s true that if somebody wants to break in and devotes enough resources to doing so, they’ll succeed.

“Having been in such a position and felt the sense of powerlessness and frustration, however, we’ve acquired much useful experience and learnt many lessons in tackling such attacks.

“I find that Hydro’s employees have become more aware and awake, asking questions and seeking help. This is about communicating with people about the threats which exist.”

He adds some helpful advice, starting with backups. “These are naturally important, and should not be connected to the regular IT platform. That will ensure access if you have to rebuild from scratch – like we did.

“We in Hydro then benefit from doing a lot of drills, thinking through different scenarios and regularly questioning whether our backup is good enough. That’s something every company should do, regardless of size.”



It also makes sense to have something on paper which can help to maintain activity should something like this happen, he adds, and points to the segregation in Hydro between the IT platform and the factories, which helped it to sustain production.

Molland reports that the group often runs courses and drills on such issues as phishing and social manipulation, and seeks to devote continuous attention to IT security in the organisation.

“That could involve everything from courses on identifying harmful e-mails to how you should relate to TikTok or ChatGPT.”

### **SENSIBLE**

Lessons learnt by Hydro were not confined to IT security. The group also found that it could be sensible to take a few technological steps back from time to time.

“Independently of the IT system, we see that our factories have gone too far in some cases with efficiency improvements and automation,” says Molland.

“A few too many buttons are removed. We learnt that reintroducing some manual control systems on machinery makes sense for maintaining output during a crisis.”

When production ceased, the group found that a number of its retirees returned and offered their expertise in manual control of the machinery.

“These devices had been so thoroughly automated that nobody in the workforce had experience of running them manually,” Molland says.

He points to a number of newspaper headlines along the lines of “Hydro saved by

the pensioners”, and would not personally go that far.

“Nevertheless, having the technical know-how to run a system both manually and through an IT system is undoubtedly important, and another valuable lesson we’ve learnt.”

### **LOSSES**

This incident left the Hydro group with documented losses of more than NOK 800 million.

Today, however, the Norwegian police know a lot more about who carried out the assault and not least – thanks to all the documentation from Hydro – how better to halt such attacks.

Molland regards this as further confirmation that Hydro did a lot right in the hours after the assault.

“We hadn’t expected the police or the Norwegian National Security Authority (NSM) to discover so much about this case. But it only shows, once again, the importance of being open.” ★

*To learn more about this story, in Norwegian only, see the Cyberangrepet episode at [psa.no/](https://psa.no/) podcast. Halvor Molland and Torstein Gimnes describe in their own words how they experienced the 2019 attack.*



## FACTS:



### Strengthened ICT security

Protecting ICT systems is as significant in the petroleum industry as it is in other sectors. That applies both to the systems managing hydrocarbon production and to information on enterprises and activities in the industry.

Over time, the Norwegian government has addressed the intelligence threat to the petroleum sector and the need to strengthen security there.

The PSA has emphasised the need to be alert and for the companies to be in control of their own ability to respond. It has also been a driver for and contributed to increased knowledge about risk related to ICT security.

Broad contacts are maintained with the industry by the authority, which communicates challenges and measures for enhancing the robustness of ICT security through various activities and collaboration arenas.



RESPONSIBLE PUBLISHER  
PETROLEUM SAFETY AUTHORITY NORWAY  
Professor Olav Hanssens veg 10  
P O Box 599  
NO-4003 Stavanger  
Tel: +47 51 87 32 00  
E-mail: [postboks@ptil.no](mailto:postboks@ptil.no)  
Website: [www.psa.no](http://www.psa.no)

EDITORIAL STAFF  
Inger Anda (editor-in-chief/journalist)  
Øyvind Midttun (editor/journalist)  
Eileen Brundtland (journalist/web editor)  
Olav Hove (journalist)  
Gunlaug Leirvik (journalist)  
Janne-Beth Carlsen N'Jai (graphic designer)  
Margrethe Hervik (distribution)  
Rolf E Gooderham (English editor/translator)

PRINT RUN  
Norwegian: 5 500  
English: 2 000

PAPER  
Cover: Munken Polar, 300g  
Inside pages: Munken Polar, 150g

PRINTER  
Aksell, Stavanger

This issue went to press on 5 May 2023.

**Abbreviations used in this issue**

HSE: Health, safety and the environment  
NCS: Norwegian continental shelf  
PSA: Petroleum Safety Authority Norway

