National threat assessment

2024

National Threat Assessment 2024
Published in Norway (2024) for the Norwegian Police Security Service (PST)
pst.no

Circulation: 3000

All faces on the front cover are generated by AI; the basis for the image was provided by NTB
Other images in the publication: Getty Images/NTB

The quote on page 25 is extracted from this article published on BBC News on October 13th 2023: "MI5 head warns of 'epic scale' of Chinese espionage" (https://www.bbc.com/news/uk-67142161)

Design and illustrations: Aksell.no

English translation: Linda Sivesind, Informatic translations

Printing: Aksell.no

Aksell AS is an Eco-Lighthouse enterprise

SVANEMERKET
Trykksak
2041 0379

TRYKT
I NORGE
NO - 1470

USING THE NATIONAL THREAT ASSESSMENT

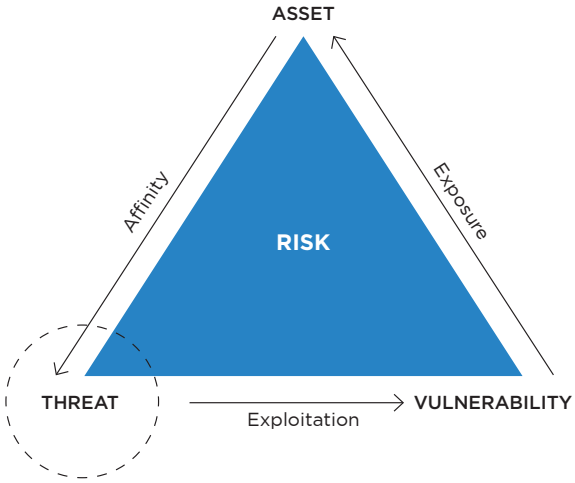
The National Threat Assessment is an analysis of expected developments in PST's sphere of responsibility in the year ahead. It is intended to raise awareness about the most serious threats facing Norway, and to provide informed decision-making support regarding critical preventive security measures for which the various undertakings are responsible. The undertakings must also take into account other threats that could impact the value of their assets, e.g. other crimes or undesirable incidents.

Using the National Threat Assessment in connection with risk assessments:

- Risk can be defined in several ways. In this context, risk is discussed as a combination of assets, threats and vulnerability, and the National Threat Assessment is intended to be used as a resource to inform the assessment of potential risks.

- A good assessment of assets provides grounds for identifying threats of relevance to a particular undertaking. Further, the assessment will highlight ways in which hostile actors can affect an undertaking's assets. In this context, it is also important to examine any dependencies, including those outside the undertaking itself. This will provide grounds for assessing vulnerabilities, and describe the extent to which an undertaking's assets are vulnerable to identified threats, which, in turn, form the basis for establishing preventive and mitigation measures.

- Based on this, a risk assessment must be performed to determine whether an undertaking maintains an appropriate level of security.



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

The Norwegian Intelligence Service (NIS) is Norway's foreign intelligence service. Although it reports to the Chief of Defence, the service's areas of responsibility include civilian as well as military matters. NIS's main tasks are to provide information on external threats against Norway and high-priority Norwegian interests, to support the Norwegian Armed Forces and the defence alliances in which Norway participates, and to assist in political decision-making processes by providing information of special interest in relation to Norwegian foreign, security and defence policy. NIS's annual assessment, 'FOKUS' (FOCUS), is an analysis of the current situation and expected developments in thematic and geographic areas that NIS considers to be of particular relevance to Norway's security and national interests.

The Norwegian National Security Authority (NSM) is Norway's directorate for protective security services. NSM's main responsibility is to improve Norway's ability to protect itself from espionage, sabotage, terror and hybrid threats. Through advisory services, control activities, oversight, testing and research, NSM helps ensure that undertakings protect civilian and military information, systems, objects and infrastructure of importance for national security. NSM is responsible for a national warning system (VDI) intended to identify and issue warnings about cyber operations against digital infrastructure. NSM also bears national responsibility for coordinating the handling of serious cyber operations. A report entitled 'Risiko' (Risk) is NSM's annual assessment of the risks to Norway's national security. The report recommends measures and assesses how vulnerabilities in Norwegian undertakings and services impact risk in the light of the threat picture described by the Norwegian Intelligence Service and PST.

INTRODUCTION

In the National Threat Assessment (NTA), the Norwegian Police Security Service (PST) presents an unclassified review of the threats facing Norwegian society this year. The assessment devotes special attention to intelligence threats, especially those originating with the Russian and Chinese intelligence services, as well as to the threat of terrorism and threats against Norwegian dignitaries.

NTA 2024 addresses a broad, widely diverse target group. On the one hand, the report is intended for members of the general public who require comprehensive information on the status of and expected trend in the threat picture. On the other, the NTA is addressed to individuals and undertakings that require information for their own security efforts, but do not have access to classified assessments. Accordingly, it is important that all those who read this report consider its content and make their own assessments of its relevance to and consequences for their undertakings in the light of the assets they manage. Otherwise, please see *Using the National Threat Assessment* on page three of the report.

Vigilance and tips from the public are important for PST's efforts to avert terrorist attacks, threats against dignitaries, espionage, the proliferation of weapons of mass destruction and transnational oppression, so we therefore urge anyone who might have information of interest to contact us.

> Tips can be submitted to:
> **PST.no/tips-oss**

SUMMARY

State intelligence activities

Page 8

Russia's war of aggression in Ukraine has created a new security policy situation that impacts the threat picture in Norway. The war still continues to heighten the intelligence threat from Russia. At the same time, Norway's membership of NATO and our common border with Russia mean that Russia will use its intelligence services against Norwegian targets in the foreseeable future.

China will be a significant intelligence threat in 2024. We expect that threat to increase in the years ahead. This is due in particular to the deterioration in the relationship between China and the West, China's desire for more control over supply chains, and positioning in the Arctic.

Meanwhile, we expect continued activity on the part of Iran and North Korea against Norwegian targets.

Foreign intelligence services will use a variety of different methods against individuals and undertakings in Norway. Cyber operations and the recruitment of sources will be among the most important methods in 2024. The main objective of cyber operations against targets in Norway will be to gather information. In addition, the goal of certain cyber operations will be to foment uncertainty in society. We expect the Russian and Chinese services in particular to try to recruit sources in 2024. Traditionally, the recruitment of sources takes place through physical meetings. However, a new trend is emerging, involving the recruitment of sources by digital means, such as chat applications.

We expect that Russia and China will be behind most of the attempts to acquire Norwegian goods and technology by covert means in 2024. Their goal will be to strengthen their own armed forces. Moreover, other countries of concern will also try to procure technology that is relevant for their military weapons programmes, including the development of weapons of mass destruction and delivery systems for them.

We also expect that refugees, dissidents and those who criticise regimes will be subject to mapping and monitoring this year.

Politically motivated violence – extremism

Page 28

Extreme Islamism and right-wing extremism are expected to represent the greatest terrorist threats against Norway. We believe there is an **even chance** that extreme Islamists and right-wing extremists will attempt to carry out terrorist acts in Norway in 2024. The threat from extreme Islamists is nonetheless believed to be somewhat more serious than the threat from right-wing extremists.

The threat of terror against Norway is real. Even though extreme Islamism currently enjoys little support in Norway, we have nevertheless seen several serious acts of terrorism in recent years. Statements or actions perceived as insults or oppression of Muslims or the Islamic religion may contribute to radicalisation and, in the worst case, motivate acts of terrorism in Norway.

As regards right-wing extremism, the threat will largely come from the young adults and minors radicalised through right-wing extremist digital arenas. Experience from Norway and other countries indicates that some of them may develop an intention to commit acts of terrorism.

We consider it **unlikely** that anti-government extremists will try to commit acts of terrorism in Norway in 2024. Anti-government ideas and conspiracy theories will nonetheless continue to result in the radicalisation of certain individuals, and such notions may be perceived as justification for the use of violence and non-democratic means.

We consider it **highly unlikely** that left-wing extremists or extremists motivated by climate-related, environmental or nature conservation issues will try to carry out terrorist acts in Norway in 2024. Our assessment is nevertheless that issues related to the climate, the environment and nature conservation have a potential for radicalisation.

