PST
POLITIETS SIKKERHETSTJENESTE

National Threat Assessment

2025

PST
POLITIETS
SIKKERHETSTJENESTE

Beate Gangås
Photo: Norwegian Police Security Service

Foreword

The main responsibilities of the Norwegian Police Security Service (PST) are to understand, communicate and counteract the most serious threats to the safety of the realm. Our National Threat Assessment (NTA) describes the threats we believe will be most prevalent in 2025.

These are troubled times. The security situation is in ux, placing demands on society's ability to adapt. War, con ict and rivalry in the world will continue to mark the threat situation in Norway.

Russia remains the greatest threat against security in Europe. Over the past year, Russia has demonstrated its resolve and ability to carry out sabotage operations on European soil. It is likely that this may also a ect Norway. Meanwhile, the intelligence threat from China is also increasing. Several states may use proxy actors to achieve their objectives in Norway.

We expect 2025 to be marked by hybrid threats. Such threats include sabotage, in uence operations and illegal intelligence. Hybrid threats engender uncertainty, unrest and fear among the people, corroding our democracy. Overall, the threats to Norway posed by state actors are more unpredictable, extensive and demanding than they have been for many decades.

Escalation in the level of con ict in the Middle East could a ect threat actors in Norway and lead to more radicalisation, polarisation and unrest. We are seeing ever younger individuals being radicalised into extremism, and many of them are struggling with mental illness and di erent types of exclusion.

Extremists and state actors alike seek to in uence our opinions, thoughts and feelings. Threat actors try to manipulate public opinion, either to increase support for their own views or to undermine trust in our society. Such activity can fuel polarisation. We expect smears and threats against dignitaries when controversial issues attract a great deal of media attention, especially in the run-up to the elections to the Norwegian Parliament (Storting) and Sámi Parliament (Sámediggi) this coming autumn.

Smooth, close cooperation with other social actors is decisive if we are to successfully counteract the threats facing us.

Beate Gangås
Sjef PST

Introduction

The National Threat Assessment (NTA) is an unclassi ed report on threats from state actors and extremists, and threats to dignitaries in the year ahead. It is intended to help facilitate a shared national understanding of the threat situation.

The NTA is intended to enable other actors in society to protect themselves against threats. It is important that all who read this report consider the content, and determine for themselves its relevance and consequences for them or their businesses. Businesses and individuals must identify their own assets and vulnerabilities in order to introduce appropriate protective measures of their own.

The NTA is also intended to raise awareness in society in general. Tips from the public are important for PST's e orts to avert and prevent threats to Norway. Accordingly, we urge anyone who has a concern or information of interest to contact us. There is a low threshold for contacting PST.

PST.no/tips-oss

THE COMMUNICATION OF THREATS

National standard	Description
Highly likely	There is very good reason to expect
Likely	There is good reason to expect
Even chance	Something is equally likely and unlikely
Unlikely	There is little reason to expect
Highly unlikely	There is very little reason to expect

The assessment employs a set of standardised terms for degrees of probability. The purpose of this is to create a more uniform description of probability in the assessments, thereby minimising ambiguity and misunderstandings.

PST's terrorism threat scale

PST's terrorism threat scale is intended to give an overall impression of the terrorist threat situation. While the degrees of probability represent PST's assessment of the likelihood that there will be an attempt to carry out an act of terrorism, this scale expresses the severity of the situation.

The scale applied has five steps, from level 1, which means no threat of terrorism, to level 5, which involves a critical threat of terrorism. When stipulating threat levels, PST takes the current threat assessment as a basis, then combines it with an assessment of (i) the degree of severity/damage potential of a possible terrorist act, (ii) the uncertainty and the extent of the gaps in the intelligence associated with relevant threat actors, and (iii) our/the authorities' ability to implement countermeasures before any threats are carried out.

The terrorist threat level is determined on the basis of a qualitative assessment. The terrorist threat level is an attempt to describe several complex conditions in a simple manner.

A threat assessment will always be the basis for any change in the level of the threat of terrorism. It will involve an assessment of how relevant factors, actors and events a ect the threat situation in Norway.

Level	Concept
5	Critical threat of terrorism
4	High threat of terrorism
3	Moderate threat of terrorism
2	Low threat of terrorism
1	No threat of terrorism

PST's terrorism threat scale

Critical threat of terrorism: PST's assessment is that a terrorist attack is imminent, or a terrorist attack has been carried out and more attacks may occur.

High threat of terrorism: PST's assessment is that one or more persons have speci c, realistic plans and that they are taking concrete steps to carry out terrorist attacks and/or that several factors reinforce the terrorist threat.

Moderate threat of terrorism: PST's assessment is that one or more persons intend to carry out a terrorist attack, but that they have not taken speci c steps or devised realistic plans and/or that some factors reinforce the terrorist threat.

