# National threat assessment 2021

PST
POLITIETS SIKKERHETSTJENESTE

**The national threat assessment** made by The Norwegian Police Security Service is one of three official threat and risk assessments published during the first quarter of every year. The remaining two are published by the Norwegian Intelligence Service and the Norwegian National Security Authority.

**The Norwegian Police Security Service (PST)** is Norway's domestic security service, and is subordinate to the Ministry of Justice and Public Security. Its main task is to investigate and prevent serious offences that threaten national security. This includes the identification and assessment of threats related to intelligence, sabotage, the spread of weapons of mass destruction, terrorism and extremism. The assessments provide a foundation for policy-making and political decision-making processes. PST's annual threat assessment is part of the service's duty to inform the public and presents an analysis of expected developments within its areas of responsibility.

**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 supply information on external threats to Norway and high-priority Norwegian interests, to support the Norwegian Armed Forces and the defence alliances to which Norway belongs, and to assist in political decision-making processes by providing information on matters relating to Norwegian foreign, security and defence policy. NIS's annual assessment, Focus, is an analysis of the current situation and expected developments in geographic and thematic areas that are particularly relevant to Norwegian security and national interests.

NSM

**The Norwegian National Security Authority (NSM)** is the professional and supervisory authority within the protective security services in Norway. It advises on and supervises security of information, information systems, objects and infrastructure of national importance. NSM also has a national responsibility for cybersecurity, including the detection, notification and coordination of responses to serious cyber attacks. In its annual report Risiko, published in the first quarter of the year, NSM assesses the risk of Norwegian society being subjected to intentional acts that may directly or indirectly harm critical national interests.

# Introduction


**The 2021 threat assessment** has been compiled during a global pandemic. The national authorities in most countries are facing huge challenges as they attempt to safeguard the needs of their citizens in terms of health and financial security. The national lockdowns and extensive travel restrictions come at a high cost, and it is difficult to predict the long-term consequences of the covid-19 pandemic and how these will affect the threats facing Norwegian society.

**Cyber threats** will continue to be an issue in 2021. The threats represented by the intelligence activities of foreign states are serious, and there is no reason to believe that they will diminish. Extremist groups and potential terrorists are being formed and influenced by propaganda in online networks. Thus the work of identifying, detecting and preventing threats in cyberspace affects most of PST's tasks in its various areas of responsibility.

**PST's national threat assessment** is an integrated part of its communication with the public. The target group is those members of the public who wish to know about expected developments in the threats facing Norwegian society. In drafting the assessment we need to strike a balance between simplicity, clarity and the need to present a set of general evaluations, and it is up to the individual user to adapt the information to their own activities. We also expect users to notify PST if they become aware of any of the issues discussed in the assessment.

**PST's evaluation of developments** in the threat picture in the coming year should be viewed in the context of two supplementary analyses. One of these is NIS's report FOCUS 2021, which discusses which developments taking place abroad will be of interest to Norway and Norwegian security. The second is NSM's report RISIKO 2021, which discusses vulnerabilities in Norwegian organisations and evaluates risks to national security.

# Degrees of probability

The following is a list of the degrees of probability used in this assessment. The aim is to reduce as far as possible the risk that our evaluations are unclear or could be misunderstood. The following terms and definitions have been developed in cooperation between the police, PST, NIS, and the Armed Forces.

## Highly likely

**There is very good reason to expect**
**More than 90 % probability**

## Likely

**There is good reason to expect**
**60–90 % probability**

## Even chance

**Equally likely and unlikely**
**40–60 % probability**

## Unlikely

**There is little reason to expect**
**10–40 % probability**

## Highly unlikely

**There is very little reason to expect**
**Less than 10 % probability**

# Summary


**State intelligence activity**
**Pages 5–15**

Several countries' intelligence services will dedicate considerable resources to intelligence activity in Norway in the coming year, with the aim of obtaining information and influencing decisions. The greatest threats will come from Russia and China.

Russian and Chinese intelligence activities will be mainly concentrated on computer network exploitation. Cyber espionage is cost-effective and has a lower risk of detection than other intelligence methods.

Foreign intelligence services will seek to map Norwegian infrastructure and try to recruit insiders. Russian intelligence officers devote a good deal of time to cultivating contacts with individuals in Norway.

Foreign intelligence services can obtain information and influence that will prejudice Norwegian interests through acquisitions and investments targeted at Norwegian businesses.

In the coming year several countries will try to obtain Norwegian technology illegally. Some will also make use of contacts in the academic world with a view to acquiring knowledge illegally.

Authoritarian regimes identify and spy on refugees and dissidents living in Norway, and individuals belonging to exile communities may be subjected to threats.

## Politically motivated violence – extremism
Pages 16–29

Islamic extremism and right-wing extremism are still expected to represent the greatest terrorist threats to Norwegian society. There is an even chance that one or more of these extremists will try to carry out a terror attack in Norway in 2021.

The threat posed by Islamic extremists will be higher in the coming year. This is due to the increased tension between freedom of speech and utterances that many Muslims feel are a desecration of Islam. This may inspire certain individuals to plan terrorist acts.

Radicalisation to right-wing extremism is also expected to become more wide-spread. Online platforms are important arenas for radicalisation and may inspire right-wing extremists to plan terrorist acts.

Attempts at terrorism by left-wing extremists are highly unlikely. However, combating right-wing extremism will continue to be a rallying point for this group.

Anti-state movements that regard the state as an illegitimate entity have the potential to radicalise individuals in 2021.

Environmental activism has the potential to radicalise individuals over the long term.

## Threats to dignitaries
Pages 30–34

Threats against dignitaries are expected to increase somewhat in the coming year. They are likely to be inspired by opposition to covid-19 restrictions, the greater number of radicalised right-wing extremists and the increased publicity of certain issues and politicians in connection with the parliamentary elections in the autumn.