Threats to dignitaries

Page 44

We consider it **unlikely** that dignitaries will be the target of serious acts of violence in Norway in 2024. However, we expect that dignitaries will be subjected to threats and harassment. Dignitaries are also vulnerable targets for foreign states' intelligence services.


NORWAY
SWEDEN
FINLAND
Helsinki
Stockholm
Oslo
Tallin
ESTONIA
Riga
LATVIA
LITHUANIA
DENMARK
Copenhagen
North Sea
Baltic Sea
White Sea
UNITED KINGDOM
Amsterdam

State intelligence activities

Russia's war of aggression in Ukraine has engendered a new security policy situation that impacts the threat picture in Norway. The war continues to aggravate the intelligence threat from Russia, compared with before the invasion. At the same time, Norway's membership of NATO and our common border with Russia mean that Russia will use its intelligence services against Norwegian targets in the foreseeable future.

Given the current security policy climate, the intelligence threat from China is also significant. In our view, the threat will gain momentum in the years ahead. Among other things, this is due to China's positioning in the High North, deterioration in the relationship between China and the West, and China's desire to control critical supply chains.

In addition, we expect continued activity on the part of Iran and North Korea against Norwegian targets in 2024.

Individuals, as well as public and private undertakings, are vulnerable to foreign states' intelligence activities. For example, you might be exposed to foreign intelligence in the form of an email with a link you should not click on, a business contact that asks detailed questions about your job, or a company that is interested in buying a product made by your company. The following is a description of which states represent the greatest threat in Norway, and what methods and means they use to strike Norwegian targets.

THE ACTORS

Russia

Russia will represent the greatest intelligence threat against Norway in 2024

Russia has a perpetual need for intelligence in Norway, not least because of our common border and Norway's NATO membership. Political processes of relevance for Russia and military targets in Norway are examples of this. What Russia perceives as military and political threats against the Russian regime will also be given priority at all times. In 2024, the Russian intelligence services will focus on targets related to Russia's warfare in Ukraine.

In the light of this, we expect that the following will be likely targets for Russian intelligence activities in Norway this year:

Photo: minoandriani/Getty Images. Svalbard, Pyramiden.

- **Actors involved in arms donations and the training of Ukrainian personnel:** They are especially at risk of being targeted because arms deliveries could have a direct impact on the battlefield in Ukraine.
- **Undertakings associated with Norwegian oil and gas activities:** They are especially at risk of being targeted because Norway has become a more important energy supplier for Europe since the start of Russia's war of aggression against Ukraine. Russia sees the use of energy-related means as a vital step in fomenting discord in the West.
- **Norwegian technology that has civilian and military utility value:** This field is targeted in particular because Russia depends on western, including Norwegian, technology. Warfare in Ukraine serves to exacerbate Russia's need for western technology, expertise and knowledge.
- **Norwegian defence forces and Allied military activities in Norway:** This area is especially at risk of being targeted, as it has been for quite some time, since Russia would like to get an overview of the capacity and plans of the Norwegian defence forces and their NATO allies. Information about changes in military strategy in response to the enlargement of NATO in the Nordic countries will be of particular interest in 2024 because it will impact how Russia can defend itself in a potential conflict situation.

Russian intelligence activities will be aimed at targets throughout Norway. The High North is nevertheless in a unique position when it comes to attracting the attention of Russian intelligence activities, and this has been the case for some time. It is important for Russia to maintain its understanding of the situation throughout the entire region. This need is becoming increasingly compelling inasmuch as the Arctic has gained strategic significance as tensions have risen in the security policy situation. Svalbard and the border areas in Finnmark County are of exceptional strategic significance for Russia. Norwegian politicians, ministries and others that contribute to Norwegian policy for the High North in general, including Svalbard, will therefore be high-priority intelligence targets. In 2024, the Arctic Council will be of even more interest because Norway has the presidency.

We expect that Russian services will be willing to take great risks in relation to their intelligence activities in 2024 due to their heightened need for information, compared with the time before the war of aggression began in 2022. Meanwhile, they have little to lose by engaging in intelligence activities on Norwegian territory, since bilateral relations between Norway and Russia have reached a new low.

Russia will compensate for the loss of intelligence officers at the embassy

In April 2023, 15 intelligence officers under diplomatic cover at the Russian Embassy in Oslo were declared *personae non gratae* in Norway. This reduced Russia's opportunities to carry out intelligence activities under the auspices of the embassy.

Several arrested for intelligence activities on behalf of Russia

Since Russia's invasion of Ukraine in 2022, at least 35 European nationals have been arrested and indicted at different places in Europe for having engaged in intelligence activities commissioned by the Russian services. For example, they have obtained information about their own countries' defensive capabilities, critical infrastructure and Allied activities, then handed it over to Russian intelligence officers. While some acted in response to pressure, most of them were motivated by monetary incentives. Such cases are indicative of a prolonged high level of activity by Russian intelligence services in Europe.

We expect that Russia will try to compensate for the loss of the intelligence officers. They may do this, for example, by sending more travelling agents and by recruiting sources online. Individuals with family members in Russia or other close ties to Russia will be of particular interest for recruitment attempts. At the same time, we expect that Russia will try to reestablish its intelligence capacity at the embassy in 2024.

In addition, Russia has a wide variety of means available to them that are not affected by the reduced capacity at the embassy. These include cyber operations, signal intelligence and the use of civilian vessels as platforms for intelligence activities.

Russia may also use hybrid means to achieve strategic advantages in relation to Norway. Hybrid means are understood as a state actor's use of a variety of means aimed at one or more targets, and supporting one or more strategic objectives. The means that are combined may be transparent and legal, or covert and illegal, and they are intended to support and reinforce each other to achieve the desired effect. One example of hybrid means might be that Russia combines diplomatic pressure with covert influence operations to influence Norway's political decisions on specific issues.

China

The intelligence threat from China is significant and will grow over time

China will represent a significant intelligence threat in 2024. We expect the threat to grow in the years ahead due to deterioration in the relationship between China and the West, China's desire for more control of supply chains, and its positioning in the Arctic.

Collaboration on research, business, industry, and political ties make Norway an intelligence and influence target for China. Norwegian undertakings, the research and education sector, local and national decision makers, foreign policy groups and individuals who criticise China's government and human rights situation must assume that they will be exposed to both direct and indirect threats from Chinese intelligence actors in the years ahead.

Chinese intelligence actors operate in the grey zone between legal and illegal activities

Even though China's intelligence services are technologically advanced, they use a wide range of actors to carry out assignments on their behalf. Chinese intelligence and influence activities in Norway are largely carried out by intermediaries, Chinese state-owned and private companies, organisations, academic institutions and think tanks.

In addition, Chinese intelligence services recruit Norwegian nationals in an effort to gain access to sensitive and classified information. We expect this to continue in 2024. These are often individuals who have some

Photo: NTB/AP Photo/Ng Han Guan. The Chinese Communist Party Congress, the Great Hall of the People in Beijing, 2022.

affiliation with China through studies, employment, friends or family.

China is characterised by its lack of distinction between the private sector, the state and the Chinese Communist Party. Chinese authorities involve commercial technology enterprises in the modernisation of the country's military. This means that technology and knowledge from all Chinese actors are to be made available to the Chinese military forces, the People's Liberation Army (PLA).

China is still trying to carve out a position in the High North

Its strategic location in the High North, access to natural resources, and proximity to future trade routes make Norway an interesting intelligence target for China. We expect that the Chinese party-state will continue to give priority to its long-term positioning in the Arctic, gradually escalating its presence and intelligence activities. For instance, Chinese research activities on Svalbard can help normalise a Chinese presence, facilitating intelligence activities. China will continue to strive actively to obtain information and to influence Norwegian processes related to the development in the north. On behalf of the Chinese party-state, Chinese commercial actors will seek to establish businesses or infrastructure on strategically located properties in the High North.

Threat actors seek to influence Norway's policy in respect of China

Chinese intelligence services will continue to oppress individuals in Norway who criticise China's form of government and human rights situation. The goal is to undermine opposition to the Chinese Communist Party, as well as to influence Norway's policy in respect of China and discussions about China. Chinese intelligence services use their cyber capacity against government targets in Norway to obtain information about attitudes, decision-making processes and views on issues of importance to China.