Low threat of terrorism: PST's assessment is that there are few people who want to carry out terrorist attacks and/or that few factors reinforce the terrorist threat.

No threat of terrorism: PST's assessment is that no one wants to carry out a terrorist attack, and there are no factors that exacerbate a terrorist threat.

MAIN POINTS

State intelligence activities, influence operations and sabotage

Page 10

Russia's full-scale invasion of Ukraine and the deteriorating relationship between Russia and the West continue to characterise the threat situation in Norway. In addition to extensive, continuous intelligence and in uence operations, there is an increased likelihood that Russian intelligence services will try to carry out sabotage operations in Norway.

Norway is an intelligence target for China, and we expect the intelligence threat to increase in the long term. We also see that in uence activities on the part of Chinese actors are becoming more prominent, and that Chinese actors are using both legal and covert methods for achieving their goals in Norway.

The fraught security situation and con icts in the Middle East will continue to impact the threat situation in Norway. The fact that the terrorism threat level in Norway was high in autumn 2024, due to some extent to the threat from actors with ties to Iran, illustrates this.

Foreign intelligence will use a number of di erent means and methods, constantly adapting to changing conditions and Norwegian countermeasures. Several of these measures are included in what is often referred to as the use of hybrid means. These include cyber operations, the recruitment of sources, in uence operations, sabotage, covert procurements and use of security-threatening economic means. In addition, refugees, dissidents and those critical of regimes will be subject to tracking and surveillance on the part of several authoritarian regimes.

Politically motivated violence – extremism

Page 28

Islamist extremism and right-wing extremism are expected to pose the greatest terrorist threats against Norway. We believe there is an even chance that both Islamist extremists and right-wing extremists will try to carry out terrorist acts in Norway in 2025. The threat from Islamist extremists is still considered to be somewhat more serious than the threat from right-wing extremists. This is due to more Islamist extremist attack activity in Europe, the fact that the terrorist organisation the Islamic State (ISIS) is more determined to carry out attacks in the West, and that the warfare between Israel and Hamas in Gaza has led to more radicalisation. The threat from right-wing extremism primarily comes from right-wing extremists who participate in transnational digital networks that incite violence.

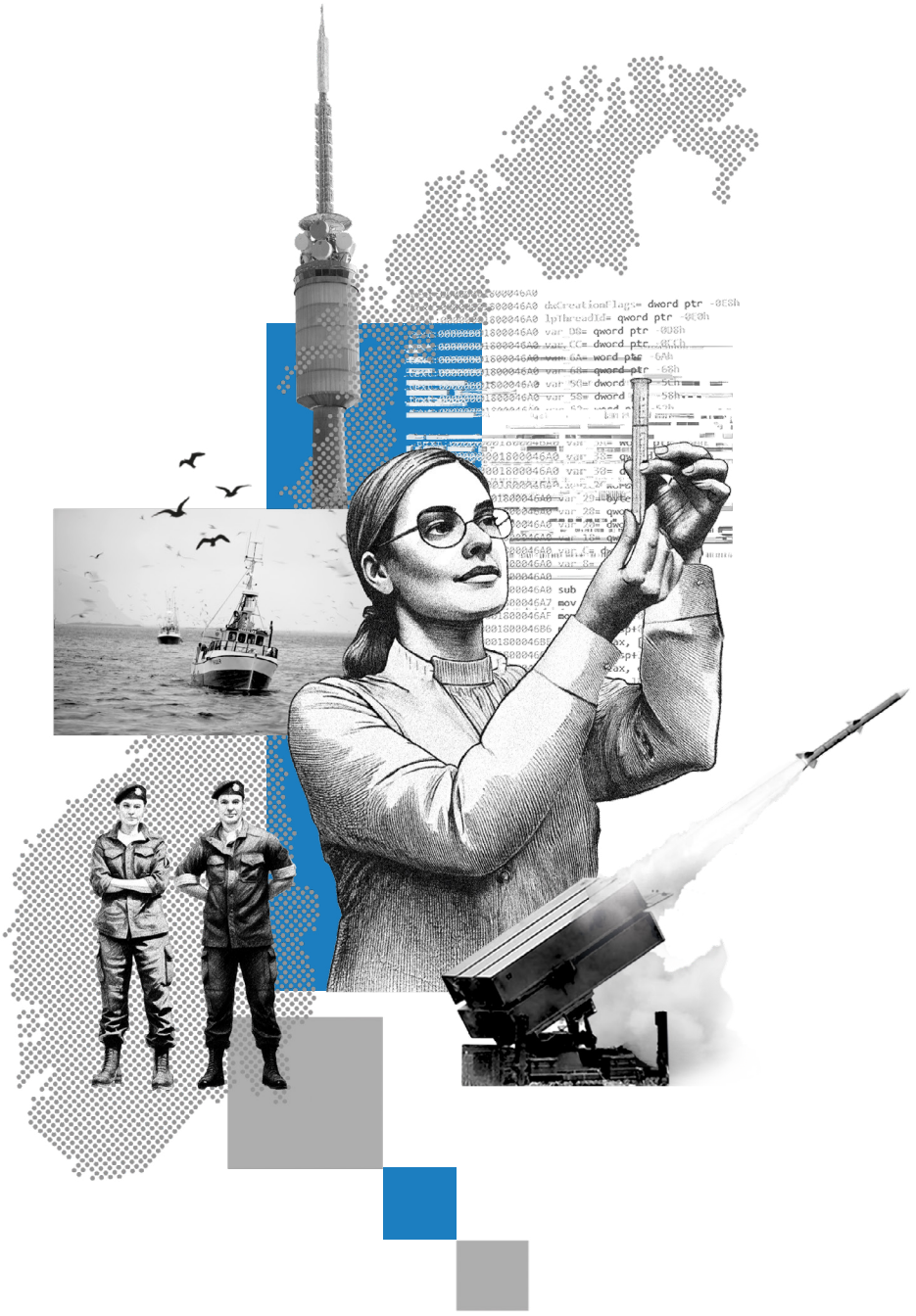
Digital platforms are major arenas for radicalisation and recruitment. We are seeing broader dissemination of extremist content on popular commercial platforms than earlier.