# State intelligence activity

**In the coming year foreign intelligence services will devote considerable resources to infiltrating Norwegian computer networks and will attempt to recruit sources and agents in Norway. The intention is to obtain access to information and influence Norwegian decision-making processes. The greatest threats will come from the Russian and Chinese intelligence services.**

**A Russian hacking group is likely to have been responsible for cyber attacks on the Storting in 2020.**

Foreign Minister Ine Eriksen Søreide meets the press outside the Ministry of Foreign Affairs.

PHOTO: ØRN E. BORGEN / NTB

**Why are intelligence operations harmful to Norway?**
Whereas the consequences of a terror attack are immediate, intelligence operations primarily cause damage over the long term. Most intelligence operations are covert, and can continue for a long time without being detected by the target. The totality of intelligence activity has the potential to cause serious damage to Norwegian society, the business sector and individuals.

Unless the operations are detected and prevented, the activities of some intelligence services will be able to:

- weaken our democracy
- weaken our civil and military crisis management capacity
- reduce the legitimacy of the authorities among the population
- influence political decision-making processes in a way that harms Norwegian interests
- weaken Norway's position in international negotiations
- weaken the competitiveness of Norwegian companies
- steal sensitive information related to research and technology
- limit the individual's freedom of speech

**Computer network exploitation**
Cyber espionage by other states' intelligence services represents a serious long-term threat to Norway. In recent years foreign intelligence services have succeeded in infiltrating networks in both the public and the private sector.

Most Russian and Chinese intelligence activity against Norway takes the form of computer network exploitation. Cyber espionage is cost-effective and low-risk compared with other intelligence methods. Hostile states wishing to infiltrate Norwegian computer networks are continually discovering new vulnerabilities to exploit.

In the coming year Norwegian organisations will detect or be notified that foreign intelligence services have tried to obtain

**Cyber attacks against the Storting**

In autumn 2020 a number of cyber attacks were carried out against the Storting and certain Norwegian organisations. PST's investigation revealed that the cyber espionage group Fancy Bear, also known as APT-28, was probably behind the attacks. The group is part of the Russian military intelligence service GRU.

There have been several reports in the media of Fancy Bear's activities in various countries. In 2018 the US authorities charged a number of GRU officers with hacking into computer networks in connection with the 2016 presidential election. Fancy Bear has also apparently been involved in operations targeted at international sports organisations, national sports federations, government agencies and national assemblies in several other countries. Fancy Bear has been executing cyber attacks on Norwegian targets for many years.

In the cyber attack on the Storting, Fancy Bear succeeded in stealing sensitive information from a number of email accounts. We believe the group's objective was to steal basic information about Norwegian society that could be used in more narrowly targeted intelligence operations. Sensitive information that has come into the wrong hands can also be used to influence individuals or political processes, for example to put pressure on employees or Storting members to cooperate with the intelligence service or to influence political processes such as this year's parliamentary elections.

access to their computer networks. However, we must assume that many operations will never be detected.

Public and private actors working in the fields of foreign affairs and defence and security policy will be particularly targeted by intelligence services. The same applies to technology companies and research communities who work with space-based services, maritime technology, health and the defence industry. The petroleum sector must also be prepared for attempts by hostile actors to steal data.

Attempts to infiltrate an organisation usually start with reconnaissance efforts to identify the assets, employees and technical vulnerabilities. The actor then has a number of possible actions. An effective method is to send customised emails with infected attachments or links that appear to be legitimate. Another is to target the operation at internet-exposed services such as email by, for example, making use of weak passwords and the absence of two-step authentication to obtain unlawful access to the network.

Hostile actors make use of global networks of digital infrastructure both before and after their attacks on Norwegian organisations. They do this in order to hide who they are, what type of data they are interested in and what they have stolen. Such infrastructure usually consists of inadequately secured servers, and there have been cases where intelligence services have anonymously rented space on servers in Norwegian data centres. Given the increasing number of data centres, there is a risk that Norwegian centres will be used for computer network attacks.

The purpose of most computer network exploitation in Norway by foreign states will continue to be to steal information. However, in recent years hostile actors at the international level have appeared who are able and willing to manipulate information and sabotage digital systems, and it is only a question of time before such operations are used to attack Norway.

### Smart cities

The development of 5G and the Internet of Things has meant that an increasing number of municipalities are digitalising, coordinating and automating parts of their administration, enabling them to improve the quality and efficiency of their services. However, smart city technology leads to new dependencies and an increase in sensitive information in a growing number of social sectors. This development provides foreign states with new targets for intelligence and sabotage.

The increased linking of units, processes and services to the internet creates long and complex digital value chains. Elements that are secure in themselves become vulnerable to other, less secure, elements in the same chain. Overview and control of the chain is often outsourced to large foreign commercial actors.

Through open and covert participation in the research, development, production and maintenance of physical and digital smart city solutions, state actors can achieve a very detailed overview of critical infrastructure in Norway, such as the electricity supply, traffic, water supply and sewerage systems. In a worst case scenario the overview will create serious vulnerabilities that can be exploited to paralyse cities and even whole regions.

## Mapping of critical infrastructure

In 2021 foreign states will continue to try and map Norway's critical infrastructure with a view to identifying functions and vulnerabilities. Some intelligence services also feel the need to continually update their information on bridges, harbours and military installations, divisions and materiel. Much of this activity is performed through technical surveillance.

Some intelligence services also make use of Norwegian personnel to gain information on conditions in critical infrastructure such as military installations. These personnel have a variety of covers but they are generally of a kind that allows the individual to travel freely around Norway under the simple guise of being a tourist.

## Recruitment

One of the core tasks of intelligence services is the recruitment and running of covert agents, and some services devote considerable resources to such operations in Norway. This activity will be continued in 2021.