The Chinese party-state also works through local Norwegian politicians and business people to promote its foreign policy and circumvent national decision-making processes. This may, for example, involve Chinese actors offering sponsored trips to China, delegations making repeat visits, and the Chinese exhibiting other types of favourable attention. Several Norwegian municipalities and individuals have signed friendship agreements with Chinese actors operating on behalf of the Chinese party-state.

Norwegian technology could support the development of China's military capacity

To resist political and economic pressure from the West, China strives to be self-sufficient in terms of technology. China's increasing control of critical supply chains remains a threat against our innovativeness, as well as against our economic and political freedom of action. In the long term, this could also affect Norway's emergency contingency capability. China uses acquisitions, investments, insiders and research collaboration to obtain information and develop expertise to help build up its own military capacity. In recent years, the number of Chinese organisations and technology centres engaged in overt and covert international transfers of technology has multiplied rapidly. China is Norway's largest collaborator on technological and scientific research projects. This allows Chinese actors considerable freedom of action, either voluntarily or under duress, to transfer Norwegian technology to Chinese military programmes.

- **Personnel associated with the Chinese military (PLA) are in Norway**

  Chinese research managers, visiting foreign researchers and students from institutions associated with the PLA are working in Norway. Research collaboration with personnel associated with the PLA will directly or indirectly support the development of China's military capacity.

Other countries

Iran will try to quell resistance against its own regime and collect information about Norwegian technology

In the year ahead, Iranian intelligence services and actors working on their behalf will continue to engage in intelligence activities aimed at Iranian oppositionists in Norway. Their objective is to quell resistance and criticism against their regime. This is done both through cyber operations and through human-based intelligence activities. As part of Iran's mapping of oppositionists, Norwegian undertakings that have information about such people may also be vulnerable to Iranian intelligence activities.

In 2024, Iran will also deploy some students and researchers to Norway to gain access to civilian technology, research and manufacturing infrastructure intended for the Iranian military as the end user.

The threat from North Korea is primarily manifested in the cyber domain

Also in 2024, North Korea will perpetrate cyber operations against targets in Norway. This will be done for financial gain and to support the country's weapons programme and military armament. In recent years, North Korean cyber actors have carried out several successful cyber operations against financial institutions, and against political and military targets in the West.

Photo: Halfpoint/Getty Images

THE METHODS

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

- **Cyber operations**
- **The recruitment of human sources**
- **Intelligence involving civilian vessels**
- **Influence operations**
- **Sabotage**
- **Covert attempts to make procurements**
- **Economic instruments that threaten security**
- **Transnational oppression**

The threat in the cyber domain is dynamic and constantly evolving

Norwegian undertakings, organisations and private individuals will be subject to cyber operations by state actors in 2024. Operations can be targeted or opportunistic, and they represent a lasting, serious threat against Norwegian society.

The main objective of cyber operations is to obtain information. In addition, cyber operations are increasingly used as a means to foment uncertainty in society, e.g., using denial-of-service attacks. Cyber operations are also used for financial gain and transnational oppression. Although we have not observed any destructive operations in Norway to date, foreign states may carry out this type of operations against Norwegian targets in 2024.

State cyber actors' primary targets in Norway

- **Public administration and political decision-makers**
- **The Armed Forces**
- **Individuals, in particular, individuals in diaspora communities, refugees and regime critics**
- **Undertakings and organisations in the following sectors: finance, health, research and education, aerospace, technology, telecommunications, logistics and transportation, energy and the maritime sector.**

The actor landscape is growing increasingly more complex

Russia and China are the main hostile actors targeting Norway in the cyber domain. Russian and Chinese cyber actors have vast capacity, are very sophisticated, and have maintained a high level of activity against Norwegian targets for several years.

In recent years, North Korea and Iran have also made substantial investments in cyber capacity and have become powerful threat actors in the cyber domain. In addition, other countries have the opportunity to purchase or rent cyber capacity that can be used against Norwegian targets. This makes threats in the cyber domain less predictable.

The actor landscape is also influenced by the fact that the distinction between state and non-state cyber actors is becoming increasingly more diffuse. State actors work closely with private and public cyber security and high-tech enterprises and with hacktivist groups and cyber criminals. These actors help develop states' technical capacity and help carry out cyber operations. That also strengthens state actors' ability to hide their involvement in an operation.

State actors engage in digital industrial espionage

Several state actors have a targeted, specific strategy for using cyber operations as a means to carry out industrial espionage. The purpose may be to improve their own defensive capabilities, boost the state's competitiveness, or avoid sanctions. Through cyber operations, state actors can retrieve vast volumes of data from Norwegian undertakings, which could, collectively, impact national security interests.

North Korean cyber actor stole information from a Norwegian undertaking

In 2022, a Norwegian undertaking was subjected to digital industrial espionage by a North Korean cyber actor. The cyber actor contacted an employee on LinkedIn, introducing himself as a recruiter from an IT company. The communication exchange then moved on to WhatsApp, where the employee was tricked into opening a file that contained malware. The malware gave the actor access to the undertaking's network. The cyber actor retrieved large volumes of data that could damage Norwegian security interests.

Development trends

State cyber actors employ a wide variety of methods. To cover their tracks and make it difficult to ascertain who is behind a cyber operation, multi-layered digital infrastructure is often used.

Supply chain attacks and the integration of home electronics into a cyber actor's infrastructure are examples of this. In addition, we have witnessed advances in the use of zero-day vulnerabilities and social manipulation.

Zero-day vulnerabilities

A zero-day vulnerability is a vulnerability that is unknown to the public, the developer or the manufacturer of a product before it is used in a cyber operation. Such vulnerabilities are hard to identify and prevent. Accordingly, the method is valuable and efficient. State actors continuously search for zero-day vulnerabilities and apply this method frequently. The cyber operation carried out against the Norwegian Government Service and Security Organisation in summer 2023 is one example.

Social manipulation

Several cyber actors are spending more time and resources carrying out reconnaissance on their targets. They exploit the human aspect more and spend time developing a relationship of trust with the victim, before attempting to lure the person in question to click on a malicious link or attachment. They appear more credible and are harder to identify. They use interfaces like LinkedIn, Instagram, WhatsApp and Telegram, in addition to email and SMS messages.

Supply chain attack

Supply chain attacks are cyber operations aimed at weak, more peripheral points in an undertaking's supply chain, e.g., through subcontractors. Undertakings with robust data security systems are vulnerable if their subcontractors do not have similar security measures.

Artificial intelligence can create challenges in today's threat picture

We have not observed that foreign states have used generative artificial intelligence (AI) in cyber operations in Norway. However, we expect they will try to exploit the opportunities presented by rapid technological development in AI to their advantage. For example, AI can be used in influence operations, for social manipulation, or to identify vulnerabilities in software. Similarly, AI can probably also be used to detect and counteract these operations. Whether AI will be most advantageous for those trying to exploit it for offensive cyber operations or for those trying to prevent such operations, remains to be seen.

Photo: gorodenkoff/Getty Images

Expecting physical and digital recruitment of sources

Foreign states' intelligence services will try to recruit sources in Norway this year, too. This refers in particular to the Russian and Chinese intelligence services. One important development trend is that recruitment is taking place through digital channels, rather than solely at physical meetings.

As a rule, foreign intelligence services recruit sources in several steps:

Traditionally, all the steps have involved physical meetings between the potential source and a representative of the foreign intelligence service. For many years, intelligence officers have taken advantage of conferences in Norway to approach potential sources.

This kind of traditional physical recruitment and handling of sources will continue. However, some change is expected.

One important development trend is that foreign intelligence services are also using social media and chat applications for the recruitment and handling of sources. One method we have seen is that contact is initiated by conveying an offer of employment, either for an anonymous employer, or for a seemingly legitimate undertaking. Upon accepting the offer, the source will,

Example of digital recruitment

In 2023, 16 individuals in Poland were arrested and indicted for having performed illegal activities on behalf of Russian intelligence. They were recruited through job vacancy ads published in groups on the chat app named Telegram. Their assignments included taking photos of military targets, spreading Russian propaganda, and sabotaging western weapons deliveries to Ukraine. After submitting documentation to prove their assignments had been completed, the parties involved were ostensibly paid through wire transfers or crypto currency.

for example, be asked to collect information in return for remuneration, and then to transfer the information digitally to Russian intelligence, for instance.