We observe a negative trend as more young people are consuming online material that incites violence. This raises the risk of radicalisation and recruitment to extremism among young people in Norway. Our concern is that some individuals will translate extreme views into acts of terrorism.

Threats to dignitaries

Page 42

In general, we consider it unlikely that anyone will attempt to carry out serious acts of violence against dignitaries in Norway in 2025. We expect more smears and threats against dignitaries when controversial issues receive a great deal of media attention, especially in connection with the general and Sámi parliamentary elections. Dignitaries will continue be vulnerable targets for foreign states' intelligence activities.



State intelligence activities, influence operations and sabotage

The past year has brought to light several examples of the severity of the threat from state actors. In 2024, we saw that Russia succeeded in carrying out dozens of incidents of sabotage and disruptive activities on European soil. In Norway, PST arrested two Norwegian nationals on suspicion of spying for Russia, China and Iran. We have seen Russia attempt to rebuild its capacity to engage in intelligence activities from its embassy in Oslo, after the government declared a number of intelligence o cers personae non gratae in Norway in 2023. We have also experienced a high terrorism threat level for much of the autumn, to some extent due to the danger of actors with ties to Iran carrying out terrorist acts in Norway.

Large parts of the threat situation remain unchanged in 2025. Russia and China are highlighted as the most central actors, although we also expect activities on the part of Iran and North Korea. At the same time, we would point out some important changes in the threat situation in this year's NTA. The threat of sabotage posed by Russia is greater now than it was a year ago. So-called proxy actors are being used by more states. Cyber operations are becoming increasingly di - cult to detect. In addition, we expect the threat of in uence operations from China, among others, to become more prominent.

In 2025, Norway will be exposed to intelligence activities and in uence operations and potential sabotage from state actors. These are all means that are part of what is referred to as the 'use of hybrid means'.

The following chapter is our assessment of what we may face in the year ahead.

THE ACTORS AND THEIR TARGETS

Russia

Heightened threat of sabotage from Russia

The security situation has increased Russian intelligence services' propensity to accept risk in Europe. Since late 2023, Russian intelligence has carried out dozens of sabotage actions and disruptive activities using proxy actors. The actions have primarily targeted property and logistics infrastructure related to deliveries to Ukraine, in addition to ordinary civilian infrastructure, including means of transport and shops. So far, we have not observed any attempts at such actions in Norway.

However, PST finds it likely that Russian intelligence will try to carry out such actions against targets in Norway in 2025. The purpose of any actions against targets in Norway will be to prevent us from making deliveries to Ukraine or to negatively influence public opinion on support for Ukraine. The targets of any actions in Norway will probably be similar to what we have seen in Europe. In addition, Norwegian-owned energy infrastructure may also be a target for sabotage in the year ahead. Whether, how and the extent to which this will happen depends, among other things, on Russia's intentions and on how the war in Ukraine unfolds.

> Proxy actors are individuals or organisations with no formal ties to intelligence and security services or to other government agencies and which, intentionally or unintentionally, carry out activities on behalf of, or in support of, the authorities. The activity may be politically, ideologically or financially motivated.

