PST
POLITIETS SIKKERHETSTJENESTE

National Threat Assessment

2025

National Threat Assessment 2025
Published in Norway (2025) for the Norwegian Police Security Service (PST)
pst.no

Circulation: 4000

Images in the publication: Getty Images/NTB

Design and illustrations: Aksell.no

Printing: Aksell.no

Aksell AS is an Eco-Lighthouse enterprise

SVANEMERKET
Trykksak
2041 0379

TRYKT
I NORGE
NO - 1470

The Norwegian Police Security Service (PST) is Norway's domestic intelligence and security service, and it is subordinate to the Ministry of Justice and Public Security. PST's main responsibility is to prevent and investigate serious crimes that threaten national security. This includes the identification and assessment of threats related to intelligence, sabotage, the proliferation of weapons of mass destruction, terrorism and extremism, as well as threats to dignitaries. The assessments are intended to provide a foundation for policy-making and to inform political decision-making processes. PST's National Threat Assessment (NTA) is part of its duty to inform the public by presenting analyses of expected developments in the threat situation.

The Norwegian Intelligence Service (NIS) is Norway's foreign intelligence service. Although subordinate to the Norwegian Chief of Defence, NIS does not concern itself exclusively with military matters. The main tasks of NIS are to warn of external threats to Norway and high-priority Norwegian interests, to support the Norwegian Armed Forces and the defence alliances Norway is part of, and to assist in political decision-making processes by providing information of significance to Norwegian foreign, security and defence policy. In the annual threat assessment 'Focus', NIS presents its analysis of the current situation and expected developments in geographic and thematic areas considered particularly relevant to Norwegian security and national interests.

The Norwegian National Security Authority (NSM) is Norway's agency for national preventive security. The agency's mission is to strengthen Norway's ability to counter espionage, sabotage, terrorism and hybrid threats. NSM helps organisations protect civilian and military information, systems, objects and infrastructure that are relevant to national security by giving advice and performing control activities, supervision, security testing and security research. In order to protect digital infrastructure, NSM operates a national warning system for critical infrastructure (VDI) and coordinates national efforts to handle serious cyber operations. Risiko, NSM's annual risk assessment, aims to help Norwegian enterprises manage security risks by providing information about vulnerabilities, threats and security measures.

NSM

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 flux, placing demands on society's ability to adapt. War, conflict 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 affect 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, influence 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 conflict in the Middle East could affect 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 different types of exclusion.

Extremists and state actors alike seek to influence 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 unclassified 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 efforts 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 affect 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 specific, 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 specific 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 influence 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 influence 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 conflicts 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 different 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, influence 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.

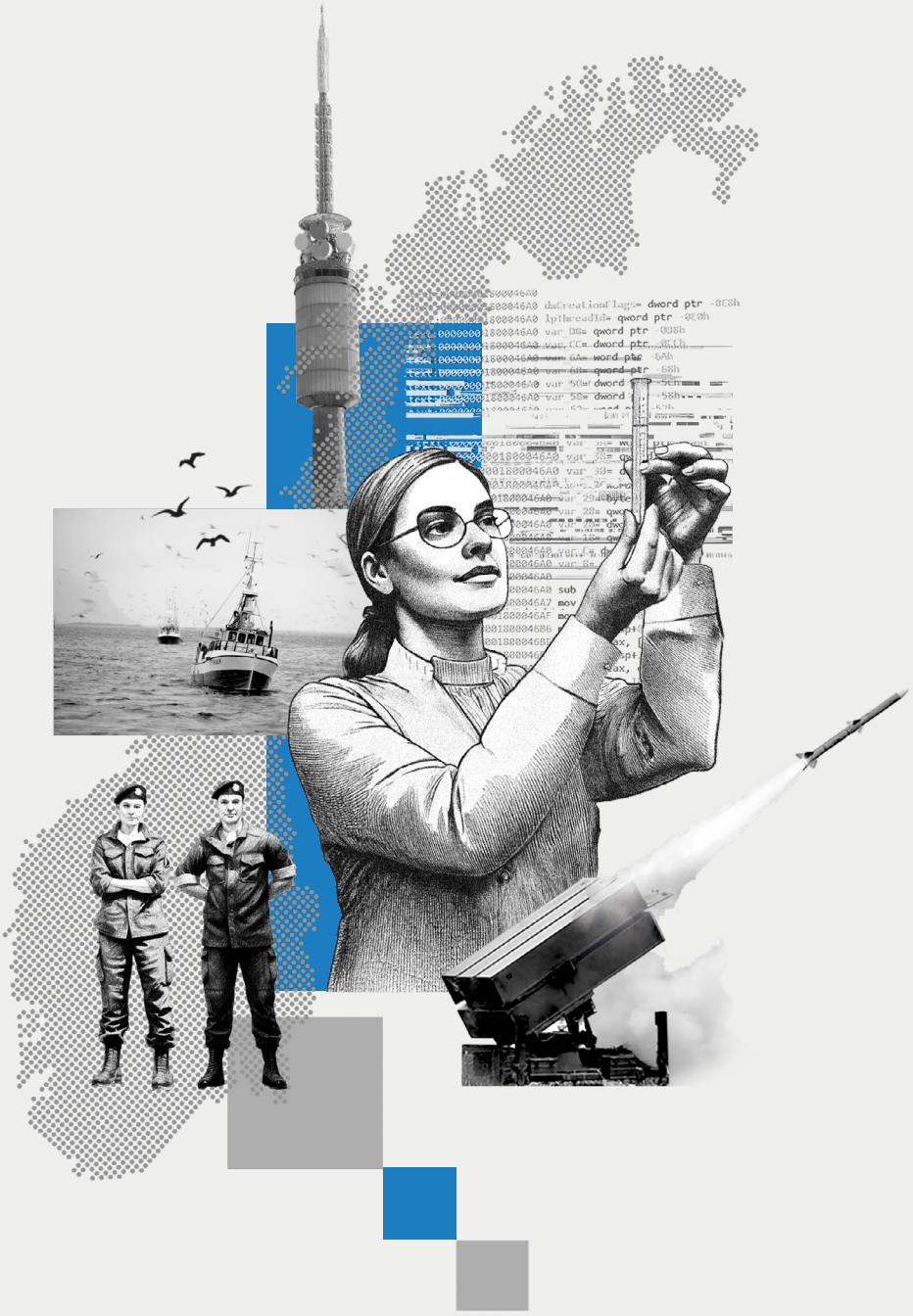
Digital platforms are major arenas for radicalisation and recruitment. We are seeing broader dissemination of extremist content on popular commercial platforms than earlier.

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 officers 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 difficult to detect. In addition, we expect the threat of influence operations from China, among others, to become more prominent.

In 2025, Norway will be exposed to intelligence activities and influence 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 influence operations, not least in an effort to influence 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 influence 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 influence 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 newspaper 'Viking United News' was part of a larger international campaign involving a Chinese commercial company that created 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 professionalise China's digital influence operations. This includes, e.g. the sale of fake user accounts, the production of video material and the hiring of influencers. Accordingly, we expect the quality of Chinese disinformation to improve and the scope of its digital influence 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 classified 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 contacted 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 sanctions 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 affiliated 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.