The recruitment of a source could have formidable detrimental effects on Norway. The source could provide sensitive information or critical national information about conditions that would not serve Norway's best interest if such information were to fall into the hands of foreign states. The person in question might also be asked to identify vulnerabilities that could be exploited by an intelligence service, e.g., pertaining to an undertaking's routines, security measures or ICT infrastructure. A source might also be asked to perform practical tasks, e.g., to purchase sanctioned goods or technology, install technical surveillance equipment, harass certain individuals or, as the ultimate consequence, to perpetrate acts of violence or sabotage.

Photo: Justin Pumfrey/Getty Images

Russian intelligence uses civilian vessels in its operations

Intelligence activities are being carried out from civilian vessels in Norwegian waters at all times. We expect this to continue in 2024. Russia represents the greatest threat, but China may also use civilian vessels to collect information about conditions in Norway.

Civilian vessels can be used for a number of different tasks. These include:

- **Information gathering:** The vessels can be used to survey Norwegian and Allied military capacity and activities, as well as critical infrastructure on the seabed and along the Norwegian coast.
- **Sabotage:** The vessels can be used to strike Norwegian or Allied assets on or under the water.
- **Influence:** The vessels can be used to create a situation at sea that is intended to smear or undermine Norway's reputation. A prime example of this might be to stage an accident in an attempt to identify weaknesses in Norway's emergency preparedness or crisis management.
- **Circumventing sanctions regulations:** Fishing vessels with legitimate access to Norwegian ports may be used to smuggle goods and components subject to export control or sanctions.
- **Infiltration:** Civilian vessels can be used to infiltrate intelligence personnel into Norway.

Norwegian nationals will be subject to influence from foreign states

We expect that several authoritarian states, in particular Russia and China, will carry out influence operations in Norway in 2024.

The goal of influence operations is to change opinions held by individuals, groups or the general public to better align with the foreign state's interests.

Influence operations are often carried out digitally through social media. Disinformation and half-truths are spread at a rapid pace there. We expect that foreign states will exploit both new and existing controversies in attempts to polarise and destabilise Norwegian society.

Artificial intelligence can be a helpful tool for foreign states conducting influence operations. AI can be used to raise the quality of the narratives being told, which, in turn, may open new opportunities for foreign states to achieve their goals.

The threat of sabotage is greater due to the war in Ukraine

According to the assessments made by PST and the Norwegian Intelligence Service, Russia may find it prudent to carry out physical or digital acts of sabotage against targets in Norway.

Russia's paramount objective for any act of sabotage would probably be to improve the country's position in the war in Ukraine. If Russia was to feel pressured due to the situation on the ground in Ukraine, the likelihood of acts of sabotage would be greater than if Russia was satisfied with the progression of the war.

Any act of sabotage would most likely be performed in a manner that would make it challenging to prove who was behind it. One important reason for this is that Russia wants to avoid any situation that could trigger Article 5 of the NATO Treaty regarding collective defence.

Targets connected to Norwegian gas exports or Norway's military support to Ukraine are considered to be the most likely targets for any act of sabotage. An act of sabotage on the part of Russia against targets related to Norwegian gas exports might be intended to trigger or exacerbate an energy crisis in Europe. In such case, Russia's paramount objective might be to reduce Norway's willingness to continue military support for Ukraine.

An act of sabotage against Norwegian weapons donations to Ukraine, or related weapons training, could reduce Ukraine's defensive capabilities. The goal may also be to deter other countries from providing additional weapons.

Foreign states will try to acquire Norwegian technology

We expect that Russia and China will be behind most of the attempts to acquire Norwegian goods, services and technology by covert means in 2024. Their primary objective will be to strengthen their own military capacity. Moreover, other countries of concern will also try to procure technology that is relevant for their military weapons programmes, including the development of weapons of mass destruction and delivery systems for them.

A number of Norwegian undertakings manufacture, develop and market goods and technology of interest to foreign states. The export of sensitive goods, services and technologies is strictly regulated. Consequently, countries we are concerned about in this context spend resources to circumvent export control regulations using covert and clandestine methods.

Covert attempts to make procurements will focus not only on military goods, services and technology, but also on dual-use goods. Dual-use goods have qualities that allow them to be used for both military and civilian purposes. One example is equipment for inertial navigation, which is deployed on all modern vessels. Such equipment is needed to maintain a vessel's stability in rough seas. The same equipment is also needed to manoeuvre missiles with sufficient accuracy. Norwegian undertakings must be cognisant of whether their technology may be useful for military applications.

Many fields of technology will be subject to procurement attempts. These include sensor

and detection technology, maritime technology, semi-conductor technology and aerospace and satellite technology, as well as drone and communication technology.

Emerging disruptive technologies such as artificial intelligence, maritime autonomics, biotechnology and quantum computers will also be of interest.

A comprehensive regime of sanctions, as well as more stringent national export restrictions have been implemented against Russia.

A Russian intelligence officer bought subsea technology from a Norwegian undertaking

In 2020, a company in Oslo sold different types of subsea equipment to a Russian. That person wanted to buy increasingly more sensitive products from the same company. The most recent items he wanted to buy could have been used, among other things, to locate subsea cables. After Russia initiated the war of aggression in Ukraine, the undertaking contacted PST. Upon closer examination, the buyer was identified as a Russian intelligence officer. Norwegian undertakings must be aware of this type of escalating procurement activities on the part of actors from countries of concern to us.

However, Russia is still dependent on western technology and expertise to sustain and maintain its military capability. Russian actors also adapt their *modus operandi* to the Western sanctions. For example, they have reduced the quality requirements applying to technology for military applications. This means that a broader range of Norwegian and other western undertakings might be vulnerable to Russian procurement attempts than was the case before the invasion.

To conceal the identity of the real end-user of a product or technology, a threat actor often employs several intermediaries. We have seen Russia and China increasingly using companies in European countries as intermediaries for their procurement activities.

Examples of fields of research of particular interest to foreign states:

- **Nanotechnology**
- **Metallurgy**
- **Cryptography**
- **Robotics and autonomics**
- **Chemistry**
- **Micro-electronic systems**
- **Acoustics**
- **Nuclear physics and cyber security**

> **"If you're working today at the cutting edge of technology then geopolitics is interested in you, even if you're not interested in geopolitics."**
>
> Ken McCallum, Director General of MI5 - United Kingdom's domestic counter-intelligence and security agency

Academic institutions will be subject to illegal intangible technology transfer

We expect that the Norwegian research and development sector will be subject to attempts of illegal intangible technology transfer in 2024. The technology transfer that could enable states to develop military capacity is just as strictly regulated as the export of physical goods.

Norway has several leading technological research communities from which foreign states are eager to learn.

Researchers and students from states we consider a threat may acquire technological expertise and use equipment covered by sanctions and subject to export control while they are in Norway. For example, the Chinese party-state has talent programmes and research parks where they exploit foreign researchers' expertise to strengthen their own military capacity. On that account, institutions and undertakings that engage in research and development bear a special responsibility for assessing whether their own technology has potential military applications.

Economic instruments may give foreign states strategic advantages

We expect that Russia and China will make acquisitions and investments in Norwegian undertakings to ensure a variety of strategic advantages. Such economic instruments are often legal, but they may represent a threat against fundamental national interests when viewed collectively.

Russia will generally use such instruments to cover its military and technological needs, e.g., to purchase properties that are strategically located relative to Norwegian military installations.

China will use economic instruments *inter alia* to ensure control of goods, components and supply chains that are of decisive importance. Examples of this are critical minerals and rare types of soil that occur in large quantities in Norway. Such components are decisive for high technology, not least in fields such as weapons production and the green shift.

One example of how legal economic instruments can threaten security is Chinese companies' entry into western technology markets. Incorporating Chinese technology into Norwegian infrastructure affords Chinese manufacturers an opportunity to install back doors that allow them access points that are extremely difficult to detect.