Focus on military targets, the High North and the war in Ukraine

Given the security situation in Europe, Russia needs extensive information about NATO countries like Norway. The Norwegian Armed Forces and Allied countries' military capacities located in Norway will continuously be exposed to Russian information gathering. Russian intelligence will also continue to map Norway's critical infrastructure and try to identify vulnerabilities. This type of information can be exploited for subsequent intelligence, influence operations and sabotage activities, or ultimately, in a possible future armed conflict with Norway. Our expectation is that actors involved in Norwegian policy-making will continue to be intelligence targets for Russia. This is true in particular for actors involved in Norwegian defence, foreign and security policy, but also in the sectors of justice and emergency preparedness, trade and industry, and energy and environment.

The Norwegian Armed Forces and a number of other state and private actors in Norway are also targets owing to the support they provide to Ukraine. We expect that Russian intelligence will attempt to obtain information about Norwegian donations and direct sales of weapons and other materiel to Ukraine, and try to disrupt, delay or prevent this. Moreover,

In 2022, a Russian national was arrested by PST and charged with attempted aggravated intelligence-gathering for the benefit of Russia. The man operated under the guise of being a Brazilian researcher, but subsequently admitted that he was a Russian national. Last year, the man was part of an exchange agreement between Russia and the West. The photo was taken when President Vladimir Putin received the Russians that had been imprisoned in western countries. Photo: Sergei Ilyin/Sputnik/NTB

we expect that Norwegian public opinion will be a target for Russian in uence operations, not least in an e ort to in uence attitudes to Russia's war against Ukraine.

Russia has been subjected to a regime of increasingly more comprehensive sanctions in response to its full-scale invasion of Ukraine. This means that Russian actors will continue to carry out covert procurement activities in 2025 against companies in Norway that manufacture or develop goods, services and technology of value for military use.

The Russian intelligence services will carry out operations against targets throughout Norway. At the same time, the High North will be of particular interest to Russia. This is because of the border areas in Finnmark and the Russian presence on Svalbard, as well as the increased strategic importance of the Arctic against the backdrop of a more fraught security situation. Politicians, ministries and others that determine the main lines of Norway's High North policy will therefore be vulnerable targets for Russian intelligence and in uence activities. This includes business leaders, civil society and academia.

Russian intelligence adapts its use of means in the face of countermeasures

The Russian intelligence services employ a wide range of means and methods against targets in Norway. The means are continuously adapted to changing circumstances and Norwegian countermeasures.

Since Russia's full-scale invasion of Ukraine in 2022, Norway has cut back the number of Russian intelligence officers under diplomatic cover in Norway. In addition, stricter entry rules challenge Russia's ability to make use of visitors, and restrictions on Russian vessels calling at our ports have made it more difficult for Russia to carry out covert maritime intelligence activities.

In response to this trend, we expect Russia to increasingly conduct its intelligence activities and influence operations from Russian territory. This includes digital influence activities, signals intelligence, cyber operations and the recruitment of sources through digital channels.

At the same time, Russian intelligence will continue to be physically active on Norwegian territory. For instance, intelligence officers under diplomatic cover will attempt to recruit sources and engage in other intelligence and influence activities. Russia will also try to send visitors to Norway to engage in intelligence work. It is also our assessment that Russian vessels, as well as Russian crew members on third-party vessels, will continue to pose an intelligence threat to targets all along the Norwegian coast.

China

The intelligence threat posed by China is significant and will grow over time

Norway is an intelligence target for China because of our geographical location, influence in international forums such as the Arctic Council, and our close alliance with China's largest global challenger, the USA. Norway also has technological expertise in fields of interest to China.

In the year ahead, Chinese intelligence and security services will continue to try to gather information, to silence critical voices, and to influence groups and individuals in Norway. Chinese intelligence leverages external actors' specialised expertise, access and resources in its operations. This enhances the ability of Chinese intelligence to carry out advanced operations against targets in Norway.

China's influence operations are becoming more prominent

In keeping with China's superpower ambitions, the country's influence operations are becoming more prominent. China is increasingly demonstrating its volition and ability to carry out influence operations directly against inhabitants of Western countries. China has a comprehensive system for carrying out digital influence operations. A new trend is that

Signals intelligence (SIGINT) is the collection of signals, either from communication platforms or from electronic signals.

- Digital in uence campaign targets the Norwegian public

In 2023, for the first time, a Chinese digital influence campaign targeting the Norwegian public was uncovered. The ostensibly Norwegian online news paper 'Viking United News' was part of a larger international campaign involving a Chinese commercial company that cre ated more than a hundred fake websites that wove Chinese propaganda into a stream of news articles stolen from legitimate news sites.

commercial companies are helping to pro fessionalise China's digital in uence operations. This includes, e.g. the sale of fake user acco unts, the production of video material and the hiring of in uencers. Accordingly, we expect the quality of Chinese disinformation to improve and the scope of its digital in uence operations to expand in the years ahead.