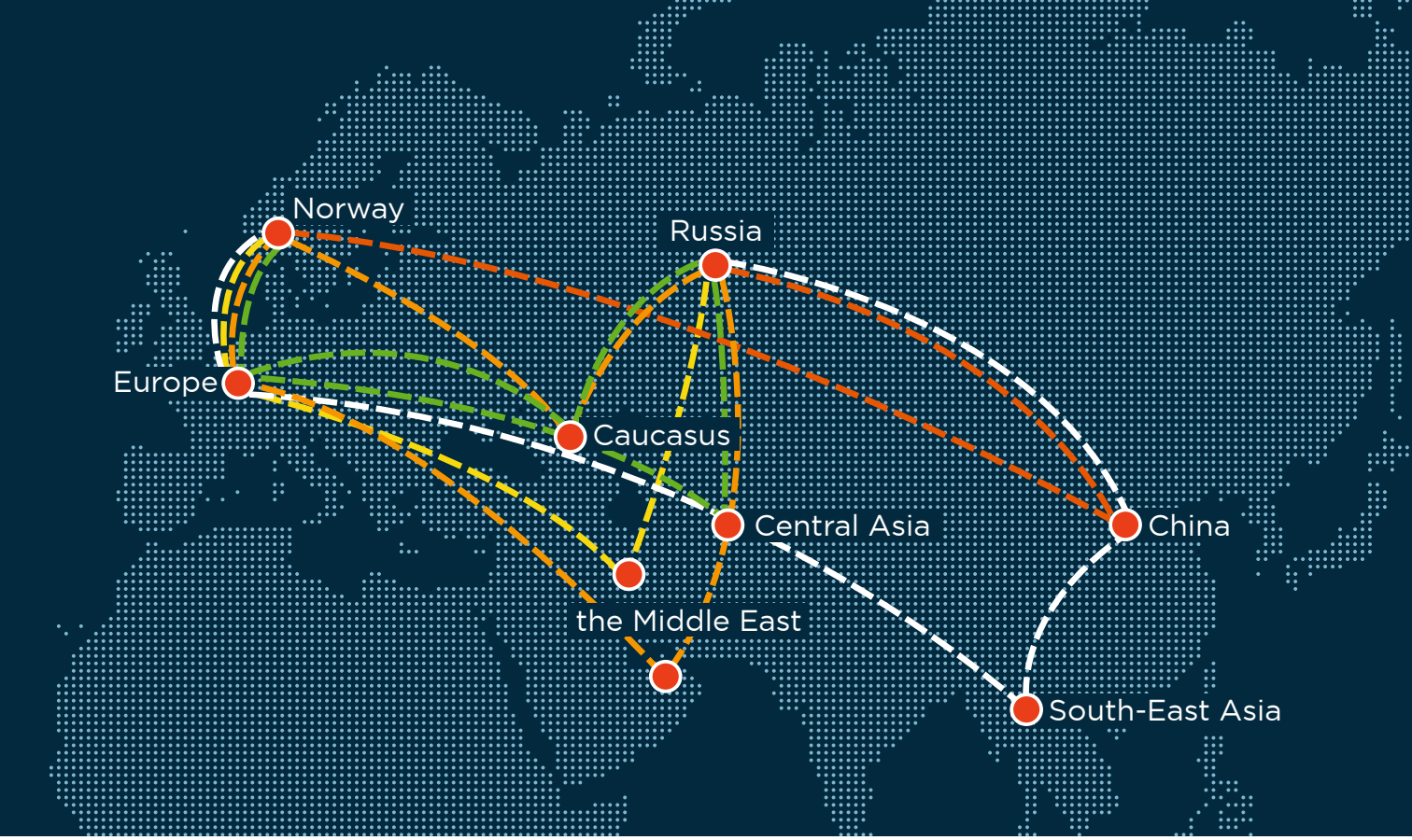
We expect Norwegian companies to continue to be exposed to significant threats from foreign actors operating in military procurement networks. Russia, in particular, needs Western technology to maintain its military capacity and ability to wage war in Ukraine. Russia is seeking to acquire both advanced 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 institutions 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 international 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 networks. They will also take advantage of research collaboration, international conferences and other meeting arenas to secure access to sensitive technology or classified information.

THE METHODS

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

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

State cyber actors are operating ever more covertly

In the cyber domain, the threat to Norway is significant, as well as unpredictable. The digital threat situation is influenced 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 figures for the number of businesses in Norway that are affected.

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 significant damage potential.

State cyber actors use different 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 difficult to expose who is really behind activities.

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

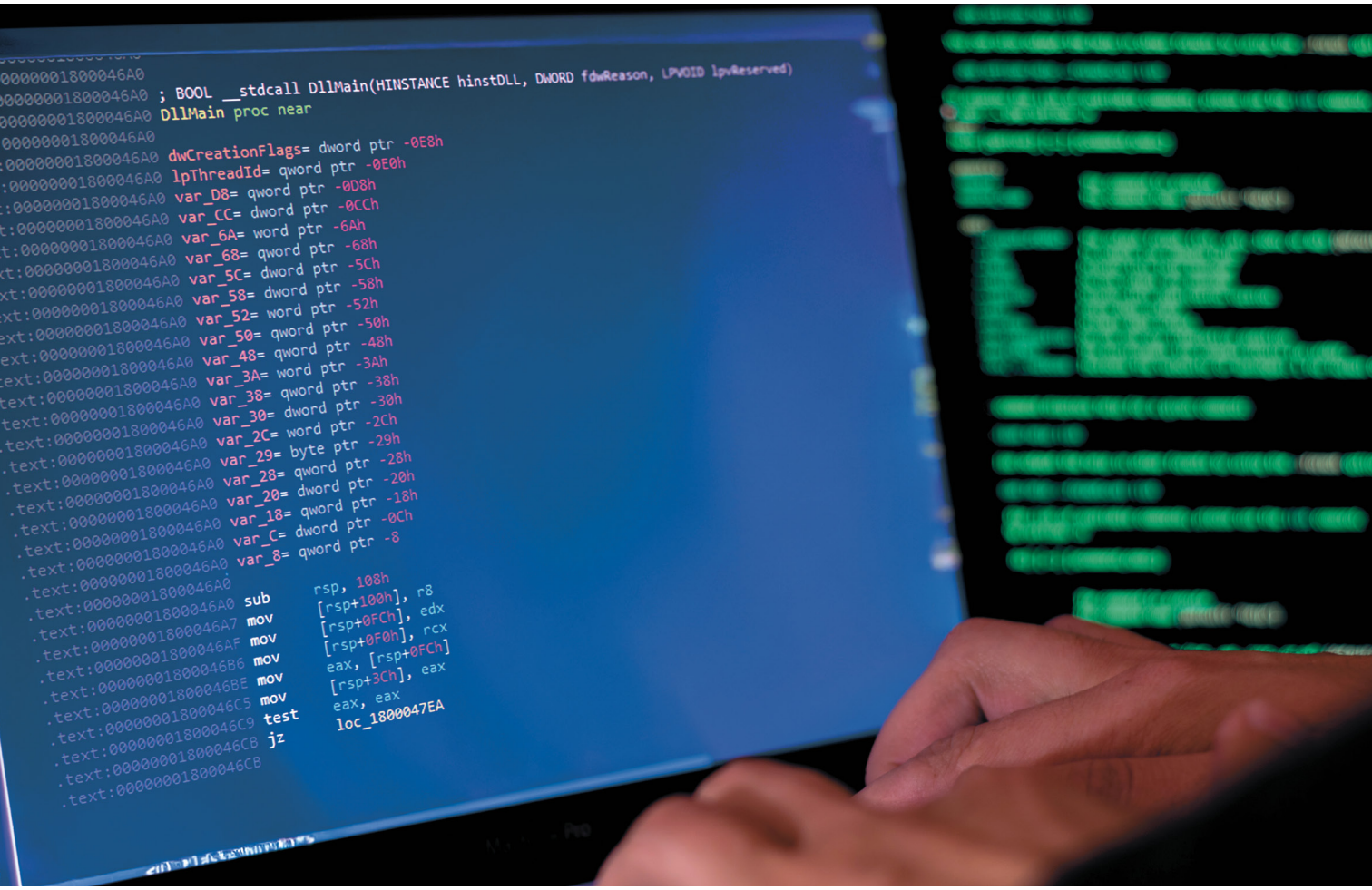
State cyber actors are constantly developing their own methods and techniques. In recent years, for example, we have seen more use of zero-day vulnerabilities and supply chain attacks. Zero-day vulnerabilities give cyber actors opportunities to exploit a vulnerability of which the victim is unaware. In certain operations, the cyber actor may have had access to a system for a long time before the vulnerability 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 exploiting existing and known vulnerabilities in products 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 vulnerability 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 Off 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.