The greatest threat in terms of recruitment will be posed by the Russian intelligence services. A considerable number of intelligence officers work in the Russian embassy in Oslo. They devote much time to establishing and maintaining relations with individuals in Norway, an undesirable activity that causes considerable damage. Intelligence officers have diplomatic immunity and thus cannot be prosecuted here in Norway.

An established source can provide valuable information on the plans and activities of individuals, public and private organisations, and political institutions. A source can also provide information about any disagreements, internal conflicts or dissatisfaction in the workplace, and can be asked to identify other vulnerabilities that are open to exploitation. Information about routines, security measures and digital infrastructure can be used in planning new intelligence operations. A source or an agent can also be used to covertly influence decisions.

Intelligence operations in Norway by foreign states are carefully planned and the recruitment and running of sources can take place over many years. For example, intelligence officers often approach young people who they believe will in the long term be in a position to acquire influence and provide access to information.

In 2021 recruitment will continue to be targeted at individuals with direct or indirect access to sensitive information. We regularly become aware of cases where intelligence officers in Norway are in contact with individuals who do not have direct access to the desired information but who belong to a network of people with such access.

Intelligence officers use a variety of arenas to identify and seek contact with potential sources. Two important arenas are seminars and conferences open to the public, which will again be held once the level of infection permits.

Intelligence officers use these meeting places to make contact with individuals they wish to recruit. In such cases the officer will pose as for example an employee at an embassy, a company or an educational institution. They will then seek to cultivate a friendly relationship based on common interests. The officer will investigate what the potential source has access to and which networks they belong or could belong to. The aim is to cultivate a dependence relationship, in which the source accepts payment and then feels under pressure or under an obligation to perform services for the officer.

A number of intelligence services try to recruit individuals through social media. A frequently used approach is to make contact and cultivate a relationship with individuals through a professional online forum such as LinkedIn. For example the intelligence officer, or an individual they control, may pretend to be a foreign expert in the subject or an employee in a recruiting agency. Over time the relationship will develop further; for example the individual will receive invitations to seminars or be asked to draft written reports, articles or op-eds for payment. However, the relationship will always be controlled by the foreign intelligence officer and used to either influence opinions and decision-making or gain access to sensitive information.

In 2021 Norwegian citizens living under authoritarian regimes will continue to be lured or pressured by the host country's intelligence service into performing services for them. Citizens from other countries living in Norway may also be pressured by their original country's intelligence service. Intelligence services often behave in a more direct and threatening way when recruiting their own country's citizens than they do when recruiting Norwegians.

### Influence operations

Many public and private actors make decisions that affect other countries' interests, and several of the intelligence services operating in this country are seeking to influence such decisions. We expect them to continue this activity in 2021.

### The High North

Strategies and processes related to Norway's High North policy are among the most sought-after intelligence targets in this country. A number of states wish to strengthen their influence and secure their commercial interests in the region. Foreign intelligence services therefore make great efforts to collect information and acquire influence over Norwegian processes aimed at further development of its northern areas. Such information and influence would give these countries an undue advantage in the exploitation of natural resources, access to technology and other commercial interests.

Intelligence activities in the High North have the potential to weaken Norway's freedom of action. Russian and Chinese intelligence services continue to pose the greatest threat. We expect Russian intelligence services to continue their efforts to identify civil and military infrastructure in the region. China and Chinese actors will continue to give priority to their long-term positioning in the region, especially in relation to the future exploitation of natural resources. We expect both states to try to buy or establish companies in strategically placed properties in the region.

In recent years we have seen individual cases where influence operations have been attempted or carried out. So far PST is not aware of any widespread propaganda or disinformation campaigns targeted at political processes. However, we should be prepared for attempts by foreign intelligence services to influence opinion and the political debate in the coming year.

Attempts at influence operations can be targeted at a broad range of actors, including the public, politicians, business actors, journalists, civil servants in central and local government, academics and members of think tanks. Particularly vulnerable geographical and thematic targets will include North Norway, Svalbard, and Norway's defence and High North policies.

> We should be prepared for attempts by foreign intelligence services to influence public opinion and political debate in Norway in the coming year.

As a result of Norway's membership of the UN Security Council we expect an increase in intelligence and influence operations targeted at the Ministry of Foreign Affairs. A number of states are interested in information about Norway's approach to particular cases that are to be dealt with in the Security Council in order if necessary to use the information to influence Norway's position. Actors that help to set standards for Norwegian foreign and security policy, such as research institutes and humanitarian organisations, will also be important targets for intelligence and influence operations.

Influence operations can take various forms. In Norway some intelligence officers try to influence the outcome of a particular case by targeting individuals with political clout. In a number of Western countries foreign intelligence services have been involved in spreading disinformation, initiating smear campaigns and spreading rumours or half-truths through social media. These methods are effective in a wide range of cases, from influencing the outcome in particular cases to weakening democratic processes.

**Technology and knowledge transfers**

Norwegian businesses, researchers and research institutes possess knowledge and technology that are sought after by

other states for the development of their advanced weapons systems and weapons of mass destruction.

In 2021 certain states will try to obtain Norwegian technology that they are not permitted to purchase under export control regulations or because of Western sanctions. There will also be attempts to transfer knowledge from Norwegian research and education institutions unlawfully. The greatest threats will come from Russia, China and Pakistan.

In countries that pose the greatest threats there are usually close ties between civil and military research programs. Research stays in other countries are used to obtain knowledge that can be applied to the development of weapons programs. Researchers may be pressured both during and after their stay in Norway to disclose their knowledge for use in development programmes for weapons systems. The damage potential of such unlawful transfers of specialised knowledge is considerable, especially in a time of weakened international arms control and growing rivalry between the great powers. If the above states succeed in developing advanced weapons systems this will affect the threats facing Norway and its allies.