Targets for Chinese intelligence activities in Norway

Chinese intelligence seeks to gain insight into political decision-making processes and to map local and national decision-makers and critics of China. Towards that end, China will continue to engage in cyber espionage against Norwegian authorities, businesses and organisations.

Chinese intelligence will also try to recruit Norwegian nationals to gain access to sensitive and classi ed information. Chinese services are generally interested in recruiting corporate actors, military personnel, researchers and people who hold sensitive positions in various government agencies and political organisations. Foreign policy communities are particularly vulnerable

Attempts will be made to intimidate people in Norway to silence them

China's far-reaching, global transnational repression is a persistent threat to individuals' democratic rights and freedom of action. Individuals in Norway who are outspoken critics of the human rights situation and governance in China are at risk.

- Norwegian national exposed to a digital recruitment attempt

In 2024, a Norwegian national was contac ted via WhatsApp by a person claiming to represent a Chinese institute. The person was looking for candidates who might have their own sources, to submit reports based on non-public information, for a fee. The actor wanted insider information on topics relevant to Chinese security interests, such as early warnings of san ctions and what the actor referred to as 'anti-China measures' that the United States and the West might introduce.

Over time, Chinese actors have shown interest in developing the Port of Kirkenes, and in establishing the port as a transportation hub in the Arctic. Meanwhile, PST has drawn attention to the growing intelligence threat from China and the party-state's desire to control supply chains and to establish a position in the Arctic.

Photo: Adam Ihse/TT Nyhetsbyrån/NTB

For example, representatives of the Chinese state have attended a human rights conference in Oslo with the intention of threatening and intimidating participants. We expect Chinese intelligence to continue trying to monitor dissidents and oppositional figures and to try to recruit sources in Chinese diaspora and dissident communities in Norway. A great deal of this activity will take place digitally. Individuals are often pressured to report to Chinese authorities by means of threats made against family members living in China.

China uses both legal cooperation and covert methods to obtain knowledge about technology with military applications

The race to adapt new technology to military use is part of geopolitical rivalry. China seeks to take advantage of private actors to ensure rapid military modernisation. In practice, this blurs the distinction between the civilian and military spheres. Research managers, guest researchers and students from institutions with ties to the Chinese Armed Forces (PLA) are working in Norway on technology that can be used for military purposes. Conferences and seminars are also arenas that are used to obtain information of military value, and to establish relationships with people who have access to such information. In 2024, people from institutions aliated with the PLA attended technology and science conferences in Norway. Further, Chinese intelligence attempts to recruit Norwegian nationals, not least through LinkedIn, to obtain information from the defence sector about advanced technology and equipment. Norwegian researchers considering travelling to China to work in talent programmes and research parks should be aware that the expertise they bring with them may be exploited for military purposes to benefit the Chinese state.

China's main instruments are economic

Even though China will take advantage of its considerable intelligence capacity in Norway, China's main instruments remain economic, e.g. investments and acquisitions. Chinese interest in the Port of Kirkenes is one example. The build-up of or Chinese involvement in logistics infrastructure, for example, paves the way for a long-term presence that improves the chances of obtaining information from and exerting pressure against Norwegian authorities.

Iran

Iran uses terror as a foreign policy tool

Iranian intelligence services will carry out intelligence and influence operations in Norway in the coming year. The Iranian regime may also employ terrorist attacks, assassinations and violence against individuals and groups in the West to silence critical voices, take revenge or express political discontent.

The regime is likely to use proxy actors to try to carry out violence and terror in the West in 2025. This could also affect Norway. Such proxies are individuals or groups without formal or ideological ties to the Iranian regime. This may include criminals and others who sell their services to Iranian intelligence services. For example, the Swedish authorities suspect that criminal networks in Sweden carried out attacks against the Israeli embassies in Stockholm and Copenhagen in October 2024 on behalf of the regime in Iran.

Acts of violence on behalf of the regime in Iran affect not only Iranian dissidents, but also Jewish, Israeli and American targets. In addition, individuals or institutions perceived as hostile to Islam are singled out. Whether Iran will carry out this type of action in Norway in 2025 depends, among other things, on how the conflicts in the Middle East unfold.

An escalation of the conflict could, for example, cause the Iranian regime to give priority to targeting Jewish and Israeli interests on Norwegian soil.

We expect the Iranian diaspora population in Norway to be subjected to surveillance, smears and threats from Iranian intelligence services and from others acting on their behalf. Those affiliated with academic institutions or the media, human rights defenders, and people who openly criticise the regime in Iran are particularly vulnerable. Such activities give rise to fear and uncertainty, and they can lead to self-censorship.