Attempts will be made to recruit individuals in Norway

Artificial intelligence creates new opportunities

Artificial intelligence (AI) will increase the capability and effectiveness of all cyber actors. It is expected that state actors will use AI in cyber operations in Norway in 2025. Several countries are investing in the development of the technology and experimenting with the use of AI to improve their own methods and techniques.

Among other things, AI can be used to improve the quality of social engineering and to enable cyber actors to better identify and exploit vulnerabilities. However, it is at least as important to point out that AI offers significant opportunities to defend against threats. It is still hard to tell whether the effect will be greatest for the threat actors or those who need to protect themselves.

State cyber actors use AI for social engineering

Artificial intelligence can boost the ability and accuracy of actors when it comes to social engineering. In 2024, it was reported in open sources that Chinese, Iranian, Russian and North Korean cyber actors used large language models to support social engineering. For instance, AI has been used to translate text into different languages, to support the cyber actor in longer dialogues with victims in specialised fields, and to generate images, audio and video. This is used in disinformation campaigns and spearphishing operations, etc.

Recruiting and running sources are important parts of foreign states' intelligence activities in Norway. In 2025, the Russian and Chinese intelligence services in particular are expected to pose the greatest threat of recruitment attempts in Norway.

In recent years, both Russia and China have increasingly taken advantage of digital channels, e.g. social media and other applications, for their recruitment efforts. The publication of job vacancies is a recurring element in these attempts at recruitment.

PST is aware that several Norwegians have been asked on LinkedIn, etc. to write reports for Chinese think tanks in return for remuneration. At first glance, this appears reasonable and legitimate. China uses real as well as fictitious think tanks that have been set up to recruit sources.

The Russian intelligence and security services carry out digital recruitment attempts using tactics like publishing vague job vacancy advertisements on social media groups, or by fictitious users establishing direct contact with people they want to recruit.

Digital recruitment is cost-effective, relatively easy to sustain over time, and entails a low risk of detection.

Foreign intelligence services will also attempt to recruit sources in person. This can happen in Norway, for example, using intelligence officers under diplomatic cover. In certain cases, however, it may be easier for foreign intelligence services to carry out recruitment

campaigns against Norwegian nationals residing in third countries.

PST believes that people with family in or other ties to authoritarian states will be especially vulnerable to recruitment attempts, both in person and digitally. In today's security situation, Norwegian nationals travelling to Russia must expect to be exposed to recruitment attempts while there.

Individuals recruited by foreign states' intelligence services may be asked to perform a number of different tasks. Classified information will always be of interest, but we also see that foreign intelligence services are often interested in sensitive, unclassified information that is not openly available. Recruited individuals may also be asked to recruit their own sources and to perform practical tasks such as purchasing sanctioned goods, installing technical surveillance equipment, or carrying out acts of sabotage, terrorism or violence.

Intelligence involving civilian vessels

In 2025, foreign intelligence will still be using civilian vessels for intelligence purposes. This is referred to as maritime covert intelligence activity. Maritime covert intelligence activity targets Norwegian interests at sea, in inland waters and in ports.

All along the Norwegian coast, there is infrastructure, technology and activities of interest to foreign states. Vessels can be used to map Norwegian and Allied military capacity as well as critical infrastructure on the seabed and along the coast. The vessels can also arrange situations at sea to expose weaknesses in Norwegian preparedness or crisis management.

Access to Norwegian ports can be used to support illegal intelligence activities. This access can be used to smuggle goods that are subject to sanctions or export controls, and to infiltrate intelligence personnel into mainland Norway.

Russia poses the greatest threat with respect to maritime covert intelligence activity. Russia is currently subject to extensive restrictions, meaning that Russian vessels do not have access to ports on the Norwegian mainland. Exceptions to the port ban have been granted for Russian fishing vessels in Båtsfjord, Kirkenes and Tromsø, but the exceptions carry significant restrictions. Nevertheless, we expect that Russian intelligence services will continue to try to use civilian vessels as platforms for

intelligence activities. Russian crew on vessels sailing under the flags of third countries may also carry out intelligence activities against Norwegian targets.

China also has the option to use maritime covert intelligence activity. The Chinese Intelligence Act ensures that all Chinese individuals, companies and organisations are duty-bound to assist the Chinese intelligence services. This means that Chinese individuals and vessels may be required to help the Chinese services obtain information about Norwegian conditions.

«Vessels can be used to map Norwegian and Allied military capacity as well as critical infrastructure on the seabed and along the coast.»

Norwegian nationals will be exposed to influence activities from foreign states

We expect authoritarian states to engage in influence activities in Norway in 2025. At a time of growing geopolitical conflict, covert influence activities and disinformation have become important means employed by foreign states in attempts to shape decisions and attitudes to their advantage. The purpose is to preserve the security of a country's own regime by undermining the West's shared values and security, strengthening the country's global position.

