PST

National Threat Assessment

2026

Aim of the National Threat Assessment

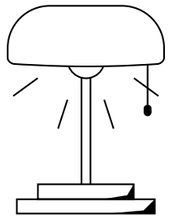
The National Threat Assessment (NTA) outlines the expected threats Norway faces from state actors and extremist groups, including those targeting dignitaries, over the coming year. Its aim is to establish a shared national understanding of the threat to national security.

The NTA also seeks to help other societal actors protect themselves from threats by providing decision-making support for organisations' protective security efforts. National preparedness is a collective responsibility, and both public and private organisations have a role to play in this.

The NTA also aims to increase vigilance in society. Reports from the public of suspicious activity play a crucial role in deterring and preventing threats to Norway. We encourage anyone with a concern they believe PST should be aware of to contact us. Reporting a concern to PST is straightforward.

Report a concern

pst.no/tips-oss



Contents

Introduction

Norway is facing its most serious security situation since World War II.

Beate Gangås
Director General PST

Photograph
Norwegian Police Security Service

Norway is facing its most serious security situation since World War II. The National Security Strategy presented by the Norwegian government in May 2025 sets out three key priorities in response to the heightened security situation: rapidly strengthen defence capability, increase the resilience of Norwegian society and strengthen economic security. The strategy document notes that delivering on these priorities requires a concerted effort across the whole of society.

The role of the Norwegian Police Security Service (PST) is to understand, communicate and counter the most serious threats to national security. In the National Threat Assessment, we outline the threats most likely to feature prominently in 2026. Along with the annual threat and risk assessments of the Norwegian Intelligence Service (NIS) and the Norwegian National Security Authority (NSM) ('Fokus' and 'Risiko' respectively), PST's national unclassified threat assessment helps ensure a shared picture of the situation across institutions and the wider public.

With foreign states conducting intelligence operations and employing hybrid tactics in Norway to undermine our resilience, protective security, intelligence and situational awareness are vital. We all need to remain vigilant and be aware that such threats could occur in the course of our daily lives.

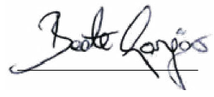
The terrorism threat landscape is more diffuse and complex than before. This is compounded by the possibility that state actors could orchestrate terrorist acts in Norway through proxy actors, making it more challenging to uncover potential terrorist activity. The most serious terrorism threat continues to come from Islamist and right-wing extremists. Anti-government sentiment is also contributing to radicalisation. Levels of ideological commitment vary, and in some cases a fascination with violence can be a pathway into extremist ideology rather than a consequence of it. The digital space remains the primary sphere for radicalisation, with the internet facilitating connections across national borders. We expect the trend of radicalisation among minors and young people to continue.

Preventing extremism and safeguarding democracy require coordinated efforts from multiple actors. I would like to extend my thanks to everyone who has worked with PST to prevent serious threats.

Maintaining public trust is vital to PST's work. The public must feel able to come forward with concerns. In 2025, PST achieved its highest-ever ranking in a reputation survey of public sector organisations. We aim to be worthy of that trust. It is our responsibility to determine whether a real threat exists, and PST staff take this duty very seriously.

PST characterises the threat landscape as serious. We aim to provide as much concrete information as possible, within the limitations of protecting classified material. Transparency is important for PST. Threats do not vanish simply because they are not discussed; on the contrary, they may continue to evolve unchallenged.

A shared picture of the threat landscape strengthens our resilience in troubled times.



Beate Gangås
Director General PST

Applying the NTA to risk assessments

Risk can be assessed in a number of ways. In our approach, a risk assessment within an organisation is an overall assessment of the *assets* to be protected, relevant *threats* and existing *vulnerabilities*.

Systematic mapping and assessment of assets provides an organisation with a firm foundation for evaluating which threats and vulnerabilities are relevant, and for understanding their potential impact on those assets. The NTA outlines a range of potentially relevant threat actors, providing a reference point to inform decision-making in threat assessments. Organisations also need to consider other risks that may affect them, including criminal activity and other types of adverse events.

Assessing vulnerabilities entails identifying weaknesses that could expose an organisation to relevant threats. This assessment should also consider external dependencies within the value chain, including subcontractors such as key card manufacturers and suppliers of information management systems or transport services.

The overall assessment of assets, threats and vulnerabilities provides the basis for identifying measures to reduce both the likelihood and consequences of adverse events. Implementing such measures can help organisations achieve an appropriate level of security.

Organisations with complex and diverse portfolios should adopt a structured approach to identifying and describing relevant assets, threats and vulnerabilities.

What is meant by assets, threats and vulnerabilities?

Asset
Assets can range from national security interests to an organisation's operational priorities. Examples include life and health, the natural environment, intangible assets, or simply the organisation's operational capability. A common feature of all assets is that any loss or temporary unavailability would have an adverse impact on the organisation or other parties.

Threat
A threat is an intention that could lead to an adverse event. For something to be considered a threat, the actor responsible must have the capability to cause the loss or temporary unavailability of one or more assets.

Vulnerability
A vulnerability is a weakness that limits an organisation's ability to withstand an adverse event or to subsequently resume normal operations. In other words, vulnerabilities are weaknesses that increase an organisation's exposure to a threat.

Probability terms used in assessments of politically motivated violence

PST uses a set of standardised probability terms to describe the probability of politically motivated violence (extremism). These terms ensure consistency in our threat assessments and reduce the risk of misunderstandings.

Standardised term	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

PST's terrorism threat scale

The terrorism threat scale represents PST's overall assessment of the terrorism threat landscape in Norway. While probability terms indicate the likelihood of a terrorist attack, the scale reflects the severity of the situation.

The scale consists of five levels. When establishing or adjusting a level, assessments are based on a qualitative threat assessment, taking into account how relevant factors, actors and events affect the situation in Norway. We also consider:

- the severity and potential damage of a possible terrorist act
- the reliability of intelligence and the extent of gaps in intelligence concerning relevant threat actors
- the authorities' ability to implement countermeasures before any threats are carried out

The five threat levels are intended to provide a simple description of a complex situation.

Level	Term and meaning
5	**Critical** PST's assessment is that a terrorist attack is imminent, or a terrorist attack has been carried out and more may follow.
4	**High** PST's assessment is that one or more persons have specific, realistic plans and are taking active steps to carry out terrorist attacks, and/or that multiple factors heighten the terrorism threat.
3	**Moderate** PST's assessment is that one or more persons intend to carry out a terrorist attack, but that they have not taken active steps or devised realistic plans, and/or that some factors heighten the terrorism threat.
2	**Low** PST's assessment is that there are few people who want to carry out a terrorist attack and/or that few factors heighten the terrorism threat.
1	**None** PST's assessment is that no one wants to carry out a terrorist attack, and there no factors that heighten the terrorism threat.

Brief synopsis of the threat landscape for 2026

The threat from state actors

- The overarching interests and activities of state actors in Norway are expected to remain unchanged in 2026.
- The tense geopolitical situation in Europe means that Russian intelligence has several areas of interest in relation to Norway and other NATO countries. Given the increase in military targets on Norwegian soil, the stronger allied presence, and additional military exercises, we anticipate heightened activity from Russian intelligence services.
- Russian intelligence may see benefit in carrying out sabotage operations on targets in Norway in 2026.
- We expect an increase in Russian cyber operations, influence operations and attempts to recruit sources via digital platforms in 2026.
- Chinese security and intelligence services have enhanced their ability to conduct intelligence operations in Norway, including cyber operations and human intelligence collection.
- In 2026, China will collect intelligence, reconnoitre Norwegian digital infrastructure and threaten groups and individuals to prevent them from criticising the Chinese Communist Party.
- The primary intelligence threat from China is in the cyber domain.
- We expect Iranian intelligence and security services to conduct intelligence and influence operations in Norway in 2026.
- The Iranian regime may also attempt to target Western interests through damage to property, targeted assassinations, terrorist acts or destructive cyber operations.
- Iran uses proxy actors to carry out operations in the West. This could include Swedish criminal networks with a presence in Norway.

Politically motivated violence

- We expect a continued high level of terrorist activity by Islamist extremists in the West.
- The Islamic State (IS) and al-Qaida are primarily seeking to inspire sympathisers to carry out terrorist acts in the West.
- Individuals in Norway will maintain links to foreign Islamist extremist networks.
- Norway is not regarded as a major enemy by IS or al-Qaida, but occupies a central place in the enemy perception of Norwegian Islamist extremists.
- Right-wing extremist terrorist activity in the West is also expected to continue. The number of minors involved in terrorist attacks in the West increased significantly in 2025.
- Many of those radicalised into right-wing extremism are inspired by violent extremist ideas with no clear ideological basis.
- Digital platforms remain a key sphere for recruitment and radicalisation.
- The challenge of radicalisation among minors and young adults is expected to continue in 2026.
- Vulnerable individuals who become radicalised may decide to carry out a terrorist act. Personal factors, such as mental health challenges, social exclusion or life crises, can significantly increase this risk.

The threat to dignitaries

- It is unlikely that dignitaries in Norway will be subjected to serious acts of violence, but they will be exposed to intelligence activity, digital threats and harassment.

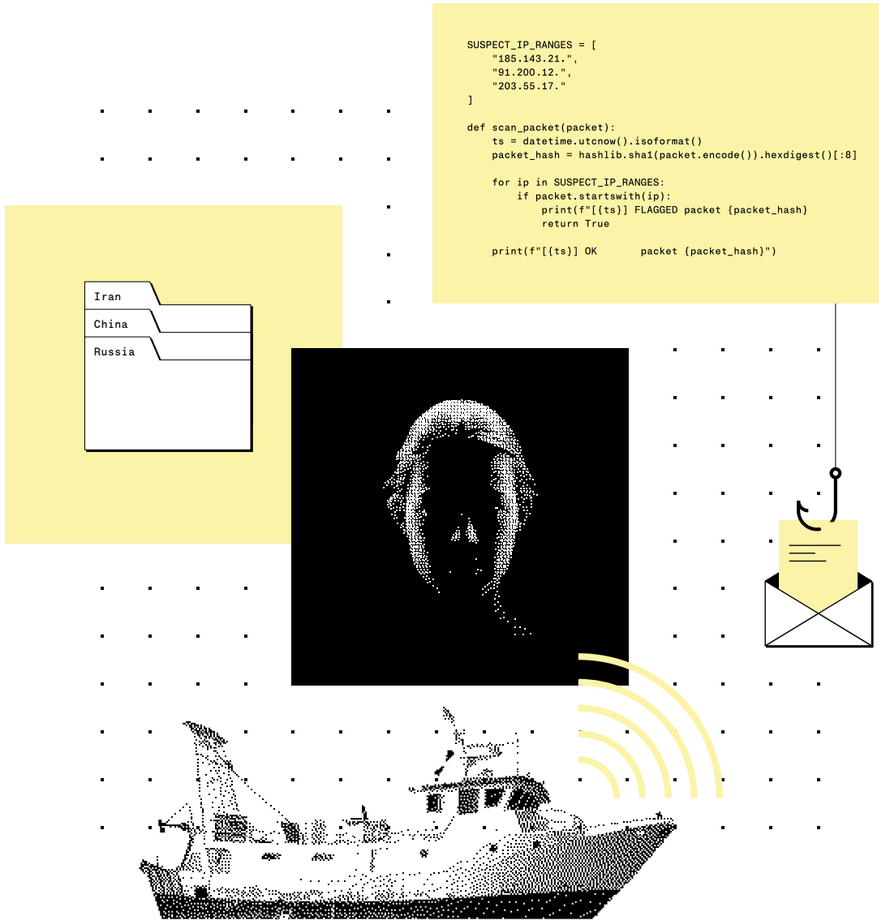


Illustration
Getty / Dinamo Design

Chapter 01

The threat from state actors

The threat landscape in Norway is complex and is shaped by a range of domestic and international factors. The security situation is serious and marked by considerable uncertainty. This is reflected in our assessment that the threat posed by state actors in Norway in 2026 remains substantial.

We expect Russian intelligence services to increase their activity in Norway in 2026, with a continued focus on military targets and allied exercises, Norway's support for Ukraine, and operations in the High North and the Arctic region. Russia is likely to employ a wide range of methods, including influence operations, sabotage, recruitment of human intelligence sources, and intelligence activity on civilian vessels.

The intelligence threat from China is also substantial. Chinese security and intelligence services have improved their ability to operate in Norway through cyber operations and human intelligence collection. Iranian intelligence services are also expected to carry out operations in Norway in 2026.

