National threat assessment 2020

POLITIETS SIKKERHETSTJENESTE

The most serious threats to Norwegian security are:

– foreign intelligence targeted at the government, the Storting (the Norwegian parliament) and the Armed Forces

– digital reconnaissance and sabotage of critical infrastructure

– terrorist attacks carried out by individuals motivated by right-wing extremism or extreme Islamist ideology

The Police Security Service (PST) is Norway's domestic security service. Its main task is to investigate and prevent serious offences that threaten national security. It publishes an annual threat assessment in the form of an analysis of expected developments within its areas of responsibility.

The Norwegian Intelligence Service (NIS) is Norway's foreign intelligence service. Although subordinate to the Norwegian Chief of Defence, NIS does not concern itself exclusively with military matters. NIS's main mission is to warn of external threats to Norway and high-priority Norwegian interests, to support the Norwegian Armed Forces and the defence alliances Norway is part of, and to assist in political decision-making processes by providing information of significance to Norwegian foreign, security and defence policy. This year's assessment, Focus 2020, contains NIS's analysis of the current situation and expected developments in geographic and thematic areas considered particularly relevant to Norwegian security and national interests.

NSM

The Norwegian National Security Authority (NSM) is responsible for preventative national security. NSM advises and supervises the safeguarding of information, objects and infrastructure of national significance. NSM also has a national responsibility to detect, alert and coordinate responses to serious ICT attacks. In its report Risiko, NSM assesses the risk of Norwegian society being subjected to espionage, sabotage, acts of terror and other serious incidents. The assessment is published in the first quarter of the year.

dsb

The Directorate for Civil Protection and Emergency Planning (DSB) is responsible for maintaining an overview of risks and vulnerabilities in Norwegian society. DSB has published scenario analyses since 2011. These cover the risk of major incidents in Norway, incidents Norwegian society should be prepared to handle. They include natural events, major accidents and deliberate acts, and the timeframe is longer than for the annual assessments published by the other three agencies.

Degrees of probability

The following is a list of the degrees of estimated 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

Likely

There is good reason to expect

Even chance

It is equally likely and unlikely

Unlikely

There is little reason to expect

Highly unlikely

There is very little reason to expect

Introduction

An increasing proportion of the activities that threaten critical national interests is taking place in cyberspace, and this affects the threats in all PST's areas of responsibility.

A digital society, with its dependence on electronic communication, is highly vulnerable to espionage, data manipulation and sabotage. Computer network exploitation [1] by a hostile actor can be highly damaging to a state's economy, security and political system.

Extremists make extensive use of the internet as an avenue of communication, in their own country and often at a transnational level, and digital communication will continue to be an important arena for propaganda and incitement to terrorism. Much of the current radicalisation and preaching of violence is done via social media, since this arena provides anonymity and opportunities for propaganda and discussion between like-minded individuals. This type of communication is frequently encrypted and takes place in closed forums.

Many dignitaries, including local politicians, are targets for hate speech, harassment and threats, which are mainly delivered online. This abuse strikes at democracy by making individuals reluctant to run for election or to participate actively in the public debate.

These cyber threats have the potential to cause enormous damage. The activity affects key social institutions and individuals' jobs and lives, and can interfere with the exercise of democracy.

[1] Computer network exploitation refers to the exploitation of data or information by a hostile actor who has unlawfully gained access to the computer network of an organisation for various purposes such as sabotage and data collection or manipulation.

Summary

State intelligence activity **S 4–13**

In 2020 foreign intelligence services are expected to direct their espionage activities at the political authorities, natural resources, the business sector, defence and emergency planning, and research and development.

Although PST considers that the Russian, Chinese and Iranian intelligence services have the greatest potential for harm, the covert activities of other states can also damage Norwegian interests and individuals.

Politically motivated violence **S 14–27**

At present there is an even chance that a terrorist act will be committed by right-wing extremists and by extreme Islamists.

The threat from right-wing extremism increased during 2019, and has so far resulted in one terrorist attack.

The low level of radicalisation to extreme Islamism is expected to continue through 2020.