Influence operations can take place in the physical or digital space. Russia's sabotage operations against supply chains for defence material to Ukraine may, for example, be intended to engender unrest in society in an effort to influence decisions about sending supplies to Ukraine. Digital influence operations may, for example, include the disclosure of information acquired through cyber operations in attempts to undermine confidence in important social institutions. This practice is referred to as 'hack-and-leak'.

In 2023, Norway was subjected to an influence operation from a cyber actor with ties to Iranian intelligence, operating under the alias 'Anzu Team'. The cyber actor began with a computer break-in at a Swedish company that offers text messaging services. The actor subsequently sent text messages to individuals in Norway, urging young Muslims to avenge Koran burnings.

China's digital influence operations have traditionally focused on quantity over quality. China and several other authoritarian states are experimenting with different techniques for the production and dissemination of influence material. Over time, this will improve its quality and persuasiveness. Even though the spread of Russian and Chinese disinformation often takes place at the global level, online communities in Norway will nonetheless be affected indirectly.

Russian attempt to influence the selection of the Nobel Peace Prize laureate

In 2015, just over a year after Russia adopted the decision to annex Ukraine's Crimean Peninsula, Norway was exposed to a Russian information operation aimed at influencing the Nobel Peace Prize Committee. The operation involved 'leaking' a fake letter from the President of the Ukrainian Parliament to an employee of the US Embassy in Oslo. The fake letter claimed that the US was trying to pressure the Nobel Committee into awarding the 2015 Nobel Peace Prize to the then Ukrainian president.

State actors' use of economic means will threaten national security interests

We expect Russia and China alike to try to protect their national security interests by investing in and acquiring companies and property in Norway.

The use of security-threatening economic means covers a wide range of activities, potentially including the acquisition of property near critical infrastructure, military installations or infrastructure of military significance. Strategically located property could lend itself for carrying out intelligence activities, meaning it may pose a threat to national security.

In other contexts, the acquisition of property may revolve around strategic positioning to gain a foothold or influence over time. For example, in 2024, the government decided that the Søre Fagerfjord property on Svalbard could not be sold without the State's consent. This decision was motivated by the desire to reduce the risk of threats to national security interests. We also see that several properties adjacent to military sites and areas of strategic importance are owned by Russian nationals with ties to the Russian state.

This activity can also be accomplished through participation in procurement processes or investments in or acquisitions of companies that allow new owners access to sensitive technology or information. This can also give states control over companies of importance for national security, or over supply chains, which could create dependencies and be used as leverage. State actors often endeavour to conceal their involvement by employing complicated ownership structures or third parties.

Authoritarian states continue to threaten critics of their regimes

In 2025, several authoritarian states will continue to identify and threaten refugees, dissidents and critics of their regimes who are living in Norway. This happens physically as well as digitally. Some may also be recruited, through intimidation or cultivation, to disclose information about diaspora communities and opposition activities in Norway.

Authoritarian states use transnational repression in the form of pressure, threats and, ultimately, lethal violence to silence criticism of their regimes. Some states use their diplomatic representations to restrict their critics' freedom of expression here in Norway, for example, by monitoring demonstrations. They also use visiting intelligence officers, criminals or infiltrators in diaspora groups for this purpose.

Transnational repression (TNR) refers to states' use of measures against individuals residing in other countries, who are considered a threat against the regime in the executive/responsible state. The purpose of the operation is to undermine or neutralise political opposition and criticism.

States use cyber operations in transnational repression

Oppositionists, diasporas and refugees are subjected to cyber operations by foreign states' intelligence services. For example, cyber actors use surveillance malware or spearphishing operations to compromise individuals. To accomplish the latter, cyber actors use various communication platforms and social media, e.g. LinkedIn and WhatsApp, in addition to traditional platforms such as email and text messaging. Through successful cyber operations, the actor can, for example, gain access to information that enables intelligence services to map networks and movement patterns.


POLITI

Politically motivated violence – extremism

The terrorist threat in Norway is at a MODERATE level. The most serious terrorist threats in and against Norway will continue to come from Islamist extremists and right-wing extremists. Although we believe there is an **even chance** that Islamist extremists and right-wing extremists will attempt to carry out terrorist attacks in Norway in 2025, we consider the threat from Islamist extremists to be the more serious.

This is partly due to more Islamist extremist attack activity in Europe, the fact that the terrorist organisation the Islamic State (IS) intends to carry out more 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 comes primarily from right-wing extremists who participate in transnational digital networks that incite violence.

The common denominator for counter-terrorism is that digital platforms are the main arena for radicalisation and recruitment. We are seeing greater dissemination of extremist content on popular commercial platforms than previously. This adds to the risk of radicalisation and recruitment to extremism in Norway. Radicalisation is continuous, and experience shows that a radicalisation process can be rapid or lengthy. Our concern is that some individuals will translate extreme attitudes into terrorist acts. Within Islamist extremism and right-wing extremism, we see that minors make up an ever-larger proportion of those who are radicalised.

Minors who are radicalised

Throughout the field of counter-terrorism in Norway, we see a growing number of children and young people becoming radicalised. We expect this negative trend to continue. The use of digital platforms by minors in particular contributes to this radicalisation.

Extremist content is readily available on digital platforms. This is where minors consume and distribute extremist material, and the content sometimes incites violence. The dissemination of this type of content on popular commercial platforms like TikTok and Instagram increases the risk of young people in Norway being recruited to extremism.

Last year, far more Islamist extremist terrorist attacks involving minors were carried out or averted in the West than ever before. The perpetrators of right-wing extremism are also getting younger, although it is mainly people over the age of 18 who carry out and plan right-wing extremist terrorist attacks in the West. For minors in general, we see continuing focus on schools as targets. For them, schools are familiar and easily accessible targets, and there are people there who fit their image of the enemy.

Several of the minors who are radicalised face various challenges, including exclusion and mental illness, which make them vulnerable and thus easily susceptible to an extremist message. Interaction with other social actors is therefore particularly important in PST's preventive work with minors.

THE THREAT FROM ISLAMIST EXTREMISM

We consider there to be an **even chance** that Islamist extremism will attempt to carry out terrorist attacks in Norway in 2025.

The threat comes from individuals and networks inspired by the ideology of the Islamic State (IS) and to some extent al-Qaeda. For instance, these individuals participate in digital fora where extremist propaganda is shared, and several of them have ties to extremist networks in Europe. These individuals are mobilised by national as well as international events. The negative trend seen in 2024, featuring more attack activity in the West, is expected to continue. The consequences of Israel's warfare in Gaza are expected to continue to be a radicalising factor. We do not expect Norway to be a priority target for Islamist extremists in 2025. New events, wars and developments outside Norway could affect the threat situation in Norway in 2025. If developments were to result in terrorist organisations mentioning Norway in official calls for terrorist acts, this would have a significant negative impact on the threat situation.

PST considers the threat posed by IS and al-Qaeda to be central, because they are terrorist organisations with an Islamist extremist agenda, and they operate on a global basis. They claim that the West is at war with Islam, both in and outside the West. Western military intervention in Muslim countries and what they perceive to be oppression and violation of Muslims in the West are used to legitimise terrorist attacks. Because Western countries elect their own leaders, the entire population is perceived as responsible. Accordingly, the civilian population also becomes a legitimate target.