Certain Norwegian companies have developed technology and components with dual-use potential. Such goods are not primarily intended for the military, but they have properties that can be useful for military purposes. Since Norway is an oil-producing country with considerable expertise in related sectors such as the maritime sector, the country possesses valuable competence in the field of advanced subsea technology.

## Indications of illegal procurement

Do you think your company is being subjected to attempts at illegal procurement? The following points may indicate such activity:

- You receive limited information concerning the buyer.
- The buyer provides limited information on the end user.
- Unusual freight conditions and payment methods are stipulated.
- The goods are to be sent to a warehouse, forwarding agent or customs-free zone.
- An established customer asks for goods the company normally does not sell.

Some states try to avoid export control regulations when dealing with Norwegian companies. Their aim is to create as much uncertainty as possible around the actual end user of the good. One method is to establish a highly complex corporate structure, with nominee and front companies and complicated supply chains. Another is to use an unusual freight route to transport the product to its final destination that makes it very difficult to detect breaches of the export control regulations. The authorities therefore have to rely on Norwegian companies to develop competence that makes them and society at large less vulnerable.


**A Russian diplomat was expelled from Norway in autumn 2020. A man in his fifties from DNV GL was charged with leaking information to a foreign state that could harm critical national interests.**

Police Prosecutor Line Nygaard in PST meets the press after the remand hearing for the man charged with espionage.

PHOTO: HEIKO JUNGE / NTB

## Financial methods

Acquisitions and investment in Norwegian businesses can allow foreign states access to information and influence that could damage Norwegian interests. In some cases where it is illegal to purchase information or technology from a particular company it may still be legal to invest or acquire ownership interests in the company, which would give the foreign state the opportunity both to access information and to share it.

Financial methods can therefore be used in some cases to achieve many of the same goals as covert intelligence operations. For example acquisitions and investment in Norwegian companies can also be used to influence Norwegian decisions and priorities. If parts of the operation and development of Norwegian infrastructure and key activities are at the mercy of other countries' political plans, Norway will be vulnerable to pressure and influence from those quarters. We have noted cases where Norwegian companies have been offered favourable financial agreements that were hard to resist. The company thereby runs the risk of developing a one-sided dependence relationship that the foreign state can exploit to pressure decision-makers to act against Norway's security interests. This threat can strike decision-makers at every level in central and local government.

The Chinese authorities have the power to force Chinese companies to act in the interests of the state. Thus a company may have to conclude unprofitable agreements with foreign companies in order to acquire information and influence of interest to the Chinese authorities. For example, it can buy up small businesses in the defence industry or conclude supplier agreements that give it some insight into the company's digital infrastructure.

Most businesses are in a weak position when faced with competitors that do not need to make a profit. It can be difficult for Norwegian public- and private-sector decision-makers to reject a business offer that

## The intelligence threat and Covid-19

The pandemic has affected intelligence requirements and provided intelligence services with a window of opportunity for their activities.

Some states have a continual interest in detecting vulnerabilities in Norway's crisis management capability. The information can be used to weaken, or threaten to weaken, Norwegian emergency preparedness and crisis management in any future conflict. Such information is obviously easier to find at present than in normal times.

Foreign intelligence services will exploit the weaker digital security solutions used in home offices, making the cyber attack more likely to succeed.

The negative economic consequences of the pandemic and the possibility of bankruptcies in the business sector give other states more opportunities for strategic acquisitions, which can be used to increase the state's influence in strategically important areas or to acquire sensitive data and technology.

is in itself very favourable. The foreign actor will often exploit the fact that while the decision and the profits are made at the local level, the cost is paid at the national level.

**Espionage against refugees**
China, Iran and other authoritarian states use their intelligence services to identify and spy on dissidents and refugees in Norway, and will continue to do so in 2021. Their aim is to undermine, neutralise or eliminate political opposition.

> Members of the exile community may be subject to threats in 2021.

Authoritarian regimes use a variety of methods to gather information about their former citizens in Norway. For example they may participate in events arranged by exile communities or try to infiltrate organisations and associations. They will monitor social media in order to gather information about particular groups and individuals. A number of countries also use their official representatives in Norway to spy on immigrant communities. Some states use religious meeting places as an arena for collecting information.

Norwegian government agencies that manage information on refugees and foreigners may be targets for foreign states. Intelligence officers will try to establish friendly relations with employees of the immigration administration, the police or the Labour and Welfare Administration in order to gain access to the relevant registers and databases. Some states are willing to take the risk of assassinating political dissidents staying abroad. For example, in recent years individuals with Chechen or Iranian backgrounds staying in Europe have been subject to assassination or attempted assassination. Thus some members of the exile communities in Norway could be subject to threats in the coming year.

There have also been cases where attempts have been made to lure individuals to travel to a third country where the intelligence service has a much better opportunity to make an arrest than it has in Norway.

# Politically motivated violence – extremism

**Islamic extremism and right-wing extremism are expected to pose the greatest terrorist threats to Norwegian security this year as well as in 2020. There is an even chance that individuals in these communities will attempt to carry out a terror attack in Norway in 2021. It is still highly unlikely that left-wing extremists will commit a terrorist act.**

# The threat from Islamic extremists

**There is an even chance that Islamic extremists will try to carry out terrorist acts in Norway in the coming year.**

**At the end of last year the terrorist threat from Islamic extremists was intensified due to the increased tension between the right to freedom of speech and what many Muslims perceived as a desecration of Islam.**

Whether the situation will remain the same, worsen or improve in 2021 depends on a number of factors. These include whether or not anti-immigration and anti-Islam groups continue to provoke Muslims by their perceived desecration of Islam and how Islamic extremists will respond.

## Increased tension in Europe affecting the threat in Norway

Islamic extremists in Europe will continue to pose a threat in the year to come. One reason for this is the debate on freedom of speech in connection with the Mohammed cartoons and the subsequent incitement to terror by ISIL and al-Qaeda.