The number of terror attacks by extreme Islamists against the West has fallen dramatically compared with the peak year 2017.

Threats against dignitaries **S 28–31**

A number of dignitaries will suffer hate speech, harassment and threatening incidents in 2020. In the case of some of them the burden will become so great that it will affect their participation in the public debate.

How does PST arrive at its conclusions? **S 32**

State intelligence activity

The targets of foreign intelligence services in 2020 will include Norwegian authorities, the business sector, defence and emergency planning, and research communities. The greatest threats are posed by the Russian, Chinese and Iranian intelligence services. The total threat picture is largely the same as that of 2019.

The work of the Norwegian government

Given Norway's border with the world's largest country, our management of enormous natural resources, our membership of NATO, and our international engagement, our policies and decisions can have major consequences for other states.

The Storting (The Norwegian Parliament), the government and the ministries are targets of the intelligence services of a number of countries. Their intelligence operations include covert tactics to obtain information that will enable foreign interests to steal a march on Norway in the field of foreign affairs.

Some countries' intelligence services also try to influence Norwegian policy in order to align it more closely with their own interests. As well as the Storting, the government and the ministries, foreign intelligence officers in Norway target political parties, consulting companies, research institutions, and the media. The aim is to influence insiders involved in Norwegian decision-making processes.

To achieve this aim, foreign intelligence officers try to cultivate individuals who have direct or indirect access to decision-making processes. The officer then tries to convince, persuade or exert pressure on decision-makers to adopt positions that promote the other state's interests.

Computer network exploitation can provide a foreign state with comprehensive information on political discussions and future decisions. These methods also include infiltrating individuals' emails, computer files, internet activity and social media profiles, making them vulnerable to persuasion or blackmail.

The influence gained by foreign states using these methods can undermine public confidence in the Norwegian government authorities. This strengthens the foreign state's room for action at the expense of Norway's, and weakens the Norwegian government's ability to safeguard the interests of the state and the individual citizen.

Norwegian politicians and civil servants visiting countries with an authoritarian regime are subject to a wide variety of surveillance methods by the local intelligence and security services. These include covert baggage searches, surveillance of hotel and meeting rooms, intercepting electronic communication, infecting phones, memory sticks and computers with malware, and contriving situations that render the individual vulnerable to persuasion or blackmail.

Espionage against refugees, and assassinations

In order to undermine, neutralise or eliminate political opposition, the intelligence services of several states use threats, detention and assassination against dissidents and political opponents of the regime who have fled to another country. To identify these individuals once they have left the home country, the services need to spy on refugees.

In 2020 foreign intelligence services will continue to spy on individuals and groups in Norway, and constitute a threat to the health and lives of individuals. For example, a Norwegian Iranian national is currently in detention in Denmark, accused of involvement in the plans to murder an Iranian exile on behalf of a foreign state. The case is due to be heard in April 2020.

In some countries political actors cooperate closely with the intelligence services. They can enable intelligence officers to collect information on Norwegian local and national politicians at a personal level and through digital or technological methods. An example of this occurred in 2018, when a political institution in a country with which Norway does not have security policy cooperation tried to install new, little-known software in the communication system of a Norwegian sister institution.

Natural resources and the private sector

Norway manages natural resources that are of critical importance for other states' energy supplies, and has untapped resources such as rare earth minerals that are used in civil and military technology.

In addition we have a number of public- and private-sector enterprises with technology communities that conduct advanced research and development. Norwegian enterprises compete with other states' economic interests in many areas, and substantial resources and important values are at stake.

In some countries state intelligence services cooperate with the business sector, and in such cases is it often difficult to distinguish industrial espionage from state intelligence activity. In many cases intelligence officers are placed in cover positions in public- and private-sector enterprises that cooperate with Norwegian actors.

During the coming year foreign intelligence services will gather sensitive information about everything from strategies and investment to product development and technological innovation. The most interesting targets are enterprises in the fields of energy, oil and gas, maritime technology, electronic communication, defence and dual-use technology, green technology and the space sector.