Negative trend in international terrorism

PST expects a continued high level of attack activity in Europe from people mobilised by the warfare in Gaza and from people in the IS network. IS has a stronger focus on mounting attacks in the West now than it has had for several years, heightening the terrorist threat in Europe..

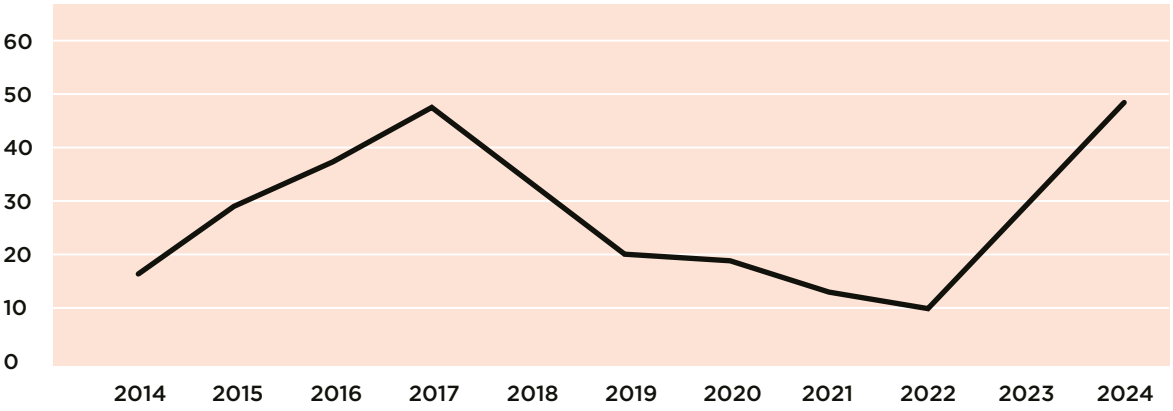
Over the past two years, attack activity has increased significantly, although the vast majority of attack plans are averted by police, and security and intelligence services. In 2024, Islamist extremists carried out nine terrorist attacks in the West. However, at least four times as many attacks were averted. This shows that there has been a sharp rise in the propensity to attack, but also a rise in security and intelligence services' ability to prevent attacks. Most of the attack activity in the West takes place in Europe.

The majority of those arrested for attack activity are individuals who sympathise with Islamist extremist ideology, but are not affiliated with a terrorist organisation. The increased attack activity in Europe in 2024 is attributed in particular to radicalisation as a result of

By extremism, we mean acceptance of the use of violence to achieve political, religious or ideological goals. Extremists accept the use of violence, but do not necessarily engage in violence themselves.

By radicalisation, we mean a process in which a person develops an acceptance of or willingness to actively support or engage in acts of violence to achieve political, religious or ideological goals.

Averted and executed Islamist extremist terrorist attacks 2014-2024



The graph shows averted and executed Islamist extremist terrorist attacks registered by PST in the West over a 10-year period. The West is defined as Western Europe, the USA, Canada, Australia and New Zealand. Graph: Norwegian Police Security Service

Israel's warfare in Gaza and subsequent calls for attacks from IS and al-Qaeda owing to the war.

At the same time, we believe that IS has become more intent on carrying out attacks in the West. IS exploits individuals and networks already located in European countries and can, for example, initiate or pre-approve a terrorist attack carried out by sympathisers. Potential perpetrators who want to carry out terrorist acts in the name of IS also contact IS. This allows perpetrators to receive guidance and practical support for planning attacks.

On several occasions over the past year, European security and intelligence services have averted attack-related activities with ties to IS. The IS branch in Afghanistan and the surrounding area, the Islamic State of Khorasan Province (ISKP), poses the greatest terrorist threat to Europe. At the same time, other IS branches will also try to instigate attacks in Europe, just as IS Somalia attempted to do in Sweden in 2024. However, IS' geographical dispersion across different continents makes it difficult for security and intelligence services to take effective countermeasures. International counter-terrorism operations have not been sufficiently successful in cracking down on those with ties to IS in Africa and Asia. Despite repeatedly losing leaders, the group has managed to expand.

IS propaganda is encouraging sympathisers to travel to the African branches in particular. It is possible that some Norwegian extremists may endeavour to travel as foreign fighters in 2025. However, we expect no major outflow of foreign fighters like the one seen just over a decade ago.

Al-Qaeda continues to prioritise local growth. Al-Qaeda has succeeded in growing in African areas in particular. Over the past year, al-Qaeda has significantly increased its propaganda production, stressing that the acts of war in Gaza must be avenged, and promoting Israeli and American interests as targets for attacks.

The threat situation in Norway is impacted by international developments

We are aware of links between individuals in Norway and different extremist networks in Europe that have ties to IS branches in Africa and Asia. Since IS is increasingly intent on targeting the West, such contact gives rise to concern. Norwegian contacts may be asked to facilitate or, in the worst-case scenario, to carry out terrorist acts.

Our assessment is that the warfare between Israel and Hamas in Gaza contributed to radicalisation in Norway in 2024. IS and al-Qaeda are both exploiting the war for the purpose of recruitment and radicalisation. Al-Qaeda has increased its propaganda production considerably over the past year, emphasising that the acts of war in Gaza must be avenged. Both terrorist groups call for attacks on Israeli, Jewish and American targets, although other Western targets such as arms manufacturers and churches have also been mentioned in this context.

We expect the warfare in Gaza to contribute to further radicalisation and to continue to have an adverse impact on the terrorist threat from Islamist extremists in 2025. This assessment is based on the fact that the warfare and the suffering are of vast proportions and have attracted a great deal of attention. Our assessment is that terrorist organisations will try to continue to exploit this in future.

The situation has been unclear since the fall of the Bashar al-Assad regime in Syria at the beginning of 2025. From the perspective of counter-terrorism, the possibility of IS gaining momentum in Syria is of particular concern.

The terrorist threat in Norway could deteriorate rapidly if international radicalisers or terrorist groups were to direct their attention toward the situation in Norway. In recent years, for example, traditional and social media have devoted little attention to Koran burnings in Norway. That being said, the threat situation in Norway could change rapidly if Koran desecrations here were to attract more media attention, or if fake news or misunderstandings about this were to gain traction. Other incidents or actions perceived as offending Islam in Norway could also exacerbate the threat.

Terrorist financing

We are of the opinion that monetary transactions are carried out from Norway for the purpose of supporting terrorist activities in other countries. To a greater extent than before, the transactions are carried out using service providers or financial institutions that are not required to report to the Norwegian authorities. For example, cryptocurrencies and foreign financial institutions that recruit customers via the Internet are being used. We expect this trend to continue, and we expect to see a constantly changing market for payment services and transfers.

A new generation of Islamist extremists

In Norway, we are currently seeing the contours of new networks of young Islamist extremists. Network-building primarily takes place online, and the new ones have little contact with previously known extremist networks.