While PST continues its focus on Russia, China and Iran, developments in the geopolitical situation may impact on which state actors operate on Norwegian soil. A range of factors, including geopolitical rivalries, may also give rise to threats to Norway from countries not addressed in this NTA.

This chapter is divided into two main sections.

The first focuses on **threat actors**, specifically Russia, China and Iran. This section outlines developments in the threat from these countries over the past year and identifies the targets that are expected to be particularly exposed in 2026.

The second section examines **six key methods** that state actors (including the three already mentioned) may employ in Norway. These six methods are:

- cyber operations
- recruitment of human intelligence sources
- transnational repression
- influence operations
- unlawful procurement of sanctioned and export-controlled technology
- economic activity that poses a threat to national security

The key threat actors

Russia

Russia continues to focus on military targets and Norway's support for Ukraine

The tense geopolitical situation in Europe has resulted in Russian intelligence showing increased interest in Norway and other NATO countries. Russian intelligence services have been closely monitoring military targets and allied activities and capabilities in Norway for many years. The presence of additional military targets on Norwegian soil, combined with a strengthened allied presence and military exercise activity, is expected to result in increased Russian intelligence activity. Russia reconnoitres Norway's critical infrastructure and identifies vulnerabilities. This information can subsequently be used in intelligence, influence and sabotage activities. In the worst case, Russia could use this information to its advantage in a potential armed conflict.

The presence of additional military targets on Norwegian soil, combined with a strengthened allied presence and military exercise activity, is expected to result in increased Russian intelligence activity

Norway's support for Ukraine will continue to shape the threat from Russian intelligence and influence operations. The targets of this activity include the Norwegian Armed Forces and a range of public and private actors, particularly with regard to information on military support and civilian aid, such as Norwegian deliveries of weapons and other materiel to Ukraine.

In addition to collecting intelligence, Russian intelligence and security services are likely to try and disrupt or obstruct these efforts. Russian influence operations may also target political decision-making and public opinion in Norway with a view to weakening support for Ukraine.

Russia employs a wide range of methods

Sanctions imposed in response to Russia's full-scale war against Ukraine have curtailed Russian intelligence's ability to operate on Norwegian soil. Since 2022, Norwegian authorities have reduced the number of Russian intelligence officers operating under diplomatic cover. Nevertheless, diplomatic channels remain an important platform for Russian intelligence. Stricter entry rules for Russian nationals and restricted access to Norwegian ports have curtailed Russian intelligence services' ability to conduct certain types of intelligence activity.

Norwegian countermeasures, along with heightened public vigilance, are forcing Russian intelligence services to find new ways to collect intelligence. They employ a wide range of methods, which are continuously being adapted and refined. In 2026, an increase is expected in cyber operations, influence operations and attempts to recruit sources via digital platforms.

Russian intelligence is also expected to expand its presence on Norwegian territory in 2026. Intelligence officers under diplomatic cover will recruit sources and engage in intelligence collection, while visitors to the country may also be used for intelligence and influence operations.

We are increasingly concerned that Russian intelligence and security services are trying to recruit Ukrainian refugees in Norway to provide information or carry out other unlawful activities on their behalf. Efforts are primarily aimed at Ukrainian nationals, who can be pressured or threatened into cooperating, for example through threats involving family members back home or property in Russian-occupied areas of Ukraine. Russian intelligence and security services may also offer incentives or operate covertly, whereby those recruited may not be aware that they are in fact assisting Russian intelligence and security services.

With approximately 100,000 Ukrainian refugees in Norway, recruitment attempts by Russian intelligence and security services are expected to present a major challenge.

Sabotage aimed at creating unrest and exerting influence

Russian intelligence may see benefit in carrying out sabotage operations on targets in Norway in 2026. The most likely targets are property and logistics infrastructure associated with support for Ukraine, but civilian infrastructure may also be affected. The aim would be to create social unrest and reduce the capability and willingness to support Ukraine. Sabotage may also be used as a tool of influence.

The geopolitical situation and the need to expand the range of operational methods have increased Russian intelligence services' risk appetite. In recent years, we have observed several instances of sabotage and disruptive activity in Europe, with a slight decline in 2025. Such activity is often carried out by **proxy actors** and involves attempts to destroy or severely disrupt targets of societal importance. It may also include less severe incidents, such as damage to property or spreading propaganda, aimed at creating social unrest.

Proxy actors are individuals or organisations with no formal ties to intelligence and security services or other government authorities, who knowingly or unwittingly carry out activities on behalf of, or in support of, the authorities. These activities can be politically, ideologically or financially motivated.

Russian crews carry out intelligence activity on civilian vessels

Norway's coastal and maritime zones are of strategic interest to other states. In 2026, Russian intelligence services are expected to collect information on infrastructure, technology and activity along the Norwegian coast. In order to conceal this activity, it will be carried out from civilian vessels. These covert maritime intelligence operations target Norwegian interests at sea, in national waters and at ports.

Russian vessels are subject to extensive restrictions and do not have access to ports on the Norwegian mainland. The exception is Russian fishing vessels in Båtsfjord, Kirkenes and Tromsø, but this access is severely restricted. Russian crews on civilian vessels registered in third countries represent a significant threat in 2026.

Civilian vessels are used to gather information on Norwegian and allied military capabilities and to reconnoitre coastal and subsea infrastructure.

Norway's northernmost counties and Svalbard are vulnerable to intelligence and influence activities by state actors

Photo
Getty

These vessels may also be used to stage maritime scenarios that test Norway's preparedness and crisis response. Access to ports along the Norwegian coast may be exploited to facilitate the smuggling of goods subject to sanctions or export controls, as well as to support unlawful intelligence activity.

The High North and the Arctic region are strategically important to Russia

Russian intelligence and security services continuously seek insight into Norwegian political processes and decisions that could affect Russian interests. Key targets include politicians, government ministries and other decision-makers with the knowledge, ability and opportunity to influence policy. Areas of particular interest include defence, foreign and security policy, High North policy and issues related to Svalbard. The business sector, civil society and academia in relevant fields are also vulnerable to intelligence and influence activities.

Russian intelligence and security services operate throughout Norway. The northernmost counties and Svalbard are of particular interest and therefore especially exposed to intelligence and influence activities. This applies to Finnmark's border areas and Russian settlements on Svalbard.

China

Chinese intelligence has increased its operational capacity in Norway

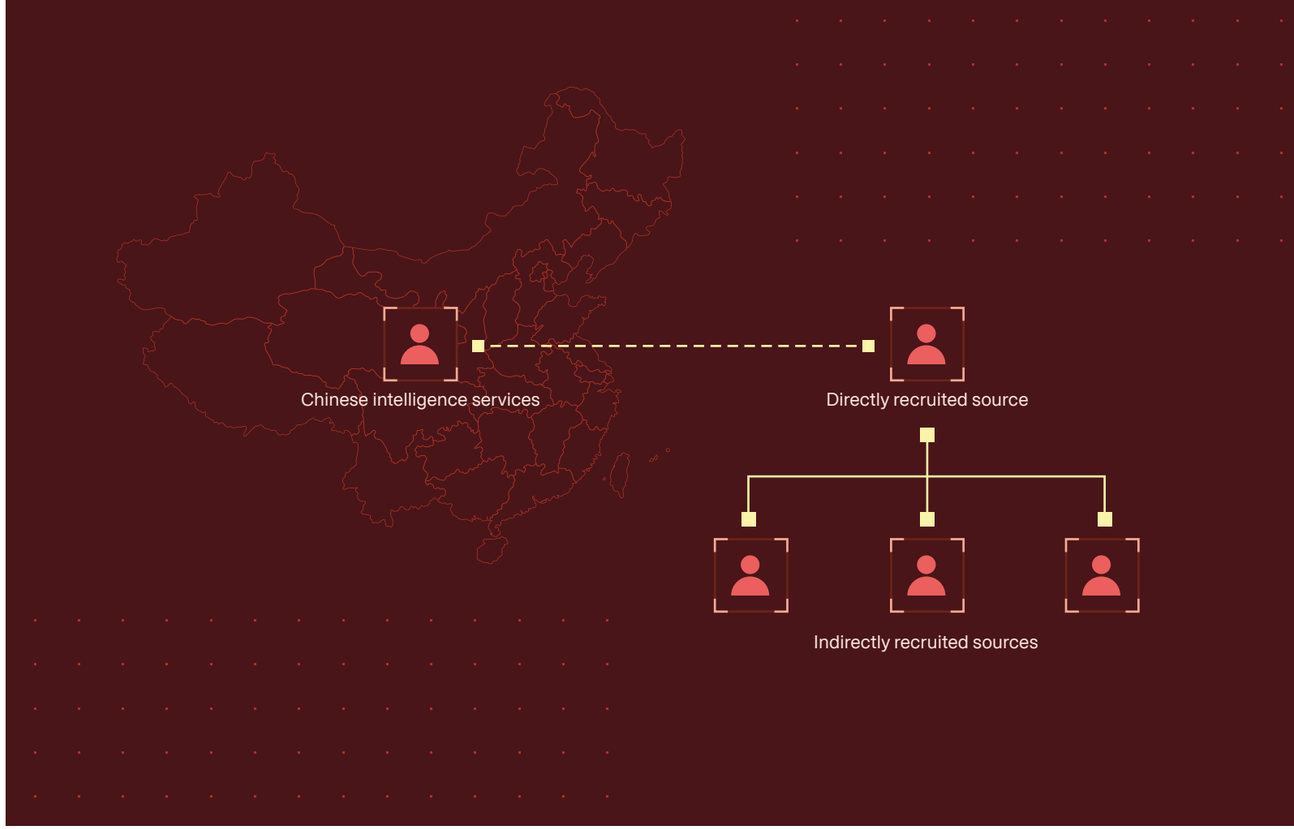
Chinese security and intelligence services have enhanced their capacity to conduct intelligence operations in Norway, including cyber operations and human intelligence collection. In 2026, Chinese intelligence actors are expected to collect intelligence, reconnoitre Norwegian digital infrastructure and threaten groups and individuals to prevent them from criticising the Chinese Communist Party. An increasing number of operations are likely to be carried out by commercial cybersecurity contractors and individuals who are not trained intelligence personnel but act on behalf of Chinese security and intelligence services.

The primary intelligence threat from China is in the cyber domain

Norwegian organisations holding sensitive information are targets of Chinese cyber operations. Chinese cyber threat actors also exploit Norwegian routers and servers to conduct operations against third countries. Chinese security and intelligence services not only conduct cyber operations directly but also via commercial cyber contractors. The role of these contractors has become more central, significantly increasing the capacity of Chinese intelligence services in the digital domain. Some contractors also conduct offensive cyber operations independently and attempt to sell access obtained by compromising systems. As such, not all Chinese cyber operations in Norway necessarily reflect the intentions of Chinese security and intelligence services. This development has created a more unpredictable and diffuse threat landscape, increasing the uncertainty about which organisations could be targeted.

Collaborative research can increase Chinese threat actors' ability to operate in cyberspace

China systematically exploits collaborative research and development (R&D) efforts to develop military capacity and strengthen its security and intelligence services. Chinese law requires all software vulnerabilities identified by Chinese researchers to be reported to the authorities no later than two days after discovery. These vulnerabilities are a key tool in Chinese cyber operations, including those targeting Norway. Norwegian-Chinese research collaboration that uncovers software vulnerabilities could therefore constitute a national security risk. Vulnerabilities identified through research collaboration are expected to be shared with Chinese intelligence and could be exploited in future cyber operations.