The number of executed terror attacks increased from 2019 to 2020. However, the figures for executed versus prevented attacks show a small decrease from 2019 to 2020. The large number of executed attacks in 2020 is due to the fact that in most cases the attacker used knives, axes or slashing weapons, making their actions difficult to predict and thus to prevent. All the planned attacks that have been prevented in the last two years have involved firearms and explosives, and most of them have involved more than one attacker.

### Executed and prevented terror attacks by Islamic extremists in the West 2019–2020

In 2020, Islamic extremists executed 15 terror attacks in Europe, as opposed to six attacks in 2019. Most of the attackers used extremely simple methods.

Three attacks were prevented in 2020, and 15 in 2019.

(Figures from PST's database.)

There are several active Islamist networks in Europe. The members include returned foreign fighters, convicted terrorists released from prison and convicted terrorists still in prison. In 2021 the threat in Europe will come primarily from members of these networks and from individuals. This will also influence the threat against Norway.

The European networks continue to radicalise new individuals. Islamic extremists released from prison are causing concern


## Tensions in Europe affect the threat picture in Norway

Thousands of protestors demonstrated in France against the killing of a French teacher who used the Mohammed cartoons to illustrate a lesson on freedom of speech. The placards read 'I am a teacher'.

PHOTO: SOPA IMAGES / SIPAUSA / NTB

in several European countries with large extremist groups. These countries will be particularly prone to attacks by Islamic extremists.

The message preached by ISIL and al-Qaeda, that the West is at war with Islam, will continue to mobilise supporters in Europe. The idea is kept alive by the revival of the debate on the Mohammed cartoons and the persistent desire of these extremists to wreak revenge on the West for its military interventions in Muslim countries. These terrorist organisations will continue to encourage their supporters to mount attacks on Western targets, especially in Europe. Their propaganda, together with the activity on extremist online networks, is expected to encourage new terror attacks in 2021.

## Intensified threat posed by Islamic extremists in Norway

Although Norway is of peripheral interest to ISIL and al-Qaeda in general, Norwegian targets are a central focus for extremists living here.

### Intensified radicalisation[1] to Islamism expected

It is likely that incidents will occur in Norway in 2021 that will be perceived by Islamic extremists as offensive, and they will use these as a pretext to make new converts to Islamism.

Repeated provocation will increase the risk that a new generation of extremists will be converted to Islamism. The extent of such an increase is difficult to estimate at present, and it can take several years before such groups are formed and their members are inspired to commit terrorism.

Incidents that Muslims find offensive spread rapidly through traditional and social media and reach a wide audience both at home and at the global level. We have also noted that images and videos have been edited to give the impression that Norway is a nation that desecrates Islam. Such fabrications could make Norway a more important enemy target for Islamic extremists in other countries and increase the risk of violence directed at Norwegian goals and interests.

### Other factors that may intensify the threat

In addition to perceived insults to Islam, a Norwegian military presence in Muslim countries and the conflicts there, will increase the threat of terror in 2021. This also applies to debates and incidents in Norway that are perceived to prevent

[1] The term 'radicalisation' is used to describe a process in which an individual increasingly accepts the use of violence as a means of achieving political, religious or ideological aims.

individuals from practising their religion. These will strengthen the perception that the West is at war with Islam. Major Islamist terror attacks in other countries are also likely to inspire individuals to plan such attacks in Norway.

A number of digital extremist communities that operate partly or completely outside the more traditional terrorist organisations have begun to play a central role in the threat picture in recent years. These communities take several forms, from loosely organised, uncommitted groups to networks with extremely security-conscious members linked by social ties. These are also arenas for radicalisation and incitement to terror.

In spite of the various European governments' recent campaigns to suppress online propaganda, 10- to 20-year-old propaganda is still being circulated, and continues to be effective. ISIL and al-Qaeda are targeting their propaganda at ever younger age groups using their preferred arena of online forums and adapting the message to appeal to the young. Larger numbers of younger individuals are being radicalised than in previous years.

Norway has fewer returned foreign fighters and few imprisoned Islamic extremists than many other European countries. However, the ties between Islamic extremists in Norway and those in Europe have a bearing on the threat picture in Norway. This applies particularly to contact between extremists in Norway and released prisoners and returned foreign fighters in other European countries.

**Continued support for terror despite small number of new foreign fighters**

In 2021 few Islamic extremists from Norway are expected to travel as foreign fighters to conflicts in countries like Syria, Afghanistan and Somalia. This is partly due to the lack of organisation and reception facilities in these countries, and the fact that the conflicts are losing their appeal.

Norwegian Islamic extremists will, however, continue to support global terrorist and extremist organisations in regional conflicts to which they themselves have links. Online forums continually feature fund-raising campaigns, sometimes disguised as emergency aid, to support extremists and terrorists. It is also likely that some mosques and Muslim cultural centres raise funds on behalf of extremist groups. The funds are channelled through banks or hawala [2)].

[2)] Hawala is a system of money transfer without money movement across borders. It is based on trust and Islamic tradition and is used as an alternative to banks.

### Simple, isolated attacks on crowds or symbolic targets most likely

Any Islamist terror attack in Norway will probably be carried out by only one or two individuals. The most likely targets are a crowded public venue with low security or a symbolic goal.[3] As long as the covid restrictions prohibit large crowds, the attackers are likely to aim at smaller gatherings.

[3] Symbolic targets are those associated with the ideological causes supported by Islamic extremists.

The choice of targets and methods depends on a number of factors. The most likely symbolic targets include individuals associated with insulting Islam and police officers or military personnel who are out in the public arena. Other symbolic targets are churches, synagogues and similar meeting places.

Although an attack may be carried out by a lone wolf or one individual with a partner, the person is likely to have had contact with others who share their views. Online networks are one of the main arenas for radicalisation and planning attacks, and may replace some of the functions of terror organisations.