In 2025, Iran will also attempt to gather information about Norwegian dual-use technology, weapons technology and academic research. In this way, the regime seeks to circumvent international sanctions.

Illicit procurement, and proliferation of weapons of mass destruction

Norwegian technology is sought after by state actors

In 2025, we expect foreign states to attempt to acquire Norwegian goods, services and technology through covert means. Several Norwegian companies produce technology that is sought after by a number of state actors, including Russia, China and Iran.

A wide range of advanced technologies are currently sensitive in terms of security because they can be used for military purposes. Exports of military technology and civilian technology with military applications - known as ”dual-use technology” - are therefore strictly regulated through export control and sanctions regulations.

> Procurement attempts often involve several intermediaries in third countries. In 2024, for example, Russia used Chinese intermediaries to try to procure sanctioned technology from several Norwegian companies. Companies in Europe are also exploited for covert procurement attempts.

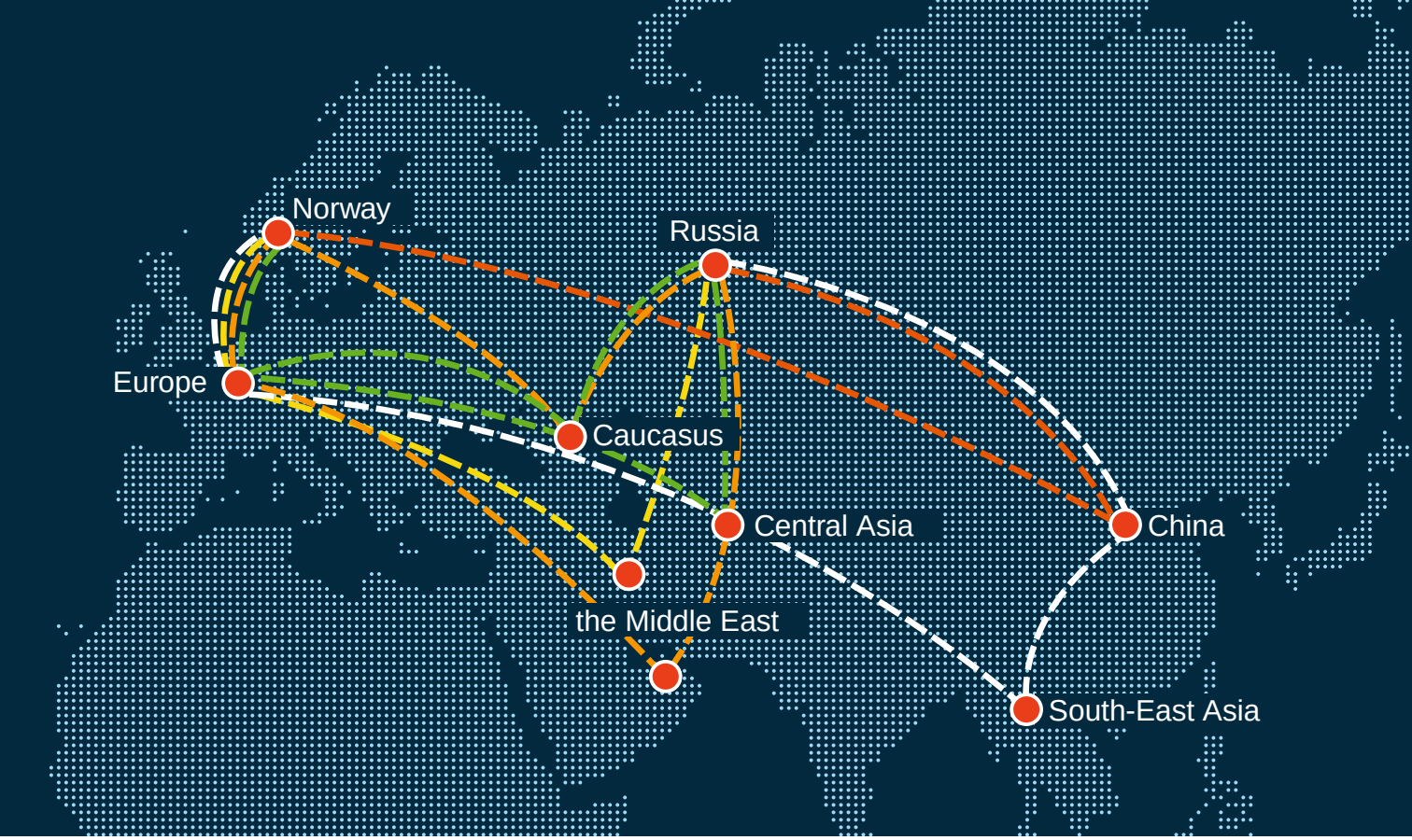
We expect Norwegian companies to continue to be exposed to signi cant threats from foreign actors operating in military procurement networks. Russia, in particular, needs Western technology to maintain its military capacity and ability to wage war in Ukraine. Russia is seeking to acquire both advanced and more basic technology to meet its military needs. This means that a broader range of Norwegian companies will be exposed to procurement attempts than was the case before the invasion.