Individuals recruited by Chinese intelligence establish human source networks

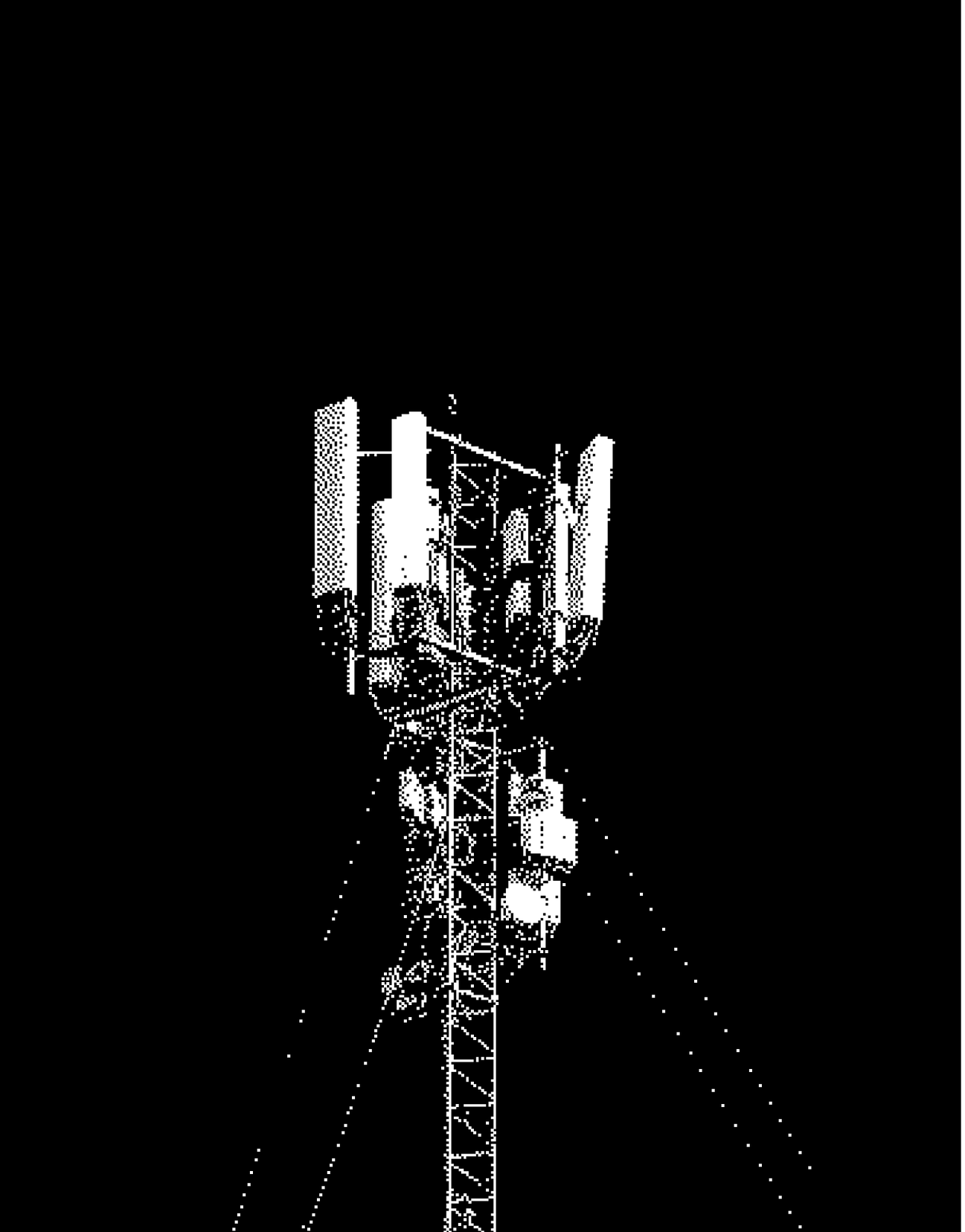
Chinese intelligence services try to recruit Norwegian nationals to gain access to sensitive and classified information, using both direct and indirect methods. People with links to China through study, work, friends or family are particularly vulnerable, as these connections increase intelligence services' potential for intimidation or inducement.

There is also an increasing trend of Chinese intelligence services encouraging sources to establish their own networks, for example by advertising part-time positions on job recruitment websites or approaching individuals via LinkedIn. Those recruited indirectly are often unaware that they are reporting to Chinese intelligence. The client's identity is often concealed; sources are typically told they are working for a think tank, an international company, a consultancy firm, or similar. Sources are initially asked to provide non-public information in exchange for payment, such as details on the activities or plans of companies, public sector organisations or political institutions. Over time, they can be assigned more specific tasks. This approach strengthens Chinese intelligence's ability to collect information via human sources. Chinese intelligence services are expected to try to recruit Norwegian nationals through sources in other Western countries.

↑

People recruited by Chinese intelligence are increasingly being encouraged to recruit their own human source networks, for example by advertising part-time positions on job recruitment websites or making contact via LinkedIn. Those recruited indirectly can be unaware that they are reporting to Chinese intelligence. The client's identity is often concealed.

Illustration
Getty / Dinamo Design



Chinese threat actors will attempt to silence individuals in Norway

Chinese threat actors continuously monitor and pressure individuals and groups in Norway who openly criticise China's government or human rights record. Individuals are coerced, threatened and intimidated into thinking they have no choice but to stop criticising the regime or involuntarily return to China. Intimidation tactics range from repeated phone calls from hidden numbers to actual death threats.

Threat actors also seek to recruit people in Norway to report on members of diaspora communities. When the Chinese state lacks direct influence over critics or their families, the internet becomes the preferred platform for suppressing dissent. For example, Chinese cyber threat actors distribute malware via seemingly legitimate mobile apps designed to appeal to Tibetan and Uyghur communities. Individuals living in Norway are likely to be subjected to such digital surveillance.

China will try to use research as a gateway to Norwegian territory in the High North

Media scrutiny of Chinese activity in the High North, alongside Norway's national security strategy, has curtailed Chinese actors' ability to operate on Norwegian territory in the region. Nevertheless, they continue to seek a foothold. In our assessment, they view the research and education sector in the region as one of the few remaining spheres where cultivation and collaboration are still possible. Chinese efforts on Norwegian territory in the High North will continue and we expect them to be carried out covertly by Chinese research institutions and individuals acting on behalf of Chinese security and intelligence services.

Chinese security and intelligence services have enhanced their ability to conduct intelligence operations in Norway. In 2026, this will include reconnaissance of Norwegian digital infrastructure.

Illustration
Getty / Dinamo Design

Iran

We assess that Iranian intelligence and security services will carry out intelligence and influence operations in Norway in 2026. The Iranian regime may also attempt to target Western interests in the form of damage to property, targeted assassinations, terrorist acts or destructive cyber operations. Such attacks are used as political tools to express discontent, exact revenge or silence critics.

Iran aims to target dissidents, critics and Israeli interests in Norway

The target profile of Iranian intelligence and security services in Norway and the West in general remains relatively stable, and includes dissidents, human rights organisations, academics and journalists who criticise the Iranian government. American, Israeli and Jewish interests, as well as non-Iranian Western politicians who support one or more of these groups, are also considered at risk.

The use of criminal networks and other proxy actors makes it more difficult to trace activity back to Iran.

These target groups are viewed as potential threats to the legitimacy and survival of the ruling authority in Iran. Iran's prioritisation of groups varies depending on the geopolitical situation in the Middle East, including the conflict between Israel, Iran and the United States, or internal events, such as social unrest within Iran.

Iran exploits criminal networks in Norway

Iran uses proxy actors to carry out operations in the West. These actors have no formal affiliation with Iranian government authorities but knowingly or unwittingly carry out activities on behalf of, or in support of, the Iranian government. Proxy actors can include Swedish criminal networks with a presence in Norway.

The use of criminal networks and other proxy actors makes it more difficult to trace activity back to Iran. These actors also have extensive freedom of movement within Europe, good local knowledge and access to weapons. However, reliance on proxies can reduce Iran's control over operations, and the actors' lack of experience may result in effects that are either greater or more limited than intended.

Iran monitors dissidents in Norway

Iranian intelligence and security services monitor and exert pressure on Iranian dissident and separatist groups in Norway using a range of methods, both physical and digital. For example, Iranian cyber threat actors compromise email accounts, social media profiles and private computers belonging to dissidents to collect information about them and their networks. These actors have advanced capabilities and will continue to develop their methods to conduct increasingly targeted and intrusive operations against individuals in Norway.

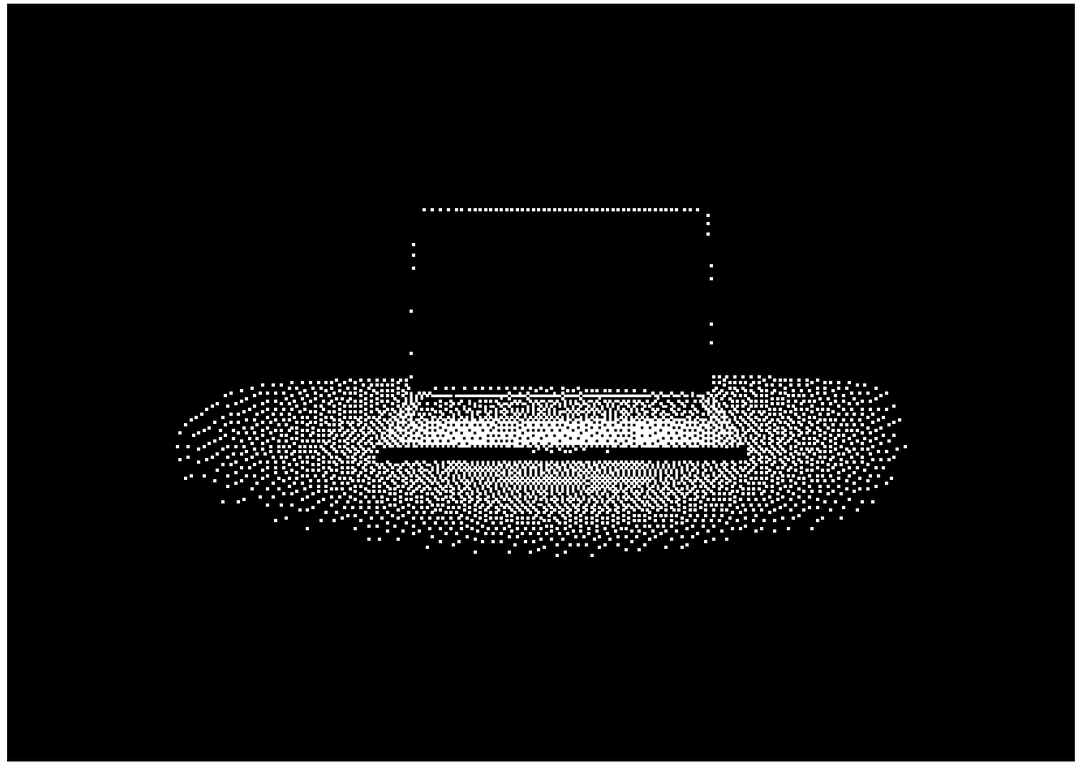
Information is also gathered via human sources, for instance during demonstrations or other public events. Should developments in Iran or external factors prompt the Iranian authorities to identify certain groups as significant threats, this information could be used to plan attacks in Norway.

Iran seeks access to dual-use technology

Iran remains subject to stringent international sanctions. As in previous years, Iran is likely to attempt covert acquisition of goods and technology from Norway that could be used to advance its military capabilities.

Iran monitors dissidents in Norway and compromises, for example, their email accounts, social media profiles and computers.

Illustration
Dinamo Design



Key methods

Cyber operations

Cyber operations are a key tool for foreign states' intelligence activities in Norway. Russia, China, Iran and North Korea are examples of countries carrying out cyber operations in Norway, either directly or through proxy actors. We expect these activities to continue in 2026, with several operations likely to succeed. Methods vary and can include intelligence collection, reconnaissance, influence operations, sabotage and disruptive activity. Financial gain may also be a motive. This variation means that cyber operations affect a wide range of targets.