Critics of the regime will be subject to mapping and threats

This year, PST expects refugees, dissidents and critics of regimes to be subjected to mapping and threats in Norway. This will take place physically during demonstrations and digitally through cyber operations, as well as by mapping on social media. Individuals residing in Norway and their close relatives in their country of origin will be harassed and threatened - both physically and digitally. Some may also be recruited, through pressure or cultivation, to hand over information about diaspora communities and dissident activities in Norway.

Authoritarian states engage in transnational oppression in the form of pressure, threats and, in some cases, lethal violence to thwart criticism against their regimes. Some states use their diplomatic representatives to limit their critics' freedom of expression in Norway. Visiting intelligence officers, organised criminals or infiltrators in diaspora communities are used for this purpose.

Transnational oppression refers to states' use of different means against individuals residing in other countries who are considered a threat against the regime in the executive/responsible state. The purpose of the activity is to undermine or neutralise political opposition.

Example of transnational oppression

In 2022, a dissident in Norway was the target of a spear phishing operation staged by an Iranian cyber actor. To contact the person in question, the cyber actor claimed to be a potential professional partner. The dissident was tricked into clicking on a link to a digital meeting room. The link led to a fictitious login page, where the cyber actor got access to the person's login details. By using them, the cyber actor gained access to email accounts, social media, plans and networks of contacts. The access details were also used to send phishing messages by email and LinkedIn to the dissident's contacts. After being hacked, the dissident was the subject of smears and threats on social media.

Photo: anyaberkut/Getty Images

Politically motivated violence – extremism

The terror threat level in Norway is still at the moderate level. The most serious threats of terrorism in and against Norway in 2024 will continue to originate with extreme Islamists and right-wing extremists. We believe there is an even chance that extreme Islamists and right-wing extremists will attempt to carry out terrorist acts in Norway in 2024. The threat from extreme Islamists appears somewhat more serious than the threat from right-wing extremists.

The increased global focus on the desecration of the Koran and the conflict between Israel and Hamas may adversely impact the threat from extreme Islamists. Thus, the threat can change quickly. The same applies if Norway were to be identified as a terrorist target in terrorist organisations' propaganda.

The threat from right-wing extremists is complex and unpredictable. Online platforms will continue to be the main arena for radicalisation, where individuals can be inspired to commit acts of terrorism. Right-wing extremism still includes a transnational dimension, where we witness inspiration spreading across national borders.

In anti-government extremism, distrust of the authorities will continue to fuel conspiracy theories. It is the potential for violence in these theories that gives cause for concern. The climate, the environment and nature conservation also have the potential to radicalise certain individuals. Left-wing extremism will continue to be a marginal phenomenon.

THE COMMUNICATION OF THREATS

Degrees of probability in the assessments of politically motivated violence – extremism

The field of politically motivated violence – extremism – uses a set of standardised terms for degrees of probability. The purpose of this is to create a more uniform description of probability in the assessments and thereby to minimise the risk that they are unclear or could be misunderstood. The terms and their associated descriptions have been compiled jointly by the police, the Norwegian Armed Forces, and PST.

National standard	Description	Percentage
Highly likely	Very good reason to expect	>90%
Likely	Good reason to expect	60–90%
Even chance	Equally likely and unlikely	40–60%
Unlikely	Little reason to expect	10–40%
Highly unlikely	Very little reason to expect	<10%

PST's terrorism threat scale

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

The scale applied has five levels, from level 1 that is **no** threat of terrorism to level 5 that involves a **critical** threat of terrorism. In determining threat levels, PST takes into account the current threat assessment, along with an assessment of (*i*) the degree of severity/damage potential of any possible terrorist act, (*ii*) uncertainty and the scope of the shortcomings in the intelligence related to relevant hostile actors, and (*iii*) our/the authorities' ability to implement countermeasures before any threats are carried out.

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

The threat from extreme Islamism

We believe there is an **even chance** that extreme Islamists will attempt to carry out terrorist acts in Norway in 2024. The threat of terror primarily comes from individuals who are inspired by the ideology and message of the terrorist organisations the Islamic State (ISIS) and al-Qaeda. The threat is considered to be somewhat higher this year than last year, owing to the increased global focus on the desecration of the Koran and the conflict between Israel and Hamas.

The threat picture could be further exacerbated if Norway were to be singled out as a terrorist target in terrorist organisations' propaganda. In addition to being able to inspire sympathisers to commit acts of terrorism, such propaganda may indicate that the terrorist organisations *per se* intend to use their own networks to strike Norway and Norwegian interests.

- **By 'extremism', we mean acceptance of the use of violence to achieve political, religious or ideological goals. While extremists accept the use of violence, they do not necessarily engage in violence themselves.**

- **By 'radicalisation', we mean a process whereby an individual develops an attitude of acceptance for or a willingness to actively support or take part in violent acts to achieve political, religious or ideological goals.**

Any extreme Islamist terrorist act in Norway would probably be committed by a lone individual or a small group of perpetrators. Ideological guidelines and propaganda indicate that civilian populations, institutions and individuals perceived as insulting the Islamic religion, as well as uniformed police and military personnel, will often be identified as targets for attacks in the West. The threat against Israeli and Jewish targets will be aggravated due to the war between Israel and Hamas.

Expecting more attacks in the West

The planning of attacks in Western countries increased in 2023 compared with the two previous years. This trend is expected to continue in 2024. The perception that the West is at war with Islam, oppressing Muslims, and offending Islam, are key factors used as justification for terrorist attacks and for radicalisation to extreme Islamism. Since global attention is currently focused on these factors, they are expected to have an adverse impact on the threat picture.

Extreme Islamists interpret Israel's warfare against Hamas as part of western military warfare against Muslims and the occupation of Muslim land. Many also maintain that Israel receives moral and military support from an alliance of Western countries. Despite the Norwegian authorities' explicit support for a cease-fire in Gaza, most extremists would define Norway as part of western military warfare and thus as a potential legitimate target. There is, however, little indication that

Norway is a high-priority target. The prolonged and violent conflict between Israel and Hamas will result in the hatred of Israelis and Jews becoming a more salient factor in the motivation of extreme Islamists when they aspire to carry out attacks in the West.

In addition, perceived transgressions against Islam, such as burning the Koran and the publication and use of Mohammed caricatures, could lead to radicalisation and terrorist plots in Europe, since extremists interpret such acts as blasphemous. The Koran burnings in Sweden in January, June and July 2023 fuelled more activity on the part of ISIS and al-Qaeda, and both organisations have subsequently encouraged attacks to avenge the Koran desecrations. Retaliatory actions for such acts may come immediately after the acts have taken place, or months or even years later. We expect that desecrations of the Koran will also occur in 2024. The threat picture in Norway could change rapidly if Koran desecrations in Norway were to attract increased media focus, or if fake news or misunderstandings about this were to gain traction. If a development were to result in Norway being named in official calls for acts of terror on the part of terrorist organisations, this would have a negative impact on the threat picture.

The changing threat picture in 2023 illustrated how quickly isolated events can adversely impact the threat situation in the West and in Norway. We believe that both revenge for Koran burnings and the war between Israel and Hamas will also colour large parts of 2024. Meanwhile, new events that adversely impact the threat picture could take place without warning.

Sweden and Denmark are experiencing a greater threat of terrorism

In 2023, Koran burnings, especially in Sweden and Denmark, attracted attention internationally and among extreme Islamist terrorist organisations. As a consequence of Sweden being explicitly identified as a target by terrorist organisations, the Swedish Security Service raised the terror threat level to level 4 (high) of 5 possible levels last autumn. The Danish Security Service also stated last autumn that the threat against Denmark has been raised within the current level, which was already at level 4 (high) of 5 levels.

Transnational ties have a negative impact on the threat of terror in Norway

There are few active extreme Islamists in Norway and no physical openly extremist communities. However, extreme Islamists recognise no national borders, maintaining that they are part of a global religious community. In addition, they are motivated by the same core issues as extreme Islamists in other countries. In future as well, we will therefore continue to expect that terrorist plots and attacks could impact Norway.