Several Islamist extremists in Norway take part in transnational digital networks that communicate via encrypted platforms. In this way, young people who take part in these networks are influenced by the same issues as are of concern to Islamist extremists in other countries.

In particular, we are seeing an increase in minors and young adults consuming and distributing Islamist extremist material on digital platforms. The content includes the glorification of violent jihad and utterances that can be construed as support for IS or al-Qaeda.

The negative trend of more minors and young adults consuming extremist material is seen against the backdrop of reactions to Israel's warfare in Gaza and the greater dissemination of extremist content on digital platforms. IS and al-Qaeda both focus on propaganda to convey their message, recruit and issue calls for attacks.

The dissemination of this type of content on popular commercial platforms like Instagram and especially TikTok, heightens the risk of young people in Norway being recruited to Islamist extremism. The propaganda is easily accessible and produced in a format that appeals to many young people. Accordingly, we expect increased radicalisation online, mainly among young people.

The distinction between digital and physical networks will remain fluid. Radicalisation will take place in both arenas, and they have the potential to reinforce each other. In physical networks, we expect radicalisation to take place between friends, and in families, schools, religious arenas and prisons.

Many extremists consume propaganda from both IS and al-Qaeda. We are also seeing more dated propaganda being distributed yet again. We expect that artificial intelligence (AI) will be used to a greater extent in propaganda production, for example, to make efficient translations into many languages, to generate images and video, and to make fake images or videos.

Sympathisers will continue to produce terror-inducing propaganda featuring high-quality graphics and clear messages that are easy to understand. We expect that increasingly more extremist material will be translated into Norwegian, making the propaganda more accessible to Norwegian users.

«In particular, we are seeing an increase in minors and young adults consuming and distributing Islamist extremist material on digital platforms.»

Simple, easily accessible means of attack

Any Islamist extremist terrorist act in Norway will most likely be carried out by one or a few perpetrators who are inspired by the ideology of IS or al-Qaeda. The perpetrators will often be in contact with other extremists prior to the terrorist act, either digitally or physically.

We continue to expect attackers to use simple, readily available means of attack such as slashing or stabbing weapons, arson or motor vehicles. However, attacks that have been averted indicate that Islamist extremists prefer to cause mass casualties by using improvised explosive devices and firearms. Firearms include pistols, shotguns and rifles, procured legally or illegally. While improvised explosive devices (IEDs) are probably relatively easy to build, they still have the potential to cause significant damage. In future, technological developments may affect the choice of means of attack. This could stir up more interest in 3D-printed firearms and drones as means of attack. For example, we see that drones are increasingly being used in wars and conflicts, which could inspire attack planning in Norway.

Last year, minors carried out more terrorist attacks in the West than ever before. In addition, minors were involved in many attacks that were averted. Before 2024, minors were rarely able to carry out attacks, and only a few averted attacks involved minors. Even though we expect minors and young adults to take part in attack activities again in 2025, the age range of the perpetrators is expected to be wider than this group alone.

Israeli, Jewish and Christian targets more exposed

Based on propaganda and ideological guidelines from al-Qaeda and IS, we expect random civilian, police and defence personnel, as well as institutions or individuals perceived to insult the religion of Islam, to be relevant targets for Islamist extremist attack activities. In addition, meeting places for LGBT+ people and religious meeting places have become more relevant as targets in recent years.

Throughout 2024, Islamist extremist propaganda focused to a greater extent than before on Israeli and Jewish targets, although Christian targets have also been emphasised. Last year, we saw several attacks carried out and averted in the West against precisely these target categories. Our assessment is therefore that the focus on Jewish and Israeli targets has been markedly intensified, and that they have become established as priority target choices for Islamist extremism.

The terrorist threat against Jewish and Israeli targets in Norway has grown worse over time. This trend is expected to persist in 2025, as Jewish and Israeli targets have become more important to Islamist extremists, due in particular to Israeli warfare in Gaza. Photo: Javad Parsa/NTB

THE THREAT FROM RIGHT-WING EXTREMISTS

We still believe that there is an **even chance** that right-wing extremists will attempt to carry out terrorist acts in Norway in 2025.

The terrorist threat from right-wing extremists in Norway derives primarily from right-wing extremists who participate in transnational digital networks that incite violence. In our experience, individuals in these networks may develop the ability and volition to commit terrorist acts.

Norwegian right-wing extremists are united by the idea that the state and the people should be a homogeneous unit, based on a shared understanding of a 'white race' or 'white' cultural characteristics. Right-wing extremists believe that those who do not belong to this community pose a threat. Further, today's right-wing extremism is based on conspiracy theories that postulate that the 'white race' or 'white culture' is on the brink of being obliterated. This perceived existential fear makes right-wing extremists believe that violence is legitimate when it is to prevent annihilation.

Transnational networks have a negative impact on the threat situation

In recent years, the development and activities of transnational digital networks have been a key driver behind the terrorist threat from right-wing extremism in Norway. This applies in particular to networks that incite violence. In that context, participants are encouraged to commit terrorist acts. The goal is often mass murder or targeted killings of people who fit the image of enemies of right-wing extremists. We know that Norwegians participate in this type of network.

Gross depictions of violence, propaganda and tributes to previous terrorist attacks are shared in the transnational networks that incite violence. Participants in this type of network can also come into contact with like-minded individuals in other Western countries, thereby becoming part of an international network of right-wing extremists. This means that people far beyond our borders can radicalise and recruit people to right-wing extremism in Norway.

We are concerned that Norwegian individuals in these networks may develop the desire and ability to commit terrorist acts themselves. Consequently, the participation of right-wing extremists in Norway in such networks has a negative effect on the Norwegian threat situation.

Some transnational violence-inciting networks are also accelerationist. Right-wing extremists in such networks still constitute a particular concern since these networks argue for the urgency of carrying out terrorist attacks. Accelerationism has been a key ideological motivation for several right-wing extremist terrorist attacks in recent years.

It is important to emphasise that only a small number of those who participate in right-wing extremist networks will attempt to commit terrorist acts. Despite the fact that individuals may threaten to commit terrorist acts, our experience is that very few translate their words into action. It will continue to be challenging to identify and assess who will move on from consuming and publishing content that incites violence to actually attempting to commit a terrorist act.

A transnational network consists of individuals and/or groups located in different countries. The networks operate in digital and physical arenas alike, and the degree of leadership structure can vary. Participants can act anonymously or with a known identity.

Accelerationism is a right-wing extremist doctrine. The idea that a 'race war' is imminent is a major factor, as is the idea that time is of the essence when it comes to bringing about the collapse of society while the 'white race' still has a demographic majority in the West. Terrorism is highlighted as an important tool for destabilising society and initiating the 'race war'.

Digital platforms are the main arenas for radicalisation and recruitment

Large parts of today's right-wing extremist activity take place in digital arenas. We expect that digital platforms will continue to be the main arenas for radicalisation and recruitment to right-wing extremism in Norway.