Threat actors exploit both technical and human vulnerabilities

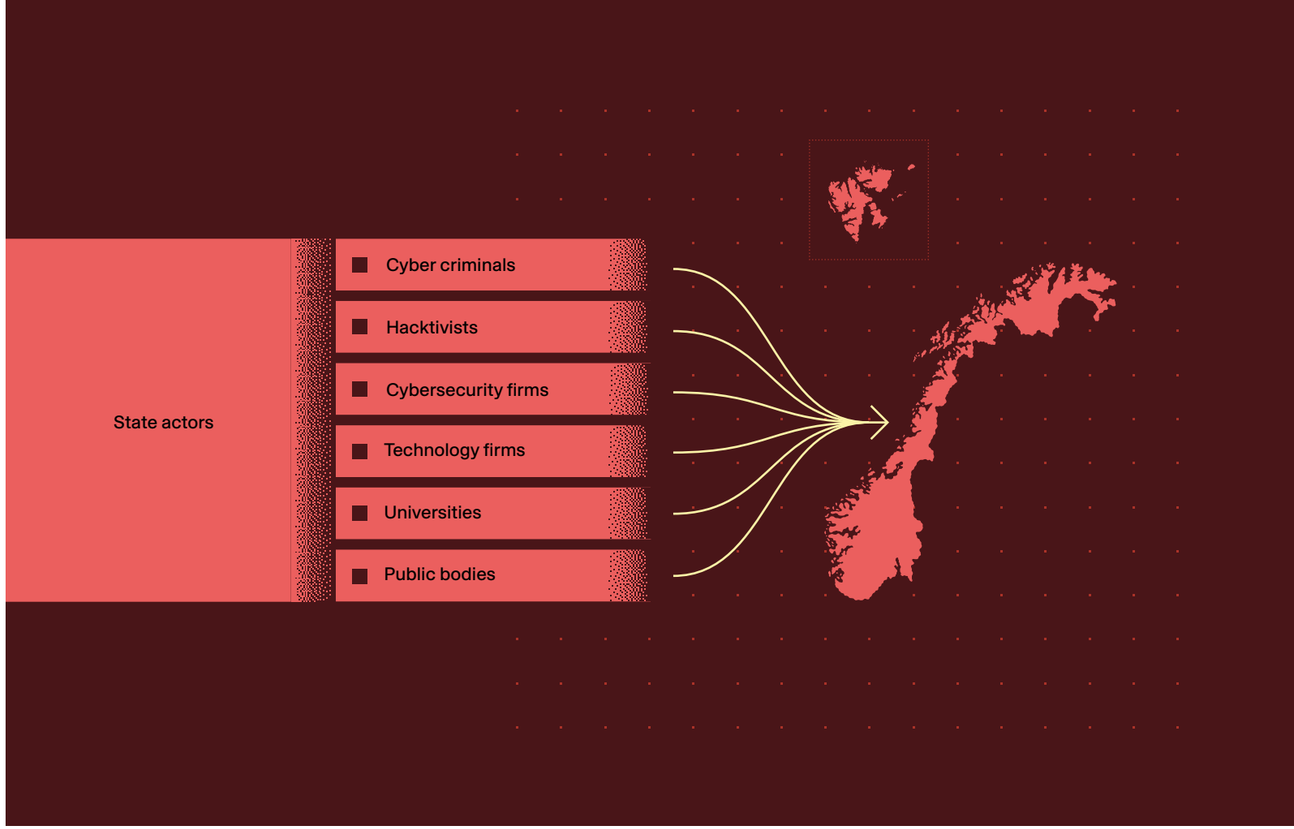
Cyber threat actors operating in Norway employ methods that exploit both technical and human vulnerabilities. This is particularly evident with Russia and China, which in 2025 exploited weaknesses in network devices, such as routers, to gain access to Norwegian digital infrastructure. The same methods are also employed for intelligence collection. For example, over the past year, threat actors accessed sensitive information by exploiting **zero-day vulnerabilities** in email services.

Social engineering was also a key factor in successful cyber operations in 2025. While social engineering is widespread among cyber criminals, state actors often use it in the cyber domain with particular sophistication, carefully planning highly targeted operations and investing time in building trust with the target.

Such tactics are evident in cyber operations aimed at transnational repression of Iranian dissidents or human rights activists in Norway. Iranian cyber threat actors will contact an activist while posing as a journalist interested in their work, often proposing a remote meeting. Over the course of an extended dialogue, the actor deceives their target into downloading malware on their computer or disclosing login details. Iran then uses this access to collect information about the victim and their network.

The Chinese cyber threat actor known as Salt Typhoon is an example of an actor who has compromised vulnerable network devices in Norwegian organisations. US authorities describe this actor as specialising in cyber operations targeting telecommunications infrastructure. Salt Typhoon is linked to private Chinese cybersecurity firms, illustrating the central role of private contractors in Chinese cyber operations and how they help enhance the capacity of Chinese security and intelligence services.

A **zero-day vulnerability** is a bug in an application or operating system that is known to certain actors but not to the public, the supplier or the manufacturer. As a result, neither the supplier nor the manufacturer has the opportunity to address the vulnerability before it is exploited by a threat actor.



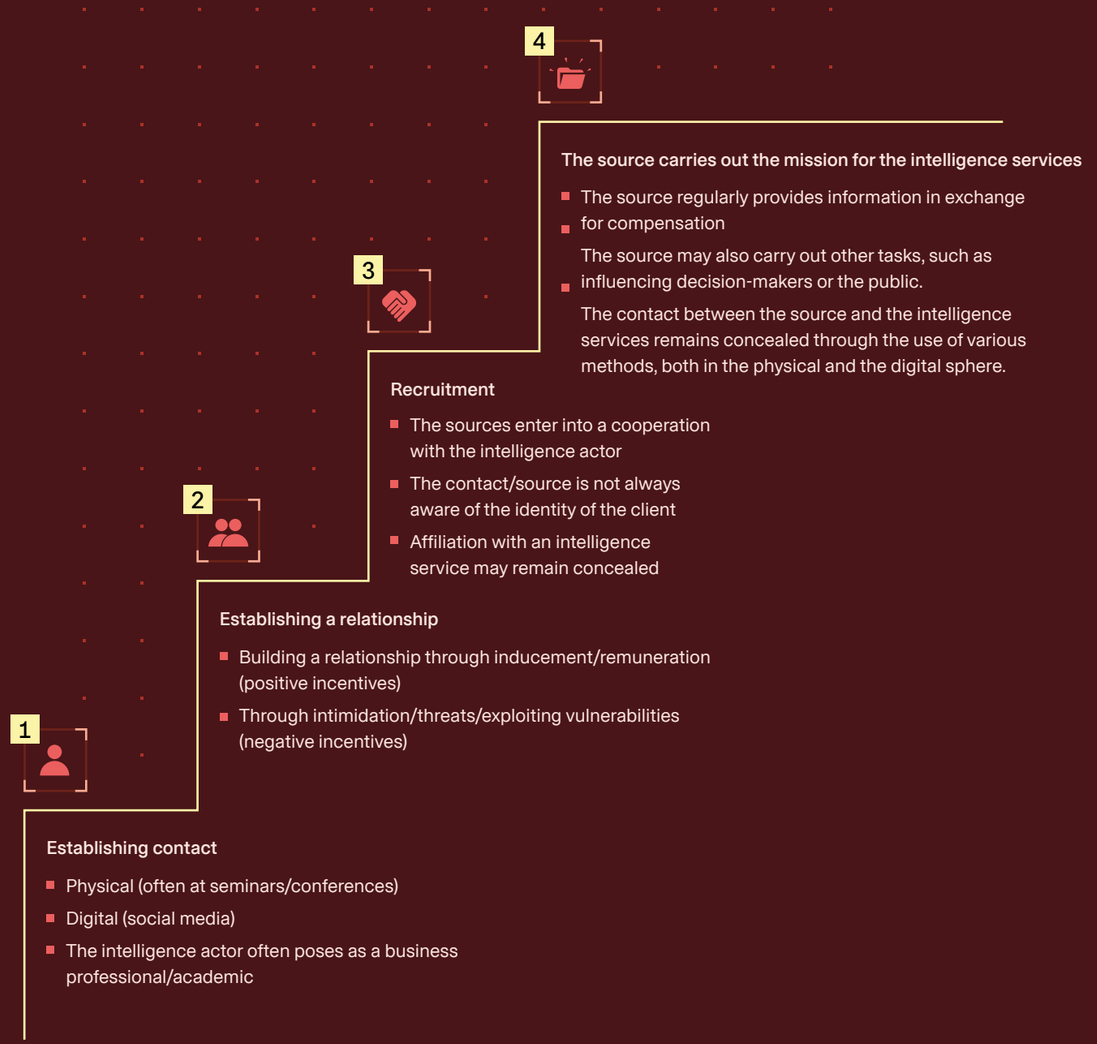
North Korean cyber threat actors are known for their creative social engineering. In an ongoing campaign aimed at Norwegian and other Western targets, businesses have been manipulated into employing North Korean IT developers. Recruitment and work duties are carried out remotely, with threat actors using methods such as forged identity documents to conceal their country of origin. Companies therefore remain unaware of the new employee's true country of origin. The salaries of North Korean employees in such positions may be used to fund the country's weapons and nuclear programmes.

Artificial intelligence creates new opportunities for cyber threat actors

Artificial intelligence (AI) is strengthening the abilities of state cyber threat actors to conduct operations in Norway. AI can be applied across all stages of a data breach, reducing the need for human operators. It also offers considerable potential for social engineering, and enables threat actors to create fake images, videos, text or audio to lend credibility to false identities. We expect that, in 2026, Norwegian organisations will be the target of cyber operations from state actors in which AI plays a key role.

Proxy actors are engaged in cyber operations in Norway. Their involvement ranges from executing operations on behalf of intelligence services to developing tools used in such operations.

Illustration
Getty / Dinamo Design



Recruitment of human intelligence sources

Foreign intelligence services will attempt to recruit human intelligence sources and facilitators in Norway in 2026, with Russia and China representing the greatest threat. People with access to sensitive or classified information, as well as those holding key positions or offices, are particularly at risk. Those with familial or other ties to authoritarian states are also at risk, as such connections increase the potential for intimidation or inducement.

Recruitment is carried out and contact is established in both the physical and digital domains. Intelligence officers operating under cover, often posing as diplomats, may attempt to recruit individuals in Norway at seminars, conferences and other professional gatherings. Social media is an established tool for foreign intelligence services, allowing them to reach a wider segment of the population. Digital recruitment is cost-effective and does not require the recruiter to be physically present in Norway. Contact may be initiated via fake LinkedIn accounts or through seemingly legitimate enquiries. Norwegian nationals may also be targeted while in third countries, and given the current geopolitical situation, those in Russia should anticipate attempts at recruitment, particularly those with influence or access to information of interest.

In the autumn of 2024, PST arrested a Norwegian national who had initiated contact with Russian and Iranian authorities in order to give them information. In 2025, the man was convicted of 'aggravated intelligence-gathering regarding state secrets' (under the Norwegian Penal Code); however, the verdict has been appealed and is therefore not legally enforceable. This case demonstrates that contact with foreign intelligence services is sometimes initiated by the person recruited.

Human sources can be tasked with a wide range of activities, which often increase in scope over time. Foreign intelligence services are not only interested in classified material but also unclassified sensitive information. Individuals who are recruited may also be asked to enlist additional sources, or to carry out practical tasks such as procuring sanctioned goods or installing surveillance equipment. Their remit could also include sabotage, disruptive activities, acts of violence or terrorist activity.

Recruited insiders within Norwegian organisations may be asked to gather information on disputes, internal conflicts, dissatisfaction and other vulnerabilities, including in procedures, security arrangements or ICT infrastructure. Such vulnerabilities can subsequently be exploited in intelligence, influence or sabotage operations.

Recruitment of human intelligence sources step by step.

Illustration
Dinamo Design

Transnational repression

Authoritarian states' transnational repression activities are driven by a fear that opposition may, over time, challenge the regime's hold on power. China and Iran in particular, but also Russia, seek to suppress speech that is critical of their policies or that could damage their reputation. Dissidents and critics of the regime are most at risk, but other public opinion leaders may also be targeted.

Some states are willing to take major risks to silence political opponents. They employ a range of repression tactics, including intimidation and threats and, in the most extreme cases, lethal violence. Dissidents can be pressured into returning to their own country, for example through threats against or the imprisonment of family members who remain there. Foreign states may use their diplomatic missions, visiting intelligence officers, organised criminal networks or infiltrators of diaspora communities to silence their critics in Norway.

Threat actors identify and monitor critics by filming or photographing participants at demonstrations and human rights events. They also conduct cyber operations to gather information on groups of interest, for instance by distributing malware via links to news articles, cultural videos or other content designed to appeal to specific target audiences.

The scope of transnational repression in Norway is determined in part by the visibility of criticising voices in the public sphere and the presence of prominent leaders. Where threat actors have no direct influence over their targets or their family members, they use the internet to suppress dissent. In the current geopolitical climate, with rising tensions between liberal democracies and authoritarian states, the latter may escalate their efforts to silence foreign critics, particularly through online channels.

Influence operations

We expect that authoritarian states will carry out influence operations in Norway in 2026. Their aim will be to protect their own national interests, often at the expense of Norwegian interests and the broader Western security cooperation. These operations can take place in both the physical and digital domains and can focus on a wide range of targets, from diaspora communities to individuals involved in Norwegian politics. Foreign states have an ongoing interest in recruiting and exerting influence over individuals with political influence, whether through formal or informal power. This may be achieved through relationship-building, threats or, in extreme cases, targeted disinformation campaigns. Individuals recruited by intelligence services may be instructed to covertly influence decision-making.