There are persistent concerns associated with extreme Islamists convicted of terrorism in Europe and subsequently released. More such convicts will be released from European prisons in future. There is little to indicate that they have been de-radicalised. Many are expected to rejoin the extremist networks they belonged to prior to their imprisonment, or to form new networks. Current and future contact between individuals in Norway and these networks could adversely impact the threat picture in Norway.

According to the Norwegian Intelligence Service's assessment in *Focus 2024*, the global terrorist organisations ISIS and al-Qaeda will continue to give priority to their build-up outside of Europe, in their core areas. The terrorist organisations are gathering momentum on the African continent in particular, where they are expanding in several places. Some years from now, this build-up could potentially affect the threat picture in the West.

The threat of terror in Europe will also be influenced by the stability of Afghanistan as a state. We expect that the Afghan branch of ISIS will try to carry out attacks on our continent to undermine the Taliban's ability to govern.

Even though certain Norwegian extreme Islamists might want to travel to areas of conflict as foreign fighters, they will have limited opportunities to participate in foreign fighter activities in 2024. This is because there are few easily accessible areas in which terrorist groups can receive non-regional foreign fighters. In the years ahead, this could, however, change if these groups achieve more stable control over land areas.

Contact between extreme Islamists in Norway and interned foreign fighters in prisons and camps in Syria could adversely impact the threat of terror in Norway. Those who are interned could help radicalise contacts in Norway or put Norwegian extremists into contact with ISIS members locally in Syria.

Online radicalisation is a persistent challenge

Extreme Islamists are, and will continue to be, part of small transnational online networks. Encrypted platforms allow users to behave and communicate anonymously and they are therefore used to establish such networks. Relationships are formed through these networks, and participants develop the trust needed to plan and support terrorist activities. Extremist propaganda, recipes for home-made explosives, and guidance on

how to carry out terrorist attacks are disseminated there.

Minors will also be taking part in transnational digital networks. A great deal of the extremist propaganda is formulated and distributed in a manner that also appeals to a younger audience. We expect that minors will also be taking part in the production and dissemination of extreme Islamist propaganda. Minors who are attracted by such networks and propaganda might be vulnerable, impressionable and generally have less understanding of the consequences of their actions than adults do. That may increase the probability that young people will be incited to carry out acts of violence and terrorism. It is nonetheless challenging to detect radicalisation through encrypted digital platforms.

Moreover, we expect that radicalisation will continue to take place through physical relationships, especially among friends and in families, at schools, in religious arenas and in prisons. The distinction between digital and physical networks will be fluid, and radicalisation will take place in both arenas.

Norwegian extreme Islamists will continue to support global terrorist and extremist organisations in regional conflicts to which they themselves have links. There are continuous fund-raising campaigns on different online fora in support of extremists and terrorist groups.

Simple, readily available means of attack are still the most likely course of action

Any extreme Islamist terrorist act in Norway will probably be committed by a lone individual or a small group of perpetrators. The perpetrators will often be in contact with other extremists prior to the act, either digitally or physically. In some cases, they will also receive guidance from extremists in other countries.

The perpetrators are expected to employ simple, readily available means of attack, e.g., axes, knives, machetes, hammers, arson or vehicles. However, averted attacks indicate that extreme Islamists prefer to use improvised explosive devices (IEDs) and firearms. If IEDs are used, they will most likely have a relatively simple structure and mode of operation. Firearms may include pistols, shotguns and rifles, and they may be procured legally or illegally.

Extreme Islamists will often want to be killed during an attack. Fake bomb belts or the like have been used on several occasions to provoke a lethal response from the police, preferably in combination with other means of attack.

Ideological guidance and propaganda indicate that civilian populations, institutions and individuals that are perceived to insult the Islamic religion, as well as uniformed police and military personnel, will often be identified as targets for attacks in the West. In addition, meeting places for members of the LGBTQ+ community as well as religious

Photo: Getty Images

meeting places have recently become more likely terrorist targets. This assessment is based on the targets chosen for completed and averted terrorist attacks.

The threat against Israeli and Jewish targets will be aggravated by the war between Israel and Hamas. Since the USA is perceived as a firm supporter of Israel, the threat against US targets is also considered higher. The terrorist organisations have called for attacks against all countries that support what they consider to be the West waging war against Islam, as well as all countries that allow Islam to be exposed to what they perceive as acts of blasphemy.

The threat from right-wing extremists

We believe there is an **even chance** that right-wing extremists will attempt to carry out terrorist acts in Norway in 2024. Right-wing extremist digital platforms will continue be primary arenas for radicalisation and inspiration for attack planning. Any right-wing extremist terrorist attacks will most likely be carried out by a single individual, and be directed at groups that fit right-wing extremists' image of the enemy. Mass casualty attacks or targeted assassinations against individuals are considered to be the most probable forms of attack.

The threat picture is becoming increasingly complex and unpredictable

Those radicalised to right-wing extremism draw their ideas and inspiration from different arenas. This may include ideas from right-wing radicals and from right-wing extremist ideological communities, as well as from digital communities that do not have clear ideological elements. Thus, the right-wing extremist threat picture is becoming more unpredictable and complex.

Nevertheless, right-wing extremists continue to be united by some shared ideas about how the world works. One central idea is that the state and the people should be organised on the basis of shared biological or cultural traits. Such ethnic nationalism involves a desire to maintain racial and cultural purity. Another basic tenet is that the 'white race' and culture are in the process of being obliterated. This perceived existential fear makes right-wing extremists believe that violence is legitimate to prevent this

What distinguishes right-wing extremists from right-wing radicals are their views on democracy and whether or not they are willing to accept violence to incite political change. Right-wing extremists aspire to dismantle democracy and accept the use of violence. However, that does not apply to right-wing radicals.

Key right-wing extremist conspiracy theories

The *Great Replacement* asserts that western governments intentionally try to subsume the 'white' and western population, ostensibly not only allowing but facilitating mass immigration from non-western countries.

The *Zionist Occupied Government (ZOG)* accuses Jews of working covertly to try to achieve world domination. This supposedly takes place by controlling authorities, politicians, the media and banking, among other things, in western states.

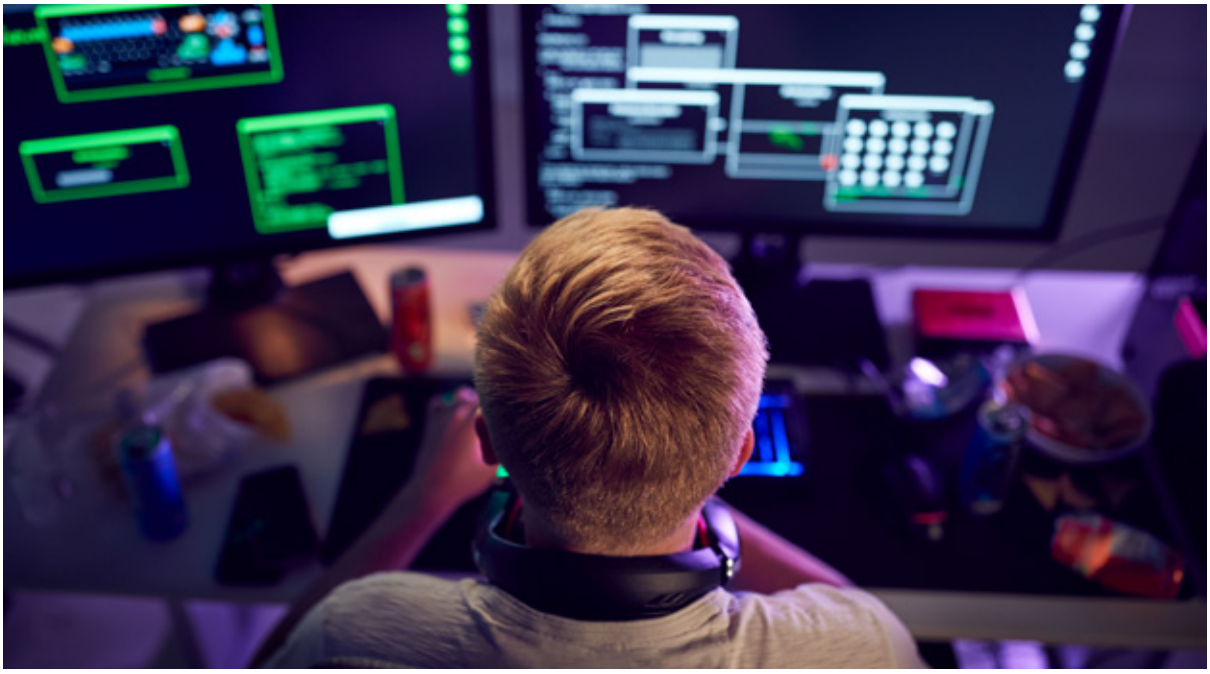


Photo: monkeybusinessimages/Getty images

annihilation. This will often be related to a fundamentally conspiratorial understanding of the world.