> **Online networks will become essential tools for radicalisation and could replace many of the functions of terrorist organisations.**

The attacker is likely to use readily available weapons such as edged weapons and blades or a vehicle, alone or in combination. Some terrorists use firearms or improvised explosive devices, and some use false suicide belts or vests.

An attack carried out by a single perpetrator using relatively simple methods against a readily available target often requires only a short preparation phase, making it difficult to prevent.

# The threat from right-wing extremists

**There is still an even chance that right-wing extremists will try to carry out terrorist acts in Norway in the coming year. The threat will primarily come from individuals who have been radicalised through online platforms. Right-wing violence is motivated by an increasing variety of ideological beliefs, and this trend is likely to continue. In recent years right-wing extremism has become more transnational. International incidents will also affect the threat in Norway.**

## Increased radicalisation to right-wing extremism likely

Radicalisation to right-wing extremism is expected to increase in 2021, and the causes being promoted have a greater appeal than before. Hatred of Muslims, non-Western immigrants, Jews, LGBT+[4)] communities, the traditional media and politicians, usually those on the political left, is central to these extremists' ideology.

4) LGBT+ is an abbreviation for the lesbian, gay, bisexual, trans and other sexual and gender minorities.

There are several factors behind the increased risk of radicalisation to right-wing extremism. Right-wing utterances and propaganda reach a wide audience through the internet. Secondly, covid has created an atmosphere of uncertainty caused by factors such as unemployment and financial considerations. Social isolation means that more people spend time on the internet, and some of them go on to explore more extremist forums.

Many right-wing radicals and extremists also have issues such as drug addiction, psychiatric problems, criminality and adjustment problems of various kinds that make them vulnerable to radicalisation.

We believe that right-wing thinking, as opposed to extreme ideology, is more likely to attract supporters. However, experience has shown that right-wing radical online forums can function as a gateway to right-wing extremism.

## Online platforms – an important arena for radicalisation

In 2021 it is likely that Norwegian individuals will participate in transnational, violence-inciting closed groups on the internet. Experience has shown that these serve to radicalise some individuals and inspire them to commit terrorist acts.

We expect right-wing radicals and extremists to continue to use the internet as the most important arena for promoting

their ideas. In recent years online platforms have been shown to facilitate network-building, and there is every sign that this development will continue. Several of the platforms are publicly accessible, and some function as meeting places for violent right-wing extremist counter-cultures that oppose established norms and standards they perceive as political correctness.

Right-wing extremist ideology makes use of memes, humour, clips from films and video games, and conspiracy theories. Transnational online platforms facilitate the rapid communication and sharing of large volumes of propaganda, which promotes group formation and dynamics. Communication is anonymous, with little or no censorship. The result is that extremist propaganda becomes normalised, and the 'enemy' gradually becomes dehumanised.

Extremism disguised as humour takes the sting out of extremist propaganda, and gradually erases the line between virtual reality and real life. This can lower the threshold of violence. Although many people who take part in these forums primarily do so for social reasons, the message and the rhetoric can have a powerful effect on some individuals and inspire them to commit terrorist acts.

## The extreme right – a source of radicalisation

The extreme right is a general term for individuals with radical or extremist right-wing ideologies. They have two main characteristics. The first is that the state and the people should be one. Any group they consider to not belong to this entity is considered to be a threat. Secondly, the far right are either opponents of democracy as a form of government or they challenge the central liberal values that underpin democracy.

What distinguishes right-wing radicals from right-wing extremists is their respective views on democracy and whether or not they are willing to accept violence as a means of achieving political change. Right-wing extremists wish to destroy democracy and believe that violence is necessary. Right-wing radicals do not accept violence. However, both groups are often suspicious of the authorities, whom they regard as corrupt.

**Participation in physical groups can also lead to radicalisation**

Far-right physical cross-border networking is expected to start up again once the covid restrictions ease up. The networks will promote contact between like-minded individuals in different countries. These communities are often very security-conscious. Charismatic leaders and other figures also have a radicalising effect.

The Nordic Resistance Movement has little support among the Norwegian population, and is unlikely to grow significantly in 2021. The organisation's long-term goal is a National Socialist state, and in recent years it has been the most active of the neo-Nazi groups in Norway.

Right-wing radical and extremist groups will continue to commit acts that are perceived as offensive by their opponents, and this will increase the risk of violence. More individuals will be radicalised as


Increased polarisation could give rise to violent clashes in 2021.

PHOTO: JIL YNGLAND /NTB

a result of recruitment and other activities by these groups, thereby increasing the potential for violence.

**Inspiration to take part in planning right-wing terror**

In 2020 the number of executed and prevented right-wing extremist terror attacks in the West declined considerably compared with the previous year. There are several possible reasons, including the presence of covid restrictions and the preventive measures taken by the security services.

The number of right-wing extremist terror attacks in the West is likely to increase somewhat in 2021 in relation to 2020. Greater numbers of radicalised right-wing extremists and a greater possibility of trigger incidents make the planning of terrorist acts more likely.

Issues and incidents that right-wing extremists perceive as threatening the white race and white culture may inspire some extremists to plan terrorist acts. Possible triggers are the increasing trend towards globalisation, a perception that the authorities are deliberately hiding the negative aspects of immigration, or the belief that Norway's immigration policy is too liberal.

In addition major right-wing extremist terror attacks will continue to motivate others to plan terrorism. If the attack results in a large number of casualties and the attacker publicises propaganda inciting terrorism (such as a manifesto or a video showing an attack), there is a greater risk that others will follow suit. For example the 2019 terror attack in New Zealand set off a chain reaction of attacks in other countries, including Norway.

**Executed and prevented attacks by right-wing extremists in the West 2019–2020**

In 2020 three terror attacks were executed by right-wing extremists in Europe. In 2019 there were 16.

Seven attacks were prevented in 2020, and 14 in 2019.