Russia and China have extensive influence networks that include their security and intelligence services, various government authorities and proxy actors. They are continually developing new methods for producing and disseminating content aimed at influencing audiences, including selling fake user accounts, creating video content and recruiting social media influencers to spread propaganda and disinformation.

Operations by foreign intelligence actors can have multiple objectives. Influencing public opinion by generating unrest and attracting attention may be one. This was demonstrated in 2025, when a pro-Russian hacktivist group conducted a cyber operation aimed at a Norwegian dam. The operation was unsophisticated and had limited potential for damage, but nevertheless attracted considerable attention when the actor publicised the incident on social media.

Unlawful procurement of sanctioned and export-controlled technology

Norwegian entities that develop, sell or conduct research on military- and dual-use technology remain targets for unlawful procurement in 2026. State actors use illegal, covert methods to acquire Norwegian technology that is subject to export controls and sanctions.

These attempts at circumvention are often creative. To conceal the real end user, threat actors often route exported goods through intermediaries in third countries, who then re-export the goods illegally to destinations such as Russia. These operations can involve multiple intermediaries, and actors from different countries may work together. For example, Russian actors under strict sanctions may try to obtain restricted goods from Norway via Chinese intermediaries. Intermediaries may be knowingly or unwittingly involved and can be located in a variety of countries, also within Europe.

Enquiries from businesses in all countries therefore carry a potential risk. Consequently, when receiving an enquiry about a product, Norwegian organisations should look for signs that it might be diverted for unlawful purposes.

■

Examples of indicators of covert procurement attempts include:

- Orders that omit end-user information, such as a URL, address or phone number.
- Customers with no website, an unprofessional website, or no contact number.
- Unusual specifications for packaging, shipping routes, declarations or payment methods.
- A shipping company, warehouse or port is specified as the end user.
- Unusually small or large order quantities, or quantities that do not align with the stated purpose.

'Know your customer and your technology' is an important principle for uncovering unlawful procurement activity.

Threat actors' technology needs are diverse and constantly evolving. Consequently, a broad range of technologies and organisations in Norway remain exposed to attempts at unlawful procurement. Many attempts are professionally executed and difficult to detect. Nevertheless, a significant number are successfully prevented due to Norwegian organisations' vigilance.

Economic activity that poses a threat to national security

The illustration shows a fictional example of how state actors use complex ownership structures to conceal their involvement in economic activity that poses a threat to national security. The example is based on a combination of different methods observed in Norway.

Illustration
Getty / Dinamo Design

Research environments will remain at risk

Foreign states seek not only to acquire physical goods, but also the technology and "know-how" behind products with military applications. The objective is to strengthen their own capability to develop and produce these products. For example, countries such as China or Iran may attempt to acquire technology by gaining access to R&D facilities and research groups in Norway.

We assess that threat actors are likely to exploit opportunities such as guest lecture programmes or access to specialised research infrastructure to engage in activities beyond those formally agreed. They also misuse data and information shared within international research collaborations. Researchers at Norwegian institutions may unwittingly be exposed to risk if they are unaware that the information could be exploited for military purposes.

Economic activity that poses a threat to national security

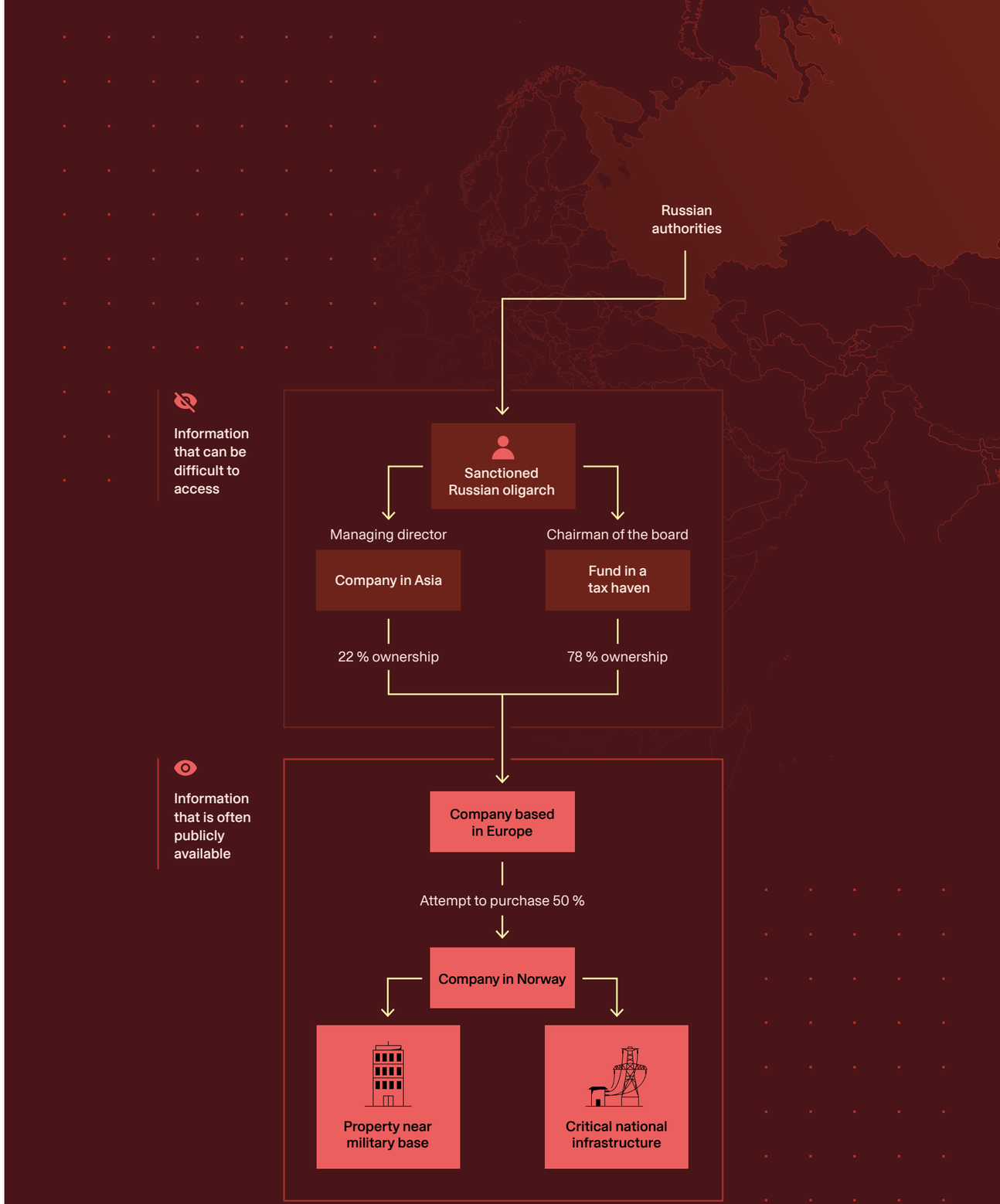
State-linked economic activity, such as investments and acquisitions, will continue to threaten national security in 2026. These methods are employed to gain access to technology, influence decision-making and collect sensitive information.

By purchasing strategically located property, state actors can gain insight into Norwegian and allied military activities, critical national infrastructure and other national security interests. Individuals linked to the Russian government apparatus have previously attempted to purchase property near Norwegian military bases, which would have provided them with valuable information on military operations and capabilities.

State actors also conduct ostensibly normal business activities, including acquisitions and investments in Norwegian companies, to gain control over critical national infrastructure and insight into corporate decision-making processes. Through ownership of key businesses, states can control value chains and create unilateral dependencies that can be leveraged to exert pressure on Norwegian decision-makers.

Threat actors can gain information on and access to physical and digital infrastructure via public procurement processes and supplier agreements. Using Chinese technology in critical national infrastructure creates opportunities for intelligence collection, as Chinese companies are legally obliged to cooperate with the Chinese authorities and intelligence services.

Economic activity that poses a threat to national security can be difficult to uncover, as state actors employ a variety of methods to conceal their involvement. They also exploit the fact that such activity often operates in a legal grey area. We have observed multiple instances in which Russian ownership of Norwegian companies has been obscured through complex ownership structures involving investment funds and companies in several countries. These structures make it challenging to identify the real owners and determine who has control in Norwegian companies.



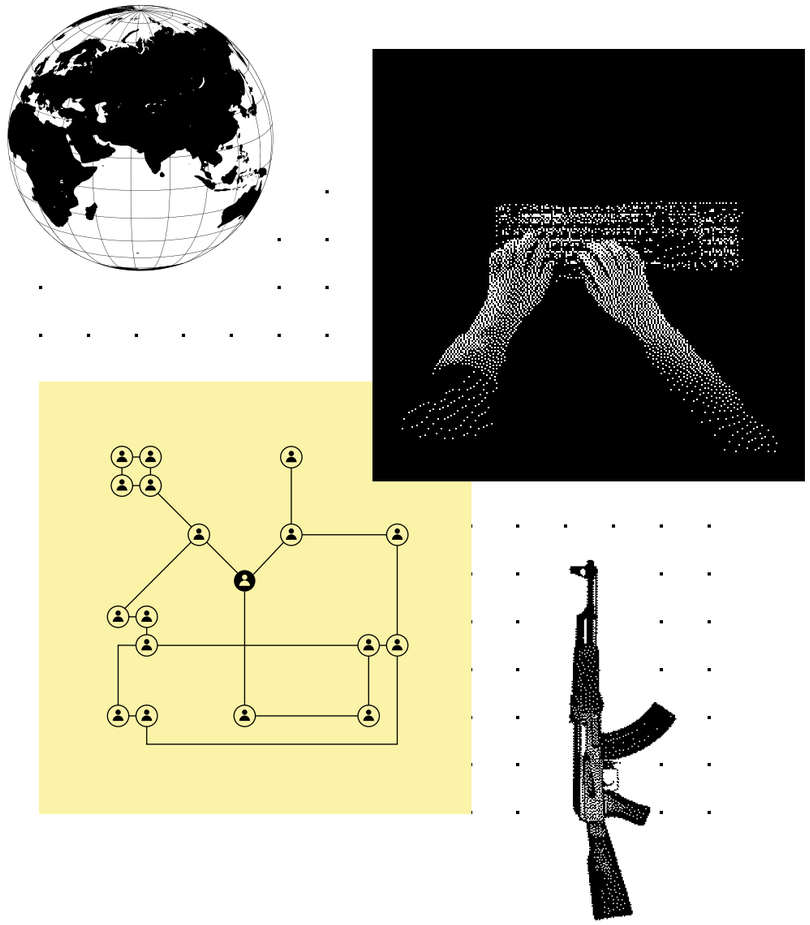


Illustration
Getty / Dinamo Design

Chapter 02

Politically motivated violence

The terrorism threat level in Norway is assessed as MODERATE, corresponding to level 3 on the national terrorism threat scale (see page 7).

While the overall threat level is MODERATE, the terrorism threat landscape is more complex and unpredictable than previously. It is also characterised by multiple actors with a variety of motivations, with overlap between state actors, terrorism and organised criminal networks. This convergence makes it difficult to distinguish terrorism from other criminal activity in the early stages of an incident.

Radicalisation of minors and young adults remains a challenge. Many are particularly vulnerable due to mental health issues and social exclusion. The threat landscape is further complicated by the conflation of ideology and fascination with violence, which makes it more difficult to uncover potential terrorist acts.

In the past two years, terrorist activity in the West has been at its highest level in several years. Although security and intelligence services manage to avert a large proportion of planned attacks, anticipating the actions of lone actors remains challenging.

This chapter focuses on the most serious threats from politically motivated violence in Norway: **Islamist extremism** and **right-wing extremism**. It also addresses **anti-government extremism**, which became increasingly pertinent over the course of 2025.

Radicalisation is defined as 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 objectives.

Extremism is defined as the acceptance or support of violence to achieve political, religious or ideological objectives.

The threat from Islamist extremism

What is **Islamist extremism**?
Islamist extremists accept the use of violence to achieve their political, religious or ideological objectives.

Their interpretation of Islam, and how it should be practised, differs from that of the majority of Muslims in Norway.

PST assesses there is an ***even chance*** that Islamist extremists will attempt to carry out terrorist attacks in Norway in 2026.