Information is stolen from sub-contractors as well as main suppliers of products and services. Small enterprises and niche companies are particularly vulnerable to industrial

5G – smart solutions and critical infrastructure

The fifth generation of mobile internet services (5G) will speed up communication and pave the way for a range of new smart solutions. Everything from private homes to critical infrastructure will be controlled by embedded internet-connected sensors, which will improve efficiency and result in financial savings for society and the state. However, 5G poses a number of security challenges.

The growing number of interrelated devices and machines (the Internet of Things) has increased the number of entry points through which a malicious actor can gain access to the digital system of an enterprise or individual. For most of us it is more or less impossible to discover whether the technology components or the software controlling them are compromised by malicious software that enables foreign actors to conduct espionage, data manipulation and sabotage.

5G development will also involve a further shift in the balance of power between the public authorities and commercial enterprises. Companies will be able to access and control an increasing volume of critical information, services and infrastructure that enable society to function. For example, a foreign state that is particularly interested in Norway can acquire ownership in a particular company in order to spy on and influence the company's operations. Our growing dependence on digital solutions means that any actor who controls Norwegian electronic communication has enormous power over our society.

Norway has natural resources that are crucial to other states' energy supplies. This gives Norway a certain leverage, which means that other states are anxious to gain insight into the Norwegian energy sector.