(Figures from PST's database.)

In 2020 the number of Norwegians who sympathise with and support right-wing terrorism increased. Many of them are members of transnational right-wing online communities where the use of terror is promoted. The feeling of belonging to a global resistance movement linked by online networks lowers the threshold for participating in a terror attack.

A particular cause of concern is groups who emphasise that resistance is urgent and explicitly incite individuals to take part in a physical struggle. Far-right accelerationism urges its supporters to accelerate

total social collapse through terrorism. Its advocates believe that a race war between the white race and all other races will soon take place. Several right-wing terrorists have been inspired to act by this way of thinking.

**Individuals whose targets fit in with their enemy stereotype most likely to commit terrorism**

A terror attack is most likely to come from an individual rather than a group, and to be aimed at a target branded as an enemy in right-wing ideology. Even lone-actor terrorists are likely to have been radicalised through an online forum or global network of like-minded individuals. Others may have been on the fringes of an established community of right-wing radicals or extremists.

The most likely scenario is an attack with a large number of casualties on a meeting place for individuals with non-Western backgrounds. As long as covid restrictions limit the size of mass gatherings, smaller ones will also be potential targets.

> **The most likely scenario is an attack on a meeting place for people with a non-Western background.**

Other potential targets are individuals that fit in with the enemy stereotype, such as politicians and representatives of the authorities who are perceived as facilitating immigration and helping to destroy the white race and its culture. The covid pandemic and the parliamentary elections in the autumn are likely to enhance the perceived dangerousness of such targets. Mosques, Jewish targets and LGBT+ individuals are also likely targets.

Firearms, edged weapons and blades or improvised explosives will be the most likely weapons.

# The threat from left-wing extremists

**It is highly unlikely that left-wing extremists in Norway will attempt to commit terror attacks in 2021. However, we expect that some members of this group will attack individuals they consider right-wing extremists.**

### Left-wing extremist groups still small in Norway

There are still only a small number of left-wing extremist groups in Norway. They have few active members and the number is not expected to increase significantly in 2021. Covid is unlikely to have much effect on these groups.

Left-wing extremist groups will continue to be in contact with like-minded individuals in other European countries, especially in the Nordic region. Certain groups in other Nordic countries have a lower threshold for terror. Since the internet facilitates recruitment and information-sharing across borders, these groups could motivate groups in Norway to greater violence.

### Combating right-wing extremists still a unifying rallying point

It is highly likely that left-wing extremists will continue to spread their political ideas through propaganda, campaigns and counterdemonstrations. This applies primarily to causes related to the struggle against the machinery of power and political right-wingers. Several demonstrations have been marked by a high level of aggression and violent clashes, and this situation is expected to continue in 2021.

It is also highly likely that left-wing extremists will continue their targeted, politically motivated violence against right-wing extremists in 2021. Some groups can mobilise rapidly. Some left-wing extremists will continue to take part in planned violence, confrontations and public harassment of individuals they label right-wing extremists. These actions will continue to polarise the various groups and increase the potential for reciprocal violence. These extremists also regard the police as an enemy and sometimes attack police officers during demonstrations.

# Other forms of extremism

Anti-state movements are expected to be potential sources of radicalisation in Norway in the coming year. They usually use online platforms to spread their ideas. Ideological movements based on anti-state and conspiracy theories have emerged in recent years and are becoming more widespread in some countries.

Although these groups have no single common ideology, they believe the power of the state to be illegitimate because its laws and rules are considered to violate the freedom and sovereignty of its citizens. The groups are likely to be strongly affected by covid restrictions. Conspiracy theories about topical news stories can provoke threats against dignitaries.

> **Ideological movements based on anti-state and conspiracy theories have emerged in recent years.**

A number of Western countries have seen a growth in radical activist groups that focus on climate and nature conservation issues, and several of them have started to step up their activities. Their goal is to make political decision-makers implement a more environmentally friendly policy and draw public attention to their causes. So far demonstrations in European countries have been non-violent. Environmental causes could radicalise individuals here in Norway as well. Local politicians and opponents have been threatened and harassed in connection with issues relating to environmental protection and nature conservation in this country, and it is possible that some of these individuals will begin to consider using violence to support or achieve their political ends.

# Threats to dignitaries

**In the year to come we expect a certain rise in the number of threatening acts against dignitaries. However, it is unlikely that dignitaries will be the object of seriously violent acts.**

## Rise in the number of threatening activities involving dignitaries

The threat to dignitaries[5] in Norway in recent years has remained stable,[6] but a certain increase in the number of threatening acts is expected in 2021. The main reasons for this are dissatisfaction with the way the authorities have dealt with covid, an expected rise in the number of radicalised right-wing extremists and greater public attention paid to causes they disagree with, and the increased media attention paid to politicians with different views in the run-up to the general election in the autumn.

Individuals with no particular ideology and individuals with pronounced extremist sympathies may both nurture hatred of the Norwegian authorities. Most threats to Norwegian dignitaries come from individuals who do not have extremist views but who hold the authorities responsible for their problems. Personal grievances are just as much of an incentive as ideology or politics. This makes it difficult to identify potential perpetrators of violence.

However, we consider it unlikely that seriously violent acts will be committed against dignitaries in 2021.

## Political causes as provocation

We expect a considerable number of threats to Norwegian dignitaries to be provoked by the way the authorities have dealt with the covid pandemic. The wide-ranging restrictions will continue to result in a large number of hateful utterances, mostly published on the internet by mentally ill individuals without any specific political views. Threats against dignitaries by individuals with extremist sympathies will come mainly from the right, since the authorities occupy a prominent place in their image of the enemy.

In the run-up to the general election in autumn 2021 politicians will be more visible to the public eye and certain issues will be given more prominence. We therefore expect the number of threats to rise during the election campaign.