The high level of terrorist activity across Europe is expected to continue, particularly in light of the situation in Gaza and elsewhere in the Middle East. Israeli military operations in Gaza may inspire new actors to target Israeli and Jewish interests in Europe. The change with regards to the profile of threat actors could make it more difficult to predict how attacks are planned and executed.

Online radicalisation, particularly among young people who consume, produce and share extremist material, remains a concern.

The high level of terrorist activity in Europe is expected to continue

The terrorism threat from Islamist extremists stems from sympathisers of the ideology of two international terrorist organisations: the Islamic State (IS) and al-Qaeda, or from individuals driven by what they perceive as provocations, affronts to Islam or the oppression of Islam and Muslims. These actors regard the West as one of their primary enemies, partly because they perceive it to be at war with Islam and Muslims. Norway has only occasionally been singled out in the propaganda and rhetoric of international extremists, but is however generally viewed as part of the Western enemy. By contrast, Norwegian Islamist extremists regard Norway as a primary target.

In the West, particularly in Europe, the level of terrorist activity by Islamist extremists has increased considerably following Hamas' terrorist attack on 7 October 2023 and Israel's subsequent military operation in Gaza. The high level of terrorist activity continued throughout 2025. Most planned attacks, however, are averted by security and intelligence services.

We expect the high level of terrorist activity in Europe to continue in 2026. This is primarily due to the radicalising effect of Israel's military operations in Gaza, combined with subsequent calls from both IS and al-Qaeda to attack targets such as Israeli and Jewish interests in the West. We assess that this negative impact on the threat landscape will continue even if a ceasefire is observed or the conflict ends.

There are also indications that the military operations in Gaza is inspiring new actors to attack Israeli and Jewish targets in Europe. Individuals who sympathise with or have links to Hamas becoming involved in potential terrorist activity in Europe, is potentially a new development. Because this is evolving, understanding how attacks are planned and executed is challenging. Additionally, Iran may attempt to use proxy actors in efforts against these targets.

We expect that in 2026, IS and al-Qaeda will primarily seek to inspire sympathisers in Europe to carry out terrorist attacks. This is largely because IS in particular has once again been weakened in several core areas as a result of counter-terrorism operations. The IS branches that have targeted Europe in attempted attacks in recent years – IS in the Khorasan Province (ISKP) and IS in Somalia – have temporarily lost some operational capability. Meanwhile al-Qaeda continues to prioritise local growth. Its branch in the Arabian Peninsula (AQAP) remains intent on inspiring or facilitating attacks in Europe should the opportunity arise.

In 2025, terrorist propaganda from official sources as well as sympathisers continued to provide operational guidance and to incite sympathisers into carrying out attacks.

While these terrorist organisations primarily aim to inspire sympathisers to carry out attacks, international extremist networks will continue to try to recruit people already located in Europe. Such recruitment efforts will generally be opportunistic and focus on guiding or, where possible, inspiring sympathisers.

The threat from Islamist extremists in Norway persists

Although Islamist extremists have not carried out a terrorist attack in Norway since 2022, PST continues to monitor and counter serious threats. The threat from Islamist extremists therefore persists, despite few people in Norway supporting them.

Several individuals in Norway have connections to European and other international Islamist extremist networks. These networks could potentially ask them to facilitate or carry out terrorist attacks. Alternatively, they could connect them with others who can help them execute such attacks.

In Norway, there are still no clear, openly visible extremist groups with a common objective operating in the physical or digital domain. Many Islamist extremists, however, are linked through looser ideological networks or other relationships, such as familial ties, shared meeting spaces, historical networks or past terrorist-related activity. Attempts are occasionally made to form groups that advocate for Islamist extremism. Should these attempts succeed, they could increase the threat, as it may ultimately contribute to mobilisation, increased transnational networking and greater capability and willingness to commit terrorist acts.

The terrorist threat is therefore largely associated with individuals who often have unclear links to national or international networks and who may be inspired or recruited to commit terrorist acts. This makes the threat more unpredictable and difficult to detect.

The terrorist threat is therefore largely associated with individuals who often have unclear links to national or international networks and who may be inspired or recruited to commit terrorist acts.

Previously established groups are largely inactive, but there is little indication that well-established extremists have been de-radicalised. We expect this situation to continue throughout 2026.

Some Norwegian Islamist extremists may attempt to travel abroad as foreign fighters in 2026, but we expect interest in doing so to remain limited over the coming year. This is positive for the terrorism threat, as foreign fighter activity can stimulate radicalisation, as well as

Islamist extremist terrorist attacks are most likely to target ordinary civilians.

Photo
Lise Åserud / NTB

network- and capacity-building. However, even lone individuals who become foreign fighters can increase the severity of the threat.

We also expect that some individuals in Norway will provide financial support for terrorist activity abroad. PST has observed a growing number of cases in which funds are transferred abroad via digital payment services, with some recipients suspected of supporting terrorism. Not all service providers have a duty to report to Norwegian authorities, and the payment services themselves are constantly evolving. We expect this trend to continue.

The threat landscape in Norway could shift rapidly if events or political developments occur that Norwegian or international Islamist extremists perceive as particularly provocative. Propaganda can also play a role in triggering lone actors and this can be difficult to anticipate. Examples of trigger events that could exacerbate the terrorism threat include Norwegian military involvement in Muslim countries, perceived support for a conflict causing suffering among Muslims, and incidents considered an affront to Islam or Muslims.

We expect further instances of Quran burning in Norway in 2026. In recent years, Quran burnings and other perceived affronts to Islam have received little public attention. Nevertheless, the threat landscape could change rapidly if these events attract more public attention. Historically, terrorist acts in response to perceived affronts to Islam can occur several months or even years after the provocation.

Digital platforms remain a key domain for radicalisation and recruitment

Much of the current activity among Islamist extremists in Norway is linked to radicalisation and recruitment. Radicalisation is expected to continue across digital and physical domains, which often overlap and complement each other. In the physical sphere, we expect radicalization to occur between friends, family members, in prisons and in gyms, schools and religious settings. Nevertheless, most of the activity is online. In national and transnational online networks on encrypted platforms, users can operate and communicate anonymously, while building the relationships and trust necessary for terrorist planning and support activities.

Support for, and the propagation of, Islamist extremist ideology is now more widespread than a few years ago. Sympathisers generally express support across previous dividing lines between IS and al-Qaeda, and they continue to circulate old propaganda. They also frequently frame their ideology in terms of their personal experiences and beliefs. Some of the material consumed reflects a fascination with violence. Nevertheless, ideology remains the core basis for the radicalisation process, sometimes alongside secondary factors such as the fascination with violence.

We are concerned that individuals may be self-radicalised into terrorism as a result of exposure to extremist ideology, violent content and environments that normalise violence as a legitimate form of action. Personal vulnerabilities,

such as mental health challenges, social exclusion or life crises, can further increase this risk.

Terrorist organisations and their sympathisers will continue to produce propaganda with high-quality graphics and clear, easy-to-understand messages that incite terrorism. The content will continue to be published in multiple languages and adapted to changes on digital platforms. Artificial intelligence (AI) will be used as a translation tool and for producing videos and images. Currently, only a small proportion of propaganda is available in Norwegian, but we anticipate that some extremist material will be translated into Norwegian.

Radicalisation among young Islamist extremists is a challenge

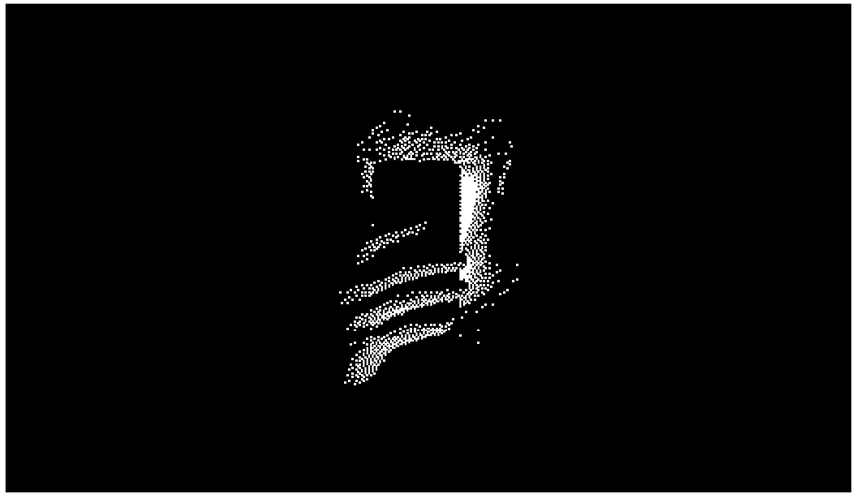
We assess that the radicalisation of minors and young adults will continue. Over the past year, PST has implemented a range of preventive measures aimed at this age group. There is a concern that young people's consumption, production and distribution of highly extreme Islamist material on popular digital platforms such as TikTok may contribute to their radicalisation into terrorism, even in the absence of explicit calls for violence. Official propaganda and material produced by sympathisers is often aimed at young audiences and disseminated via platforms that are particularly popular with them.

To date, activity among young people appears primarily to involve the propagation of ideology, the expression of opinions and frustration, the search for a sense of belonging, and the pursuit of status or recognition. Nevertheless, this activity is of concern, not least because it contributes to the spread of extremist ideology to other young people in Norway who have not previously been exposed to extremist material. We observe that some content in Norwegian is being distributed in formats and platforms that are accessible and appealing to young audiences.

→

PST is concerned that young people will be radicalised into terrorism.

Illustration
Getty / Dinamo Design



Targets and operational methods in a potential Islamist extremist terrorist attack in Norway

Any terrorist attack in Norway by Islamist extremists will most likely be carried out by one or a small number of perpetrators. These actors will often be in contact with other extremists prior to the attack, either digitally or in person.

Islamist extremists in the West continue to favour traditional means of attack, such as knives, firearms, improvised explosive devices (IEDs) and vehicles. These will continue to be relevant in attack planning, including in Norway. We also note some interest in the use of drones for attacks as well as for reconnaissance purposes. AI-generative tools, such as AI chatbots, may also be used in attack planning.

Islamist extremists consider all targets in the West to be legitimate. We assess that random civilians are still the group most likely to be targeted, followed by police and military personnel. Individuals and institutions perceived to be insulting the Islamic faith are also potential targets, and venues associated with the LGBT+ community have become more relevant targets in recent years.

We expect that Israeli and Jewish targets in particular will be the focus of somewhat more planned attacks over the next year than we have seen previously. Since 2014, such targets have only constituted a small proportion of planned attacks, but Islamist extremists' interest in them has increased since 2023, alongside an increased focus on Christian targets.

Factors that could increase the threat from Islamist extremists in Norway

The triggers of radicalisation and motives for carrying out terrorist acts vary and are difficult to foresee. However, we outline three factors that could heighten the threat from Islamist extremists if they were to occur.

- **Trigger events in or related to Norway** that attract significant attention could elevate Norway's prominence in Islamist extremists' enemy perception.
- **Increased engagement in national or international Islamist extremist networks** in physical and/or digital spaces could lead to greater mobilisation and, in a worst case scenario, strengthen individuals' capability and willingness to carry out terrorist acts.
- **Statements and propaganda from international terrorist organisations that explicitly call for attacks against Norway** could boost the number of potential threat actors and make Norway a more likely target for both homegrown and international Islamist extremists.

The threat from right-wing extremism

PST assesses there is an ***even chance*** that right-wing extremists will attempt to carry out terrorist attacks in Norway in 2026.

Many people who become radicalised are inspired by narratives that glorify violence but have no clear ideology, often through online forums glorifying grotesque violence. The threat landscape is therefore complicated by the conflation of ideology and fascination with violence, making it harder to pinpoint the factors that trigger the acceptance of violence.

We are also observing an increase in the number of minors involved in right-wing extremist terrorist activity in the West.