The radicalisation process differs from one person to the next, and there are many paths into and out of a radicalisation process. In the digital space, however, our experience is that a typical radicalisation path goes from open social media, such as TikTok and Instagram, to digital platforms that offer encrypted communication. The content on encrypted digital platforms is often more violent and transgressive. For some, social media serve as digital highways for radicalisation.

Right-wing extremist content is readily available on open digital platforms. Social media algorithms and today's user-friendly technology make it easy to consume, share and create propaganda. For example, we see that TikTok is a gateway to right-wing extremist content for many.

In addition to transnational networks, Norwegian right-wing extremist digital networks are also a source of concern as regards radicalisation. Here, too, one can be exposed to right-wing extremist ideas, share propaganda and, not least, make contact with like-minded individuals in Norway.

Even though digital networks are the main arenas for radicalisation and recruitment, there will still be activities in physical spaces. We are aware that the right-wing extremist phenomenon 'Active Clubs' have established a presence in Norway. Active Clubs are a network of smaller local groups that build a sense of community through right-wing extremist ideology and training. We are not especially concerned about terrorism in relation to Active Clubs in Norway, but we do worry that such physical arenas could lead to individuals becoming radicalised and building networks with other like-minded people.

We expect Norwegian right-wing extremists to continue to draw ideas and inspiration from various arenas. This could be from other ideological movements, but it could also refer to communities and environments without a clear ideological direction. The use of popular cultural references, along with right-wing extremist symbolism, is also an enduring trend. The fact that right-wing extremists adopt symbols and ideas from different communities and environments means that right-wing extremist ideas may appeal to more people than before. In recent years, this trend has made the threat from right-wing extremism more unpredictable and complex.

The image shows a hypothetical but realistic example of incitement to violence and jargon in right-wing extremist digital networks. Illustrated by PST, the image shows a chat log on the instant messaging service Telegram. The user is not real. Illustration: Norwegian Police Security Service

Many reasons for radicalisation

Those radicalised to right-wing extremism in Norway come from different walks of life, vary in age, and come from all over the country. In other words, radicalisation and recruitment to right-wing extremism are a nationwide challenge.

There are many different reasons why people seek out and participate in right-wing extremist networks. We see that the visual and aesthetic expression of right-wing extremist propaganda continues to appeal to those recruited to right-wing extremism. Some participate in right-wing extremist networks to offset various vulnerabilities, e.g. mental illness, loneliness or the search for social fellowship. Some are ideologically curious, while others are looking for entertainment or are fascinated with violence. Some will be attracted to right-wing extremist networks in order to push limits through politically incorrect communication.

Over time, we have noted that a proportion of those who are radicalised to right-wing extremism today are minors and young men. In the radicalisation process in respect of this age group, we see that the use of digital platforms plays a key role. We expect the trend towards and challenges in relation to minors becoming radicalised to continue.

Although there are a number of reasons why people join right-wing extremist networks in the first place, repeated exposure to dehumanising, one-sided ideas can allow the right-wing extremist message to gain momentum. In our experience, a radicalisation process can take place quickly. Our concern is that some people will translate right-wing extremist attitudes into right-wing extremist terrorist acts.

Right-wing extremism continues to inspire plans for attacks in the West

In our experience, there are a variety of events and driving forces that can radicalise and ultimately mobilise right-wing extremists to attempt to commit terrorist acts. These may include social development and current events at the local, national and international levels. In addition, personal circumstances can have a mobilising effect. The social events perceived as driving forces for radicalisation and terrorist planning are highly individual.

However, there are some general trends and events that may affect the terrorist threat posed by right-wing extremism in Norway. Generally speaking, these are trends that may support right-wing extremists' conspiracy theories that the 'white race' is under threat. For many right-wing extremists, actual or perceived increases in non-Western immigration to the West will be one such mobilising factor. Increasing immigration to Norway from countries in the Middle East and Africa due to ongoing wars and humanitarian crises is one example. For others, the perception that Norwegian society is in moral decline will be a mobilising factor. For right-wing extremists, this may involve Norwegian society's acceptance of liberal gender identities and the continued normalisation of LGBT+ rights.

We also see that right-wing extremist terrorist attacks that have been carried out continue to be an important source of inspiration and a driving force for right-wing extremists. This applies to attacks that took place several years ago as well as to recent right-wing extremist terrorist attacks. Compared with 2019, there have been fewer terrorist attacks carried out in the West since 2020. However, a significant number of right-wing terrorist attacks are still being averted. The fact that the majority of right-wing extremist terrorist attacks in the West are averted helps to prevent new terrorist attacks that have been executed from inspiring new terrorist plans. Meanwhile, this shows that the terrorist threat from right-wing extremists in the West and Norway is real.

In terms of international events, neither the war in Ukraine nor conflicts in the Middle East have led to more right-wing extremist radicalisation or attack activity. One reason for this is that the wars do not carry clear ideological significance for Norwegian right-wing extremists. That being said, some Norwegians with ties to right-wing extremism have participated in the war in Ukraine. We remain concerned that these individuals are acquiring knowledge and experience involving means of attack, seeing a lower threshold for violence, developing their extremist contact networks, and becoming more vulnerable due to war trauma.

The goal is mass murder of people who fit the image of the enemy

A right-wing extremist terrorist attack in Norway will most likely be a mass casualty attack or a targeted assassination. The attack will target individuals, groups or institutions that fit the description of the enemy of right-wing extremists. We still expect a right-wing extremist terrorist attack to be carried out by a single perpetrator, and the perpetrator will likely be part of a right-wing extremist network.

For Norwegian right-wing extremists, the image of the enemy will continue be diverse, including individuals with a non-western appearance, Muslims, Jews, non-western immigrants, politicians and representatives of the Norwegian authorities, LGBT+ people, conventional media and left-wing extremists in Norway. Right-wing extremists believe these people threaten the survival of the 'white race' or 'white culture'.

The choice of targets for a potential terrorist attack may be influenced by how accessible a target is, its degree of symbolic value, and the extent to which it is protected by security measures. Right-wing extremists will often prefer targets with few or no security measures and featuring a high density of people considered to be enemies. This is because right-wing extremists often aim at carrying out attacks that lead to a high death toll. This type of attack is one of the prerequisites for achieving high status in right-wing extremist circles.

Because a high death toll is often a goal for right-wing extremists, firearms and simple improvised explosive devices (IEDs) are often preferred by right-wing extremist perpetrators. At the same time, the choice of means of attack is influenced by factors such as the actor's target, skills, network and, not least, the availability of the means of attack. This means that a number of different means of attack are possible, including knives, slashing and stabbing weapons, vehicles and incendiary agents.

Access to new technology can also influence the choice of means of attack, e.g. the use of drones or 3D printing technology. Among right-wing extremists, we see an increased interest in 3D-printed firearms. However, it is still demanding to make functional, effective high-capacity 3D-printed firearms.

Nevertheless, we expect that developments in and the availability of 3D technology will lead to more interest in such firearms.