The general uncertainty about the pandemic, the long-term economic downturn, a perceived loss of individual freedom and financial and social problems will continue to motivate certain individuals to hate dignitaries and issue threats. Local politicians and public-sector employees are also likely to be threatened in connection with covid-related issues.

Immigration has long been an issue that attracts threats against dignitaries from individuals both with and without

[5] Dignitaries are members of the Royal Family, the government, the Storting and the Supreme Court.

[6] The threats to dignitaries discussed in this section come from non-state actors. Threats against dignitaries are also discussed in the section on state intelligence activity.

## The political campaigns in the run-up to the parliamentary elections in autumn 2021 will result in an increase in threatening activity directed at dignitaries.

Dignitaries who are perceived to have liberal views on immigration, or a Muslim and/or non-European background are especially liable to receive threats.

PHOTO: STIAN LYSBERG SOLUM / NTB

ideological standpoints. Dignitaries who are believed to hold liberal views on immigration, have a Muslim and/or non-European background or are perceived as downplaying the negative aspects of immigration are especially liable to be targeted.

Dignitaries who defend freedom of speech tend to attract more threats, especially those regarded as defenders of perceived religious violations. Politicians who advocate Norwegian military participation in conflicts in Muslim countries will also be subject to threats.

Other political issues that will attract threats in 2021 are particular issues related to climate and environment, certain child welfare cases, and certain taxes.

Broad media coverage of dignitaries involved in specific controversial issues will result in a greater number of threats against the politician concerned as long as the media interest lasts.

**Threats against dignitaries are threats against democracy**

Hate speech against dignitaries will continue in 2021. The sheer extent of hate speech, harassment, online shaming and threatening language, especially on social media, directed against individual politicians constitute a great strain. Ultimately this means that some politicians will refrain from political activity, become passive or be pressured into making decisions they would not otherwise have made. A situation like this threatens our democracy. The cornerstone of democracy is engagement and participation by citizens, trust between the different population groups and confidence in the authorities. As a general rule ministers and party leaders are subject to more and greater threats than other dignitaries.

# Purpose of the national threat assessment

# Purpose of the national threat assessment

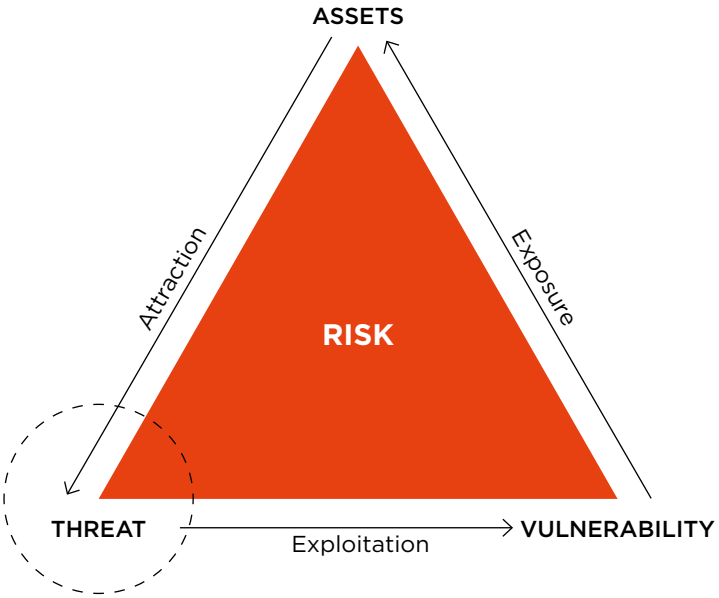
When planning preventive measures, more information can be obtained from the following websites:

**pst.no**
**politiet.no**
**nsm.no**

The national threat assessment is an analysis of expected developments in PST's areas of responsibility in the coming year. It is intended to develop an awareness of the most serious threats facing Norway and provide support for decision-making in connection with the important preventive measures to ensure security that an organisation needs to take. The threat assessment should be viewed in the context of other threats that could affect the assets of the particular organisation, such as other types of criminality or undesirable activities.

Purpose of the national threat assessment in connection with a risk assessment:

- Risk can be defined in several ways. In this context we discuss risk as it applies to values, threats and vulnerability, and the threat assessment is intended be used as a resource in decisions concerning risk assessment.
- The values of the organisation should be assessed in order to identify the relevant threats. The assessment will highlight ways in which hostile actors can impact these values. It is also important here to consider any dependencies, including those outside the organisation itself. This will provide the basis for assessing vulnerabilities. The vulnerability assessment will determine the extent to which the organisation's values are vulnerable to identified threats, with a view to establishing good preventive measures and measures to reduce adverse impacts.
- The above measures will then form the basis for a risk assessment of whether the organisation maintains a proper level of security.




**Example 1**
**State intelligence activities**
The present threat assessment discusses state intelligence activities and the threat posed by insiders: agents who are recruited or planted in an organisation where they can access information enabling them to manipulate data or sabotage data security. The organisation must take practical measures to combat such threats. On the basis of known local factors, a survey should be made of ways in which an insider could obtain access to the most critical values without being detected or prevented. An assessment can then be made of which risk-reduction measures should be taken to prevent, detect or reduce the most serious consequences of this type of threat.

**Example 2**
**Politically motivated violence**
The national threat assessment discusses the threat from extremist individuals and groups who are most likely to carry out isolated terror attacks using edged weapons and blades, vehicles, firearms and simple improvised explosives. Organisations and the actors responsible for security must themselves consider the effect of such threats on the organisation. After a threat assessment based on local conditions, the organisation can decide which preventive measures to take in order to prevent or delay a hostile actor, and whether the most serious consequences of an attack can be mitigated by for example drafting plans for immediate notification to the police and evacuation of the premises.

DESIGN AND ILLUSTRATION: CREUNA / PRINT: STAPLES


**The Norwegian Police Security Service**
vww.pst.no