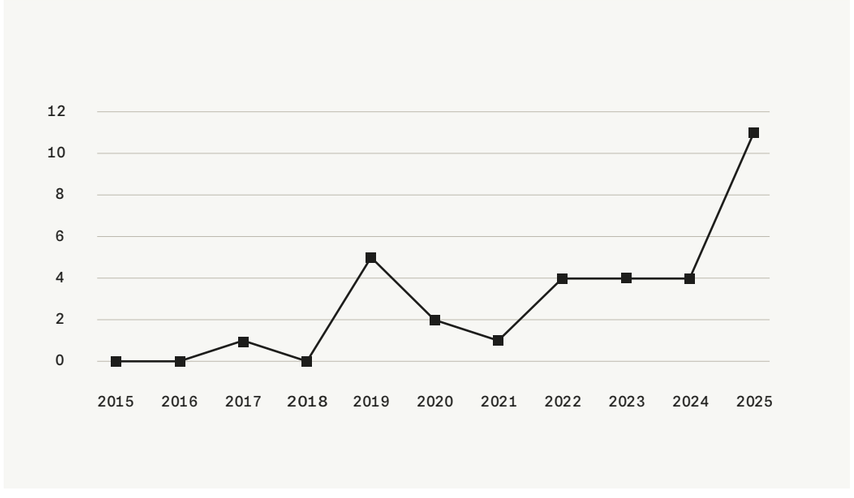
Right-wing extremist terrorist activity in the West persists, with increased involvement of minors

Right-wing extremist terrorist activity (attacks and foiled attempts) in the West has remained at a stable level since 2020. Further right-wing extremist terrorist attacks are expected.

The number of minors involved in right-wing extremist attacks has risen sharply over the past year. In 2025, minors were involved in nearly 50 per cent of all attacks and foiled attempts, compared with around 20 per cent in previous years. The radicalisation of minors has been highlighted repeatedly in recent years, and their increasing involvement in attacks in the West is a concerning trend.

Trends in right-wing terrorist activity in the West involving minors in the period 2015-2025.

Source
PST



An increasingly diverse and complex ideological landscape

Right-wing extremism encompasses a wide range of ideological currents. In recent years, the ideological landscape has become increasingly diverse and complex. Individuals radicalised into right-wing extremism are now inspired by a broader range of movements and groups. A growing number are also drawing inspiration from narratives with no clear ideological framework, which they often find in online forums glorifying grotesque violence. The combination of narratives that glorify violence and right-wing extremist ideology is concerning, as it could potentially accelerate the radicalisation of vulnerable individuals.

Supporters of the far right use a wide range of approaches with a view to realising their vision of society. Some right-wing extremists incite terrorism, some carry out terrorist acts, and others pursue long-term strategies through right-wing extremist groups. The far right also includes radical right actors who operate within democratic frameworks. Although our primary concern is with right-wing extremist terrorism, future perpetrators could also be inspired by other right-wing radical ideas. Some may find inspiration or legitimacy in lawful forms of expression.

Initial driver: ideology or fascination with violence?

The diversity of the ideological landscape makes it difficult to pinpoint the factors that trigger the acceptance of violence. Right-wing extremist ideology is one possible factor; a pre-existing fascination with violence is another. This makes the threat more diffuse and unpredictable. Right-wing extremism is also increasingly difficult to define, as ideological conviction can at times appear superficial. The conflation of ideas further means that those who are radicalised tend to occupy a grey area between the responsibilities of the police and PST, adding another layer of complexity to the threat landscape.

The greatest terrorist threat is from actors in online forums that incite violence

Digital platforms will remain the primary sphere for recruitment and radicalisation to right-wing extremism. These are platforms where it is easy to establish contacts, find inspiration and propagate extremist material globally.

The terrorist threat from right-wing extremists will often stem from individuals participating in online forums that incite violence and terrorism. This is especially concerning in transnational right-wing extremist forums, where violent content is prevalent. Former terrorists are often glorified, and users are encouraged to carry out new attacks. They also receive guidance on producing and using weapons and on tactics for executing terrorist acts. PST assesses that content in these forums contributes to radicalisation and strengthens both the capability and willingness to carry out terrorist acts.

We remain concerned about Norwegian nationals active in forums that glorify violence and terrorism. Work is ongoing to identify these

Right-wing extremists are driven by the belief that the state and its people should form a single, unified community. This is based on the idea of a homogenous 'white race' and 'white' cultural identity. Their worldview is reinforced by conspiracy theories claiming that the 'white race' and 'white culture' are under threat of extinction. Those who do not belong to this community are regarded as a threat, with particular suspicion directed at Jews, Muslims, people of non-Western appearance, governments, politicians, mainstream media, LGBT+ individuals, and actors on the political left. Right-wing extremists consider violence a legitimate means of preventing what they perceive as the destruction of their community.

individuals, most of whom are male minors and youths who have been introduced to right-wing extremism via digital platforms.

Several perpetrators of executed and averted right-wing terrorist attacks in the West have been active in transnational online forums. It is important to note, however, that potential terrorists do not necessarily participate in these spaces; radicalisation can also take place through other channels.

We expect the right-wing extremist online landscape to remain dynamic, with groups continually forming and disbanding. Right-wing extremists will also use multiple platforms, often simultaneously. Open platforms, such as TikTok, facilitate the dissemination of propaganda and enable like-minded individuals to connect. Encrypted platforms, such as Telegram and Signal, have features that enable anonymous and secure communication. Gaming platforms, such as Roblox and Minecraft, have also emerged as spheres for right-wing extremist activity. These platforms are particularly significant for the recruitment of minors, as many of them engage in online gaming.

Gaming platforms, such as Roblox and Minecraft, have also emerged as spheres for right-wing extremist activity. These platforms are particularly significant for the recruitment of minors, as many of them engage in online gaming.

The right-wing extremist landscape in Norway — spheres for recruitment and radicalisation

In Norway, right-wing extremists operate in a small number of physical spaces and numerous digital spaces. These vary in size, organisational structure, level of activity and ideological grounding. Some actors in these spaces maintain links with like-minded counterparts abroad.

We assess that the Norwegian right-wing extremist landscape poses less of a threat than many transnational networks. This is because there is no evidence of incitement to terrorism or a clear intent to carry out attacks among Norwegian actors. Nonetheless, this landscape remains significant for recruitment and radicalisation.

Right-wing extremist groups will continue to exist in the physical sphere, but they are expected to remain few in number and small in scale. The longevity of these groups requires leadership figures or lone actors who can recruit members, foster cohesion and drive radicalisation.

Alongside these real-world groups, a range of digital spaces exist where right-wing extremists share ideology and propaganda. We expect that many of these forums will be created and rapidly disbanded, while others will continue for longer.

There are multiple pathways to radicalisation. Exposure to right-wing extremist content on open social media platforms can serve as an entry point, with individuals subsequently directed to more extreme content on other

Radicalisation into right-wing extremism is largely taking place via digital platforms.

Photo
Getty

platforms. This process is often facilitated by targeted algorithms. TikTok functions as an important gateway into right-wing extremism. Gaming platforms are also a key sphere for recruitment and radicalisation, particularly among younger audiences. Right-wing extremist content can initially appear humorous or harmless, even to those not actively seeking such material.

The challenge of radicalisation among minors and young adults is expected to continue. Many have vulnerabilities, including mental health issues or social exclusion, which often seem to play a more significant role in the radicalisation process than ideology. Young people can be motivated by a desire for belonging, social cohesion and affirmation of their self-worth, which makes them more receptive to extremist messaging. The threat is particularly acute from lone individuals who may decide to carry out a terrorist act. These individuals' affiliation with right-wing extremist networks can vary, and their desire to act can be shaped by personal factors, such as vulnerabilities or life crises. Intercepting radicalised lone actors is always a challenge for intelligence and security services.

> *Vulnerabilities seem to play a more significant role than ideology in the radicalisation of minors and young adults. They can be motivated by a desire for belonging, social cohesion and affirmation of their self-worth.*

Right-wing extremists in Norway may also be used in state influence operations. Online right-wing extremist forums are a primary conduit for spreading disinformation. This can potentially fuel distrust and create division about Western political institutions and liberal values.

Targets and operational methods in a potential right-wing extremist terrorist attack in Norway

A potential right-wing extremist terrorist attack in Norway would most likely be carried out by a lone actor.

Individuals or groups perceived as enemies by right-wing extremists are the most likely targets. These may include people of non-Western appearance, Muslims, Jews, politicians, public officials, dignitaries, LGBT+ individuals, mainstream media and actors on the political left.

The growing involvement of minors in terrorism may increase the likelihood of attacks at locations they frequent, such as schools. Schools can be a familiar and easily accessible target, where groups perceived as enemies may also be present.

The most likely types of attack are mass-casualty incidents and targeted killings. Damage to or the destruction of property and facilities are also potential forms of attack. The objective would be to trigger a 'race war' and societal collapse.

Firearms, IEDs and bladed weapons have been the most common instruments of attack in right-wing terrorism in the West in recent years, and we expect this trend to continue in 2026. Arson may also be a relevant tactic.

Some right-wing extremists in the West will show an interest in new technologies for use in attacks, and we expect that 3D-printed weapons will continue to be in evidence. However, producing reliable, high-capacity improvised firearms using 3D-printing technology will remain technically challenging. Use of drones has been limited to date but they may be useful for reconnaissance. In addition, AI tools may be employed in attack planning, primarily to gather information.

Factors that could increase the threat from right-wing extremists in Norway

The triggers of radicalisation and motives for terrorism vary and are difficult to foresee. However, we outline three factors that could increase the threat from right-wing extremists in 2026:

- **Trigger events:** events and societal trends perceived by right-wing extremists as a threat to the 'white race' can act as a trigger for terrorism. How extremists exploit such events or trends to push their worldview can also affect the threat they pose. New terrorist attacks by right-wing extremists could inspire further action. Trigger events can occur suddenly and are difficult to anticipate, contributing to an unpredictable and fluid threat landscape.
- **Significant increase in the number of Norwegians engaging in transnational right-wing extremist forums that incite violence:** engagement in such networks can strengthen individuals' capability and willingness to commit terrorist acts and increase the number of potential threat actors.
- **Conflation of narratives that glorify violence with right-wing extremist ideology:** The conflation of grotesque depictions of violence and right-wing extremist ideology, particularly ideological currents that explicitly promote violence and terrorism, can accelerate the radicalisation of vulnerable people, leading some to want to commit a terrorist act.

Anti-government extremism

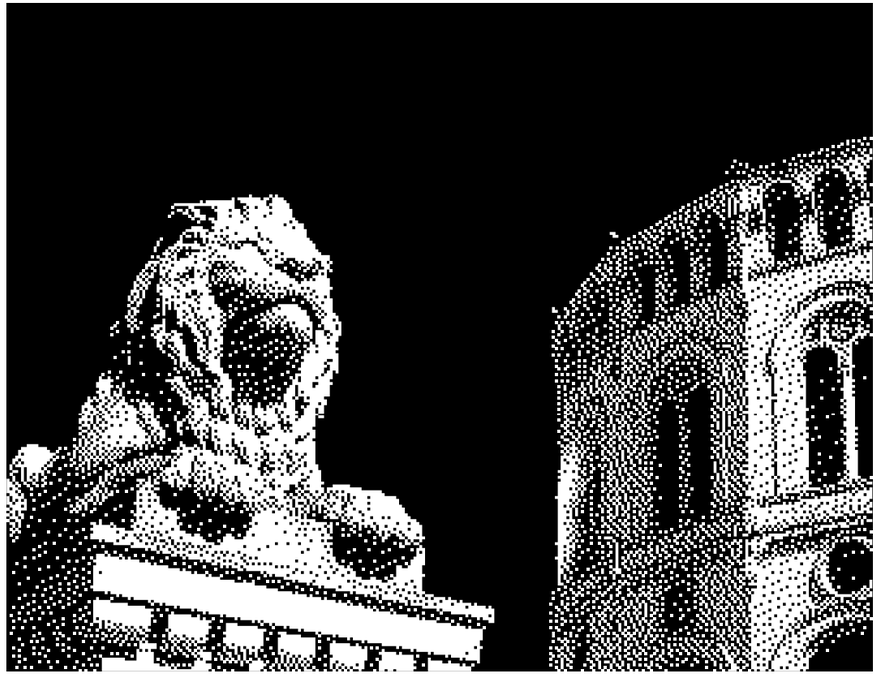
Conspiracy theories largely involve creating explanatory models. They claim that an elite or powerful group is conspiring against society, and there is a belief that these actors are working together to advance a hidden plan or agenda.

All-encompassing conspiracy theories fuel radicalisation

At the heart of anti-government sentiment are large, all-encompassing **conspiracy theories**. These theories can radicalise and motivate believers into carrying out violent acts in line with their worldview. Conspiracy theories are often used as simplistic explanations for complex issues and trends.