Threats to dignitaries in Norway

Dignitaries are members of the Royal House of Norway, the Norwegian Parliament, the Government and the Supreme Court, as well as representatives of similar bodies in other countries who are present in Norway.

We consider it **unlikely** that anyone will try to carry out serious acts of violence against dignitaries in Norway in 2025. PST expects that dignitaries will be subjected to smears, and in some cases threats.

We expect more smears and threats when controversial issues and political differences attract a great deal of attention, especially in connection with elections to the Storting (Norwegian Parliament) and the Sámediggi (Sámi Parliament) in Norway. Smears and threats against dignitaries pose an ongoing challenge to our democracy.

Dignitaries will continue to be vulnerable targets for foreign states' intelligence activities.

Increase in threats and smears against dignitaries over time

PST considers it **unlikely** that anyone will attempt to carry out serious acts of violence against dignitaries in Norway in 2025. We expect smears and threats against dignitaries that attract a great deal of media attention and are linked to controversial issues. Some of them will be subjected to confrontations that may be perceived as threatening.

Large numbers of smears and threats can be perceived as threatening and trigger restrictions on how certain dignitaries will carry out their democratic duties. Some will opt to moderate their views, refrain from speaking out, or resign from their positions in response to the strain. This is why threats and smears against dignitaries represent a serious challenge to democracy.

Over time, we have seen an increase in the scope of threats against Norwegian dignitaries. The number of people making threats has also increased.

Although very few of those who make threats genuinely intend to commit violence, we must assume that certain individuals will try to make good on their threats. Large numbers of threatening utterances online can also serve to generalise and legitimise violence against dignitaries. This can influence and inspire individuals to commit violent acts.

.

Norway will hold parliamentary elections in the autumn. PST expects dignitaries to receive more smears and threats when controversial issues and political differences attract more attention. Image from March 2023, when President of the Norwegian Parliament Masud Gharahkhani met with female politicians who have experienced smears and threats.

L. to r. Hanne Tollerud, Anita Ihle, Masud Gharahkhani and Lan Marie Berg.

Photo: Javad Parsa/NTB

Position and individual factors affect the threat

All dignitaries have complex and different threat profiles. Threats are influenced by the dignitary's position, individual factors, media exposure and the extent to which the dignitary is associated with controversial issues.

Members of government and party leaders will be more exposed to threats than less high-profile politicians due to their national responsibilities and visibility in the media. Ties to fringe parties and minority backgrounds may add to the volume of smears and threats. Female dignitaries are more likely than males to receive sexualised threats.

Controversial issues involving the Royal House of Norway will occasionally lead to more unwanted attention, smears and potential threats against members of the Royal House.

The threat situation for foreign dignitaries in Norway will to a greater extent be affected by international factors. Some are more exposed to threats than others due to conflicts in their home countries. One example is the heightened threat against Israeli and Jewish targets in Norway owing to the warfare between Israel and Hamas in Gaza.

Threat actors motivated for personal reasons rarely genuinely intend to commit violent acts

Threat actors motivated by personal reasons are expected to account for the majority of smears and threats against dignitaries. They will primarily be driven by dissatisfaction with their own life situation or a particular issue and, in some cases, they may have fixations on dignitaries. There will often also be significant vulnerability factors, particularly mental illness and substance abuse. Consequently, Norway's national capacity to deal with individuals with mental issues or substance abuse challenges will have an impact on the scope of threats against dignitaries.

Personally motivated actors will often make threats and smears, and be the source of unwanted attention online or by phone. In 2024, for example, a person was convicted of threatening to commit an armed 'live-streamed' attack on the Norwegian Parliament on Facebook.

Personal appearances and confrontations can also occur. The motive will rarely be to harm a dignitary, but rather to achieve change or help improve their own circumstances of life. It may also be to vent frustration or anger by directly approaching someone they hold responsible.

Dignitaries who fit extremists' image of the enemy

The Norwegian authorities will continue to be among the main enemies for extremists. However, extremists' expectations of security measures around dignitaries may deter them, causing them to choose other, more easily accessible targets.

Right-wing extremists see the authorities as traitors to the country, accusing them of paving the way for the annihilation of the 'white race'. All politicians are viewed as representatives of the elite and the corrupt state. For Norwegian right-wing extremists, the political left, especially the Labour Party, plays a central part in these conspiracy theories. Perceived facilitation of non-Western immigration and perceived negative consequences of immigration will continue to mobilise hatred of government in right-wing extremist circles.

Extreme Islamists advocate a world view that sees Western countries as oppressing Muslims and waging war with Islam. As a result, extremists may also consider the Norwegian authorities to be their enemies. At present, however, other targets appear to be more prominent in Norway. This could change quickly, e.g. if representatives of the Norwegian government were to be seen as insulting Islam or supporting military warfare against Muslims, or if Norway were mentioned in official terrorist calls from terrorist organisations.

Dignitaries may be exposed to intelligence activities and influence operations on the part of foreign states

In 2025, foreign states will continue to seek information about Norwegian political processes that may affect their interests. This applies to Russia and China in particular. Norwegian politicians, and people working close to them, may therefore be targets for foreign states' intelligence activities.

We expect dignitaries to be exposed to cyber operations, not least in the form of phishing. Phishing attempts are often initiated via email, social media, text messages or other communications platforms. The aim is to trick the recipient into downloading malware or providing log-in details that can be used to compromise the victim. This may result in a foreign state actor gaining access to the dignitary's personal and professional correspondence, calendar and contacts. Such sensitive information can potentially be used in intelligence activities and influence operations alike.

Dignitaries have symbolic value in foreign states' influence operations because they represent Norwegian politics or Norwegian public opinion. State actors can try to influence the public's trust in politicians and political processes in Norway, e.g. through smear campaigns or disinformation. Influence from foreign states can ultimately lead to greater polarisation and add to the volume of threats and smears against politicians.

Threats in connection with the Norwegian parliamentary and Sámi parliamentary elections in 2025

Several countries in Europe have registered an increase in the number of threatening acts and direct attacks against politicians, especially in connection with elections.

In the period before, during and after the Norwegian parliamentary and Sámi parliamentary elections in 2025, the country's politicians and the issues they champion will receive significant media coverage. We expect more smears and threats when controversial issues and political differences attract a great deal of attention. Frequent public appearances and other election campaign activities will make politicians more accessible and thus more vulnerable to confrontations.

The issues that exacerbate threat activity against dignitaries will be influenced by economic cycles, international development trends and political decisions. This might involve issues perceived as restricting people's personal finances or freedoms, perceived injustice, or conflicts in encounters with the public sector. Matters in which dignitaries are portrayed in a negative light can also trigger contempt for authority, distrust and conspiracy thoughts. This can have a negative impact on the threat against dignitaries.

Politicians and other targets related to the parliamentary elections can potentially be terrorist targets for extremists who see government officials and politicians as the enemy.

Some state actors may also use the run-up to the election as an opportunity to lobby politicians and the population in a direction that serves their interests.

Politiets sikkerhetstjeneste
pst.no