Russia uses covert methods to circumvent an ever-stricter sanctions regime. For instance, Russian buyers often try to mislead Norwegian businesses and customs authorities by providing incorrect documentation, e.g. false end-user declarations.

Academic institutions and businesses are vulnerable targets

In 2025, states with which Norway has no security cooperation will try to acquire sensitive knowledge from Norwegian research instituti - ons and knowledge enterprises. Over the past year, we have observed particular interest on the part of China and Iran. We expect interest from these and other countries of concern to continue in 2025.

The transfer of technology and knowledge to foreign states can pose a threat to national security. Norwegian research institutions and knowledge enterprises possess expertise and manufacture technology of a high internatio - nal calibre. This includes expertise that can be



This is an illustration of how Norwegian technology or goods can end up in the hands of Russian end users. Although the specific routes on the map are fictitious, they are based on the Russian method for avoiding sanctions. Illustration: Aksell

- Examples of threat-prone areas of technology:

- Biotechnology
- Materials technology and metallurgy
- Nuclear physics
- Cryptography
- Quantum technology
- Nanotechnology
- Aerospace and propulsion technology
- Sensor technology
- Navigation technology
- Robotics and autonomy
- Microelectronic systems

used to develop technology or components for military purposes. In the current security situation, some countries' governments are willing to go to great lengths to gain access to and control of such knowledge.

In 2025, research institutions and other knowledge enterprises will be particularly vulnerable to approaches from foreign states. For example, state actors will try to gain access to employee facilities, such as laboratories and instruments, as well as to know-how or net-works. They will also take advantage of research collaboration, international conferences and other meeting arenas to secure access to sensitive technology or classi ed information.

THE METHODS

Foreign intelligence services employ a number of di erent methods against targets in Norway. In this section, we outline how individuals and under-takings can be exposed to the following phenomena and means:

- Cyber operations
- Recruitment of human sources
- Intelligence involving civilian vessels
- In uence operations
- Security-threatening economic means
- Transnational repression

State cyber actors are operating ever more covertly

In the cyber domain, the threat to Norway is signi cant, as well as unpredictable. The digital threat situation is in uenced by a dynamic actor landscape, geopolitical events, and the continuous development of technology and methods. State cyber actors are operating ever more covertly, challenging our ability to detect their operations and identify who is behind them. This also means that there are probably large unreported gures for the number of businesses in Norway that are a ected.

We expect that Norwegian businesses will continue to be impacted by cyber operations mounted by countries such as Russia, China, North Korea and Iran in the year ahead. Since Russia and China have considerable cyber capabilities, they are expected to be behind most cyber operations in Norway in the coming year. At the same time, Iranian and North Korean cyber actors are also able to carry out operations with signi cant damage potential.

State cyber actors use di erent types of proxy actors

State cyber actors use proxy actors in order to operate more covertly. For example, state actors use cyber security and technology companies, cyber criminals and hacktivist groups to carry out cyber operations or to develop capabilities on their behalf. Some state cyber actors also pretend to be proxy actors, for example, by copying the digital signature of a hacktivist

group. Such covert behaviour and the actual use of proxies make it di cult to expose who is really behind activities.

The development of methods and techniques makes the threat situation more unpredictable