Anti-government extremists do not have a shared overarching ideology; they form groups based on conspiracy theories that promote distrust and alternative explanations. They thus differ from right-wing extremists and Islamist extremists, who have a deeper ideological or religious grounding. Anti-government ideas continue to partially overlap with right-wing extremist ideas. As with right-wing extremist spaces, anti-government spheres can also be used in state influence operations to spread disinformation via online forums.

In Norway, there are two strands of anti-government extremism that accept, support and legitimise the use of violence. One strand focuses on conspiracy theories about the **deep state** and other all-encompassing conspiracies. The other is underpinned by the notion of **sovereign citizens**, and regards the state as illegitimate and therefore lacking authority to exercise power. These strands, however, often overlap.



Anti-government actors consider the authorities to be one of their primary enemies.

Illustration
Getty / Dinamo Design

The enemy is demonised

Representatives of the authorities, such as the police and dignitaries, are sometimes viewed as legitimate targets for violence by anti-government actors. Anti-government sympathisers regard the state, the 'system' and government institutions as the enemy, often characterising them as an evil elite acting against the interests of the population. They believe this elite comprises of globalists, paedophiles and satanists with malicious intent. The enemy is at times framed as so dangerous and malevolent that certain individuals ultimately perceive violence as a necessary response.

Anti-government extremism remains a relatively marginal phenomenon in the Norwegian context. However, since the pandemic, all-encompassing conspiracy theories have continued to radicalize sympathisers, including in Norway. There is also an increasing focus on what is known as **militant prepping**. In other Western countries, there have been cases in which anti-government actors have attempted to build capacity to overthrow the ruling authority and expose the alleged secret plans of a malevolent elite. We assess that such capacity building and militant prepping can reinforce radicalisation, as they can strengthen the combination of capability and intent to carry out a politically motivated act of violence.

Severity and risk of violence can be under-communicated and misunderstood

Anti-government sentiment can sometimes be confused with delusional behaviour, leading to the severity of extremism and the associated risk of violence being under-communicated and misunderstood. The risk of violence can be increased when anti-government extremism is combined with other vulnerabilities, such as mental health issues.

The risk of violence can be increased when anti-government extremism is combined with other vulnerabilities, such as mental health issues.

The deep state:
The idea that elements of the government and leading figures in society are conspiring with or acting on behalf of a secret network or hidden elite seeking to seize global power.

Sovereign citizens:
The idea that the state lacks legitimate authority to exercise power, and that laws and regulations are instruments of control that undermine citizens' freedom and sovereignty.

Militant prepping refers to a form of preparation for violent resistance against the authorities and is aligned with doomsday conspiracy theories.

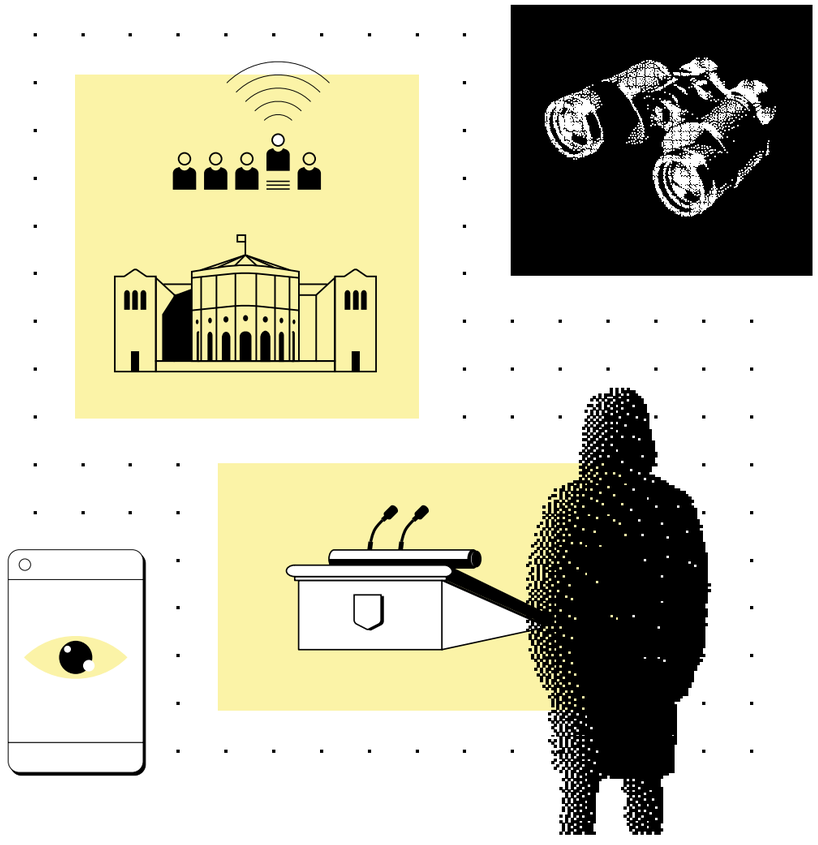


Illustration
Getty / Dinamo Design

Chapter 03

The threat to dignitaries in Norway

Dignitaries have ultimate decision-making responsibility in areas that significantly affect people's lives. They therefore attract considerable attention from the media and the public, putting their background and personal life under the spotlight. This leaves them open to online harassment and threats, reckless behaviour, and potentially minor acts of violence. It is **unlikely** that Norwegian dignitaries will be the subject of serious violent attacks. However, they will be subject to foreign intelligence activities.

Foreign dignitaries visiting Norway may remain targets of the same threats they face in their home country. For example, if they are associated with an international conflict that arouses public interest in Norway, they may be subjected to online harassment and threats, or attempts at direct confrontation.

Dignitaries include members of the Royal Family, the Storting (Norwegian Parliament), the Government and the Supreme Court, as well as representatives of the equivalent bodies from other states who are in Norway. PST has a particular responsibility for preventing and investigating threats against these individuals. Party leaders and leaders of youth political parties also fall within PST's remit.

A **personally motivated threat actor** is someone focused on a specific issue that affects them personally. They are often extremely frustrated and not motivated by extremist ideology. Such individuals may be experiencing difficult life circumstances and/or mental health challenges.

A **verbal confrontation** in this context refers to threats, harassment, and intimidating or reckless behaviour directed at a dignitary.

Online harassment and threats do not directly lead to acts of violence

When dignitaries come under media scrutiny over controversial issues, they can face extensive harassment and threats online. In most cases, this subsides, but some senior government ministers are targeted on an ongoing basis. PST has found no evidence that such activity leads to attempted or planned acts of violence.

Most of those who harass and threaten people online are what PST refers to as **personally motivated threat actors**.

PST and the police investigate the most serious threats. These threat actors tend to be seeking an outlet for their frustrations rather than wishing to commit acts of violence.

Harassment and threats against dignitaries remain an ongoing challenge for democratic processes, as they can discourage them from speaking publicly, attending events or holding office. Such behaviour can also deter people from entering politics, especially the younger generation.

Hostility towards authorities in digital spaces can lead to radicalisation

We are concerned that prolonged harassment and threats online could undermine trust in public authorities and foster violent intent. Airing frustrations on digital platforms can provide a breeding ground for conspiracy theories targeting dignitaries. Online hostility towards authorities can lead to radicalisation into right-wing extremism or anti-government extremism, and when combined with conspiracy theories or right-wing extremist ideology, can lead to violent intent.

Most dignitaries are not confronted directly

When dignitaries are approached in person, it is usually by political activists who are emotionally invested in a particular issue. This typically occurs at public events, where the activists seek to get close to the dignitaries in order to convey a political message. We expect that activists will continue to attempt face-to-face contact with dignitaries, but that their intention will be to peacefully express their message.

Approaches by political activists can be uncomfortable and threatening for dignitaries and can affect how they carry out their work. These incidents are classified as **verbal confrontations** and are expected to continue in 2026.

Some individuals, many of whom have mental health issues, try to make contact with members of the Royal Family. This is often motivated by a desire to ask for help; they have no violent intent. In some cases, individuals may wrongly believe they have a special relationship with a member of the Royal Family (known as fixation). The Royal Palace is the primary target of these contact attempts.

There have been no **physical confrontations** with dignitaries in Norway for several years. As noted, we expect some verbal confrontations going forward, and there is a risk of these unintentionally escalating into minor acts of violence. A small number of senior politicians may also be targeted in planned physical confrontations.

Extremists perceive dignitaries as enemies

As noted in the chapter on politically motivated violence, various extremist movements perceive dignitaries as enemies.

Right-wing extremists often link the authorities to conspiracy theories, claiming they are secretly working to eliminate the ‘white race’. Certain trigger events can make dignitaries a target for right-wing extremists.

Anti-government extremists consider the authorities to be one of their primary enemies. The state, the ‘system’ and the entire government apparatus are frequently characterised as an evil elite acting against the interests of the population. Current events linked to conspiracy theories can increase mistrust, thereby reinforcing anti-government extremists’ perception of dignitaries as an enemy.

Dignitaries are also perceived as an enemy by Islamist extremists, as representatives of the West. A dignitary may attract negative attention if they speak publicly or are associated with a trigger event that reinforces the notion of the West as an enemy of Islam. However, Islamist extremists’ perception of an enemy is broad, and other targets are generally more exposed.

Dignitaries will be the subject of intelligence activity

Dignitaries and their connections are vulnerable targets for foreign intelligence activities in Norway. Russia and China pose the greatest threat, though other countries also engage in similar operations.

A common form of intelligence activity is cyber operations, particularly phishing. These campaigns are conducted via email, text messages, social media and other communication platforms, with the aim of tricking people into downloading malware or revealing login details. If successful, these actors can gain access to a dignitary’s private and professional correspondence, calendar and contacts. This sensitive information may then be exploited for intelligence and influence operations.

Dignitaries are attractive targets for foreign influence operations because of the access they are afforded and their role as representatives of Norwegian politics and public opinion. State actors may attempt to undermine public trust in politicians and political processes through smear campaigns, disinformation or disruptive activity designed to create unrest. In the worst case, foreign state influence can exacerbate polarisation and lead to a rise in threats and harassment targeting dignitaries.

A **physical confrontation** in this context is a confrontation with physical contact between a dignitary and threat actor. The definition also includes throwing objects or liquids.

EOS services: PST, NIS and NSM

The Norwegian Police Security Service (PST), the Norwegian Intelligence Service (NIS) and the Norwegian National Security Authority (NSM) have adjacent areas of responsibility within intelligence, surveillance and security and are collectively referred to as the EOS services. Their annual national assessments are published simultaneously.

The Norwegian Police Security Service (PST) is Norway's domestic intelligence and security service and reports to the Ministry of Justice and Public Security. PST aims to prevent and investigate serious crimes that threaten national security. This includes identifying and assessing threats related to intelligence, sabotage, the proliferation of weapons of mass destruction (WMD), terrorism and extremism, as well as threats to dignitaries. The assessments are intended to inform policy development and support political decision-making. The National Threat Assessment (NTA) is part of PST's public communications work and sets out expected developments in the threat landscape.

The Norwegian Intelligence Service (NIS) is Norway's foreign intelligence service. It reports to Norway's Chief of Defence, but its work encompasses both civilian and military matters. NIS's core responsibilities are to warn of external threats to Norway and key national interests, to support the Norwegian Armed Forces and defence alliances, and to inform political decision-making by supplying information that is relevant to foreign, security and defence policy in Norway. NIS's annual threat assessment, 'Fokus', presents its analysis of the current threat landscape and expected developments across geographic and thematic areas deemed particularly relevant to Norway's national security and key interests.

The Norwegian National Security Authority (NSM) is Norway's directorate for national protective security. Its primary task is to strengthen Norway's ability to protect itself from espionage, sabotage, terrorism and hybrid threats. NSM helps organisations protect civilian and military information, systems, assets and infrastructure that are relevant to national security by offering advice and conducting oversight, inspections, testing and research. NSM is responsible for a national warning system (VDI), which is designed to uncover and warn of cyber operations targeting digital infrastructure. It also has a responsibility to coordinate the national response to serious cyber incidents. NSM's annual assessment of national security risks, 'Risiko', includes recommendations for mitigating risks and evaluates how vulnerabilities in Norwegian organisations and societal functions affect the risk picture in light of the threat landscape described by NIS and PST.

National Threat Assessment 2026

Published in Norway in 2026 for the Norwegian Police Security Service (PST)

pst.no

Print run: 2000

Images in the publication are sourced from: Getty/NTB

Design and illustrations: Dinamodesign.no

Printing: Konsis.no

Trykksak
2041 0785

THE NORWEGIAN POLICE
SECURITY SERVICE

pst.no