Right-wing extremists have a persistent hatred of minorities and the Norwegian authorities. The image of the enemy is broad and includes Jews, Muslims, individuals with a non-Western appearance, the Norwegian authorities and politicians, and members of the LGBTQ+ community, traditional media and left-wing extremists. They are seen as contributing significantly to the 'white race' or western culture dying out, a view supported by conspiracy theories.

Still a real threat of terrorism

In 2019, there was a substantial increase in the number of right-wing extremist terrorist attacks in the West, both completed and averted. Since 2020, the number of completed and averted attacks has remained at a lower level. In spite of this, right-wing extremist terrorist attacks are still being completed and averted in the West. This means the threat from right-wing extremists in the West, and in Norway, is real.

What might trigger radicalisation, and lead certain individuals to develop the intention to commit terrorist acts, will vary, and it can be a challenge to foresee. It may involve personal issues, or also possibly events or developments that take place at the local, national or international level. That being said, there are some overriding factors that could push people toward radicalisation in 2024.

One such factor revolves around current events and developments that support right-wing extremists' idea that the 'white race' is in jeopardy and faces an existential threat. Examples of such topics are non-Western immigration, and the perception that the society is experiencing moral decay. Among other things, this may be attributed to a discussion about liberal gender identity, as well as a perceived normalisation and expansion of LGBTQ+ rights.

Another factor is the inspiration effect. Completed right-wing extremist terrorist attacks and the perpetrators behind them are still important sources of inspiration. Thus, right-wing extremism still has a transnational dimension, where potential threat actors influence each other across national borders. New right-wing extremist terrorist attacks will also serve to inspire others to engage in terrorism. This may be further reinforced through manifestos and attack videos.

A third factor is accelerationism as an ideological direction. Even though today's right-wing extremism is ideologically complex, there is sustained concern about accelerationism. The glorification of violence and terrorism as methods, the focus on individuals committing acts of terrorism, and the belief that it is urgent to bring about the collapse of society means that we consider this ideological direction to be an especially potent threat. Our experience is also that it need not necessarily take long from the time a person is radicalised until that person decides that he/she is willing to commit a terrorist act.

The ongoing war in Ukraine and the war between Israel and Hamas do not affect the threat from right-wing extremists to any particular extent. This is because these conflicts have no clear ideological importance for Norwegian right-wing extremists. We do not see that the conflicts have resulted in more recruitment, radicalisation or mobilisation. Certain Norwegians who are affiliated

Accelerationism is an ideological direction within right-wing extremism. The idea that a 'race war' is imminent is a major factor, and time is of the essence when it comes to bringing about the collapse of society while "the white race" still has a demographic majority in the West. Accelerationists extol terror as an important tool for destabilising society and igniting a 'race war'.

The perpetrators of several completed and averted right-wing extremist terrorist acts in the West in recent years have been inspired by this idea.

with right-wing extremism have nonetheless participated in the war in Ukraine. One concern in this context is related to more extensive battlefield experience, a lower threshold for violence, and contact with other extremists. The war between Israel and Hamas has given rise to even greater anti-Semitism, and thereby further cast Jews in the image of the enemy.

Digital platforms will continue to be the main arena for radicalisation

Digital platforms will continue to be the main arena where individuals become radicalised to right-wing extremism. A number of platforms (open, closed, national and transnational) will continue to be used for communication and the dissemination of propaganda. The users will generally be anonymous, and many will participate in several fora at the same time. Algorithms in digital searches and social media can lead individuals to post more extreme content.

Right-wing extremist digital fora will continue to be characterised by an internal dynamic. In this context, the focus on violence will be commingled with ideology, humour, symbolism and pop culture. Through propaganda and memes (digital images and text with a humorous bent), a dehumanising message will be produced to corroborate the notion that groups considered to be the enemy are working behind the scenes to ensure that the 'white race and culture' will die out. Several such digital fora often also glorify masculinity, and promote intense misogyny. Extremism disguised as humour can help normalise the

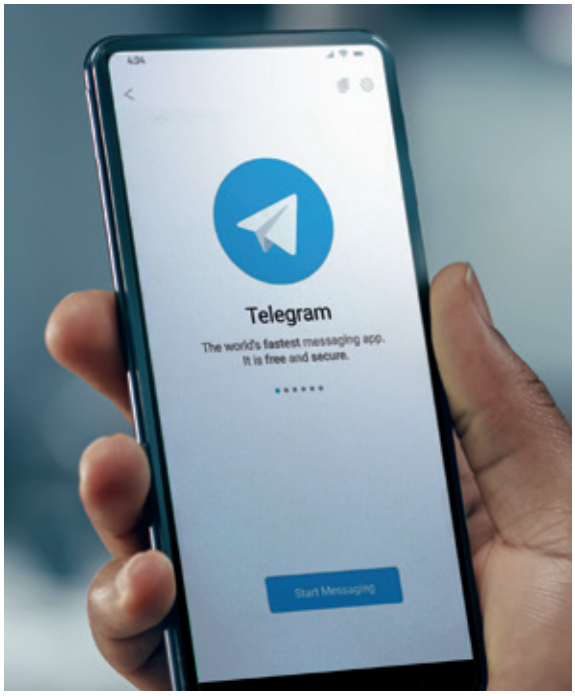


Photo from Getty Images. Open, encrypted digital platforms such as Telegram are major arenas for communication and the sharing of propaganda among extremists.

messages. For certain individuals, this could lower the threshold for committing violence.

In addition to right-wing extremism in cyberspace, there will still be right-wing extremist activities in physical spaces. PST's concern is that such physical arenas could cause some individuals to be radicalised.

Our experience is that many individuals who are attracted by right-wing extremist communities are often guided there for reasons other

than ideology. Their affinity may be based on social fellowship, entertainment, or a fascination with violence, or on politically incorrect communication, or they may be there for the aesthetics and meme culture. Even though ideology is not generally the primary reason why they are participating, repeated exposure to one-sided ideas and dehumanising rhetoric can allow the ideological aspect to gain traction. Some may take the message about carrying out acts of violence or terrorism seriously, resulting in rapid radicalisation. For security and intelligence services, it is a constant challenge to predict who might progress from consuming and publishing violence-inciting rhetoric on the Internet to actually perpetrating an ideologically motivated act of violence.

Even though there is a broad range of ages among the individuals being radicalised, we are particularly concerned about minors and young men who participate in right-wing extremist digital fora. One characteristic feature is that these individuals experience different ways of feeling like an outsider, or have other vulnerabilities, including poor mental health.

Mass murder and targeted assassinations of individuals who fit the image of the enemy are most likely

A right-wing extremist terrorist attack will most likely be aimed at individuals, groups or institutions that fit right-wing extremists' stereotype of the enemy, e.g., religious minorities, members of the LGBTQ+ community, politicians, traditional media and the authorities.

Schools may also be vulnerable terrorist targets. For minors and young adults who are right-wing extremists, schools may be familiar and readily available targets, where individuals who fit their stereotype of the enemy can be found.

Critical infrastructure has also been identified as a potential target for terrorism in extreme right-wing transnational propaganda. The accelerationist doctrine emphasises this in particular for the purpose of triggering the collapse of society. However, we have not found this to be a focal point for Norwegian right-wing extremists.

Target selection is also influenced by availability, safety measures and the geographic location of potential targets, as well as by their symbolic value. The form of attack can vary from targeted assassinations of individuals to attempts at mass murder.