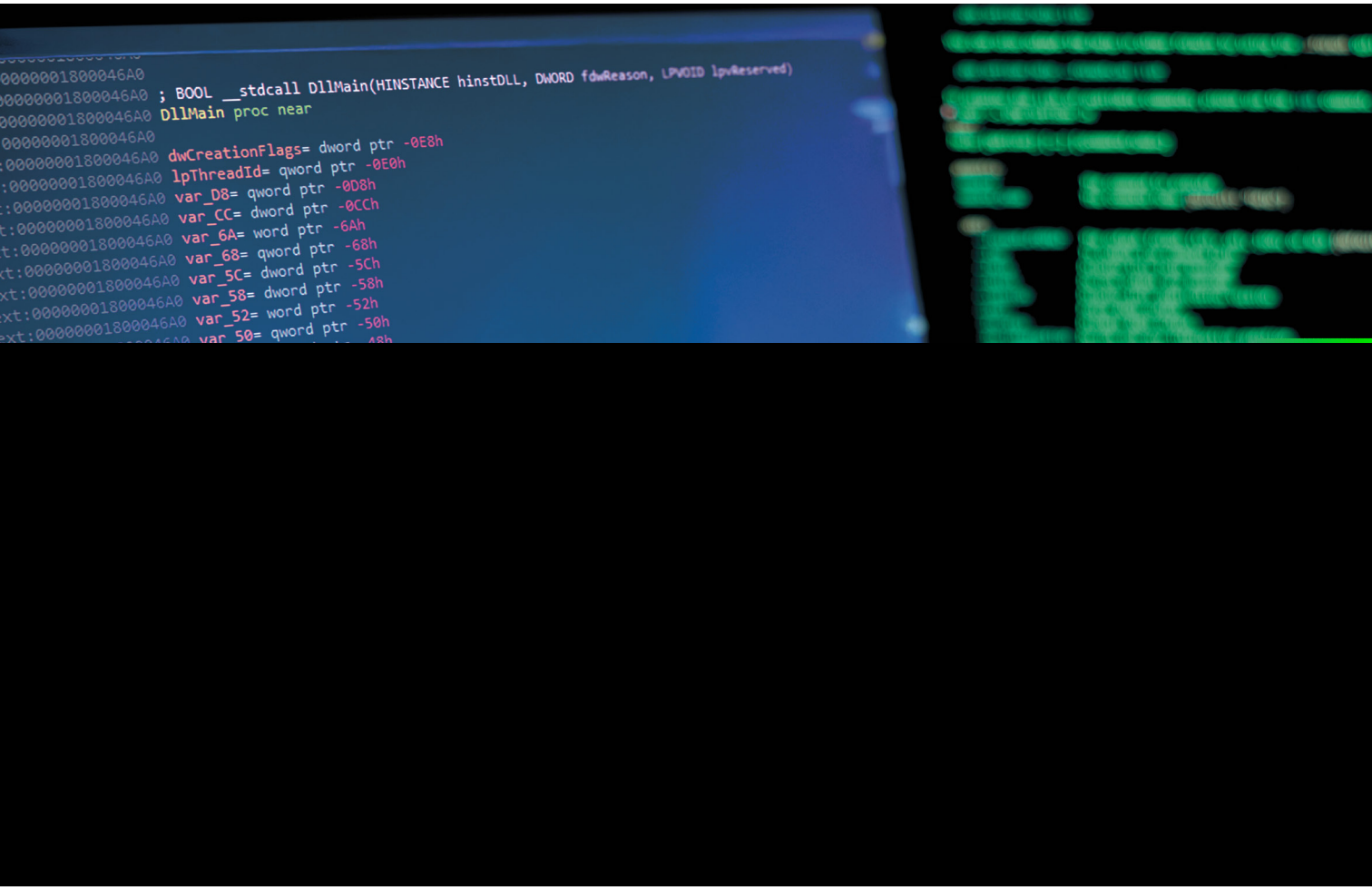
State cyber actors are constantly developing their own methods and techniques. In recent years, for example, we have seen more use of zero-day vulnerabilities and supply chain attacks. Zero-day vulnerabilities give cyber actors opportunities to exploit a vulnerability of which the victim is unaware. In certain ope - rations, the cyber actor may have had access to a system for a long time before the vulnera - bility becomes known and its presence is detected .

Another method we have seen in Norway is that state actors lease servers in data centres under the guise of being legitimate businesses. The leased servers can be used to compromise targets in Norway and the rest of the world.

In addition, we see state cyber actors exploi - ting existing and known vulnerabilities in pro - ducts made by global software manufacturers. They also rely heavily on human vulnerabilities in the form of spearphishing operations. Actors are getting better at tailoring their approaches to make it harder for the victim to detect the operation.

Zero-day vulnerability. A zero-day vulne - rability is a vulner-ability that someone knows about, but which is unknown to the public, the supplier or the manufacturer of the product in question. This means that the supplier or manufacturer has no chance to rectify the vulnerability before a threat actor exploits it.

Supply chain attack. Supply chain attacks are cyber operations aimed at weak, more peripheral links in a company's supply chain, such as subcontractors. Undertakings with robust data security systems and routines are vulnerable if their subcontractors have failed to implement similar security measures.



An excerpt from malware developed by a state actor. Photo/illustration: Norwegian Police Security Service/Aksell

«Living O the Land»

Several cyber actors use ”Living Off the Land” (LOTL) techniques in their cyber operations. This type of technique is used after the cyber actor has carried out a computer break-in and gained access to a system, i.e. the techniques the actor uses to move from the system’s front door to the actual target of the operation. These techniques involve a cyber actor using software and functions that are already part of an IT system in order to move around in the system. For example, they can give themselves multiple access points in the system. Since the cyber actor uses existing tools in the systems instead of malware, no traces are left behind, making it more challenging to detect a potential operation and find out who is behind it.