Any right-wing extremist terrorist attacks in Norway will most likely be attempted by a single individual. The perpetrator will most likely use firearms or simple improvised explosive devices (IEDs), but vehicles and axes, knives, machetes and hammers may also be relevant means of attack.

We also see growing interest in home-made 3D-printed firearms on the part of transnational right-wing extremist groups. It is, however, demanding to make effective, functional 3D-printed firearms with high capacity. Accordingly, it is considered less likely that we will see such weapons than ordinary firearms among Norwegian right-wing extremists in 2024.

The threat from anti-government extremists

We consider it **unlikely** that individuals with anti-government convictions will try to carry out acts of terrorism in 2024.

It is the potential for violence inherent in anti-government ideas that gives cause for concern. In the worst case, the perceived enemy might be considered dangerous enough to legitimise violence and terror. This applies in particular where the conspiracy theories have a revolutionary and apocalyptic focus.

Over the past year, the absence of an all-embracing banner issue, like the Covid-19 pandemic, has mitigated the threat from anti-government extremists somewhat. Distrust of the authorities will continue to be a driving force and to fuel conspiracy theories. Events that exacerbate the conspiracy theories that include an element of violence will nonetheless escalate the threat once again.

Anti-government extremism

Anti-government extremism embraces ideas and conspiracy-like theories that include an element of violence. Anti-government convictions do not have the religious or ideological grounding familiar to us from other forms of extremism such as extreme Islamism and right-wing extremism.

Transnational development trends will influence the image of the enemy and conspiracy theories

Combined with the view that the state is not legitimate, continued notions of the 'deep state' and similar all-encompassing conspiracy theories will be the main movements within anti-government extremism in Norway in the year ahead.

The essence of anti-government theories will largely remain the same. However, their development will be dynamic, related to societal trends and adapted to national and local factors. This means there are several different potential gateways to radicalisation, and it is not easy to keep abreast of and prevent all of them. We are still concerned that disinformation campaigns run by certain foreign states will exploit anti-government ideas for influencing purposes, and that this could lead to radicalisation moving in the direction of anti-government extremism.

The 'deep state'

The idea that authorities and pillars of society conspire with, or work for, a secret network or a hidden elite that seeks world domination.

Norwegian authorities and others associated with the ruling powers are considered the main enemies of anti-government actors. Conspiracy theories about what is perceived as the authorities' ostensibly malicious agenda and global alliances are ideas that are reinforced by current events. Further, we expect that anti-government extremists and right-wing extremists will continue to have fluid, partially overlapping stereotypes of the enemy.

The choice of targets will shift in tandem with the conspiracy theories

Any anti-government terrorist attacks will be directed at targets that represent the State or are associated with the authorities, i.e., infrastructure, symbolic targets or dignitaries. The purpose of striking such targets is the desire to overturn the existing system, or to identify conspiracies. However, trends in conspiratorial convictions can alter the image of the enemy and influence the choice of targets.

At times, the threat from anti-government extremists will move through a grey zone between politically motivated violence and incidents that fall within the police's sphere of responsibility, such as vandalism and disturbance of the peace.

The threat from left-wing extremists

We consider it as **highly unlikely** that left-wing extremists in Norway will try to carry out acts of terrorism in 2024. We do not expect that the groups will grow much in the coming year. The struggle against right-wing extremism will continue to be the main focus, bringing together left-wing extremists in Norway.

Left-wing extremists' ideological convictions will continue to be rooted in various forms of anarchy, Communism and anti-fascism that glorify violence. In Norway, the groups are marginal, and we do not expect them to grow to any great extent in 2024.

The fight against right-wing extremism will continue to be the main focus of left-wing extremists in Norway in 2024. We expect that certain left-wing extremists will continue to commit politically motivated acts of violence against individuals they assume to be right-wing extremists, but that they themselves will define this as self-defence. Such acts of violence will most likely be limited to using blunt weapons and physical attacks. We also expect that there will be incidents of vandalism and public harassment of individuals assumed to be right-wing extremists.

We expect that left-wing extremists will support the Palestinian side in the Middle East. In the short-term, the conflict could generate enthusiasm among left-wing extremists. This will primarily result in actions to be viewed as activism, disturbances of the peace and/or vandalism. This will fall under the sphere of responsibility of the police.

Extremism associated with climate, the environment and nature conservation

We consider it **highly unlikely** that actors focused on issues related to climate, the environment and nature conservation will attempt to carry out acts of terrorism in 2024. The majority of these actors will continue to use non-violent means to draw attention to their issues. However, our assessment is that this topic does have the potential to radicalise certain actors.

We expect that actors concerned with the climate, the environment and nature conservation will largely continue to use democratic means to promote their issues in 2024. Some will no doubt also turn to unlawful means such as disturbing the peace and civilian disobedience. These are non-violent methods and will fall under the police's sphere of responsibility.

All the same, we would maintain that this topic has the potential to radicalise certain actors. For some people, an existential fear and a perceived lack of action from political quarters might be considered justification for the use of violence to achieve their political goals.

Any acts of violence will most likely be directed at infrastructure and property since they are seen as sources of greenhouse gas emissions. Violence against people is considered less likely. Accordingly, politically motivated sabotage is something we may see more of in future.

Controversial and current events related to the topic, and subsequent conflicts of interest, will further add to the threats against dignitaries and local politicians.

Illustrative photo: leonello/Getty Images


POLITI

Threats to dignitaries

We consider it unlikely that dignitaries will be the target of serious acts of violence in Norway in 2024. However, we expect that dignitaries will be subjected to threats and smears.

Even though violent attacks against dignitaries are very rare occurrences, individuals in prominent positions will always be vulnerable. It is also a serious challenge to democracy if elected officials engage in self-censorship or withdraw from office as a result of strains caused by smears and threats over time.

Dignitaries are also vulnerable targets for foreign states' intelligence services.

Dignitaries that fall under the mandate of PST include members of the Royal family, the Government, the Storting (Norwegian Parliament), and the Supreme Court, as well as representatives of comparable bodies from other states when they are in Norway.

We consider it **unlikely** that dignitaries will be the target of serious acts of violence in Norway in 2024.

Nonetheless, we are cognisant of a stable high level of threats and smears against dignitaries and politicians in Norway. Some will also experience spontaneous confrontations and minor acts of violence. Those who receive a great deal of media attention and who are associated with issues that evoke emotional involvement are especially vulnerable.

Frustration and strong political dissatisfaction can lower the threshold for individuals to use hate speech and make threats. Economic downturns and a distrust of politicians can exacerbate this. Controversial issues and international incidents can lead to more or worse threats against certain dignitaries in Norway, including diplomatic representatives and other foreign dignitaries present in Norway.

The majority of the threats registered against dignitaries in Norway will continue to come from personally motivated threat actors. Their threats will often be influenced by mental illness and/or substance abuse.

Dignitaries are also included in the image of the enemy held by several different groups of extremists. However, extremists maintain a broad stereotype of the enemy, where dignitaries account for just one of several relevant targets. Safety measures make other targets more accessible and attractive.

Very few of the people who make threats genuinely intend to engage in violence. However, numerous threats and smears published on social media are currently certainly adding to the complexity and uncertainty of the threat picture. A climate of free speech that normalises and legitimises violence against political opponents can ultimately help ensure that certain vulnerable individuals are inspired to carry out acts of violence.

One basic prerequisite for a smoothly-functioning democracy is that our elected representatives can do their jobs without fear of violent reprisals. A growing number of elected officials restrict or censor the political statements they make in public due to smears and threats. Some have withdrawn from politics, or are considering doing so. This undermines our democratic system.

Dignitaries are also vulnerable targets for foreign states' intelligence services. Several foreign states, especially Russia and China, will continue to pursue the goal of gathering intelligence about Norwegian political processes that could affect their interests. This implies that several Norwegian politicians, and people who work in the system surrounding them, may be targets for foreign states' intelligence and influence activities in Norway in 2024.

Report tips to us!

PST's main responsibility is to prevent and investigate punishable acts that threaten the country's security. We depend on good contact with the public in order to avert any terrorist attack against Norway, threats to dignitaries, espionage and the proliferation of weapons of mass destruction.

If you have any tips, contact us at:
PST.no/tips-oss

Politiets sikkerhetstjeneste
pst.no