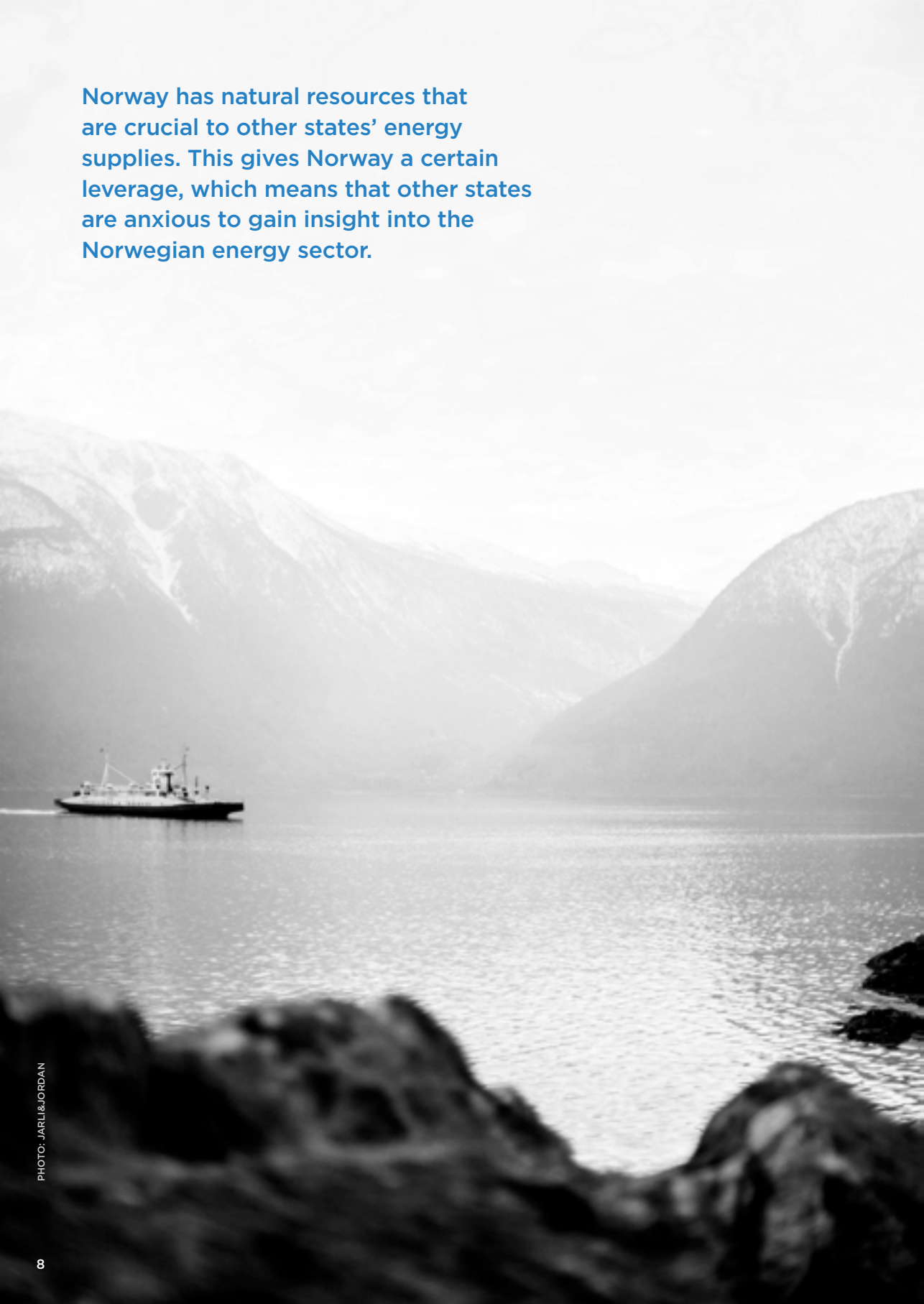


PHOTO: JARLI&JORDAN

espionage, since they usually have limited resources to spend on their security. This form of espionage is also directed at procurement activities for weapons programs.

Some intelligence officers with diplomatic cover specialise in economic and technological targets. In company with visiting officers in cover positions, they attend trade fairs and conferences in Norway to collect information and cultivate contacts who can supply them with further information.

In the coming year foreign intelligence services will continue to seek the contact details, like telephone numbers and email addresses, of employees in Norwegian enterprises. These will be used for technical collection through for example interception and network infiltration. Computer network exploitation and insiders will continue to be used to steal Norwegian companies' industrial secrets.

Foreign intelligence activity can result in the loss of a company's competitive advantage, a reduction in its market share, and the loss of income and jobs. The loss of specialists and expertise will also weaken and undermine Norwegian professional knowledge in important areas.

Defence, security and civil protection

In future crisis situations a foreign state may try to undermine Norway's defence, civil protection, crisis management capabilities and civil security in general. Institutions such as the Armed Forces, police, security and intelligence services, and agencies responsible for civil protection are important targets.

Certain institutions and industries are indispensable to the functioning of society, and may be defined as security-related targets for foreign intelligence. These include crisis management and governance (see the section on state intelligence activity) and critical sectors such as energy and water supplies, transport, banking and finance, health, and electronic communication.

Thus even in peacetime foreign intelligence services conduct reconnaissance and plan sabotage of civil and military infrastructure. Infrastructure includes bridges, harbours, shipping, radar installations, defence systems, communication lines, electricity supplies, petroleum installations, and all other military and industrial installations and facilities. The services try

Computer network exploitation – collecting, manipulating, misleading, disrupting, destroying

Computer network exploitation is an ongoing, long-term threat to Norway. A hostile actor can inflict substantial damage on Norwegian enterprises and infrastructure with very little warning and without even entering the country. Agents can steal or manipulate sensitive information and sabotage or destroy critical infrastructure anonymously, making it possible for a foreign state to deny complicity.

Another method is to recruit insiders or service personnel, or make use of visiting intelligence officers to obtain access to closed circuit systems that are not connected to the internet. There are also a number of technological methods designed to infiltrate closed systems.

Thus computer network exploitation by intelligence services can inflict the kind of damage on society and the state that was previously only possible through the use of military force.

to install reconnaissance and sabotage equipment on land and under water.

In 2020 computer network exploitation will continue to be used for data collection, reconnaissance and sabotage preparations. Hostile actors will continue to send emails with links and attachments that install malware, exploiting human error to gain entry to an enterprise. In recent years Norway and other countries have become aware of the potential for damage computer network exploitation can inflict on enterprises and infrastructure.

Foreign governments are usually able to deny any involvement in computer network exploitation against Norway. Experience has shown that state intelligence services hide their role by for example recruiting criminal agents to do the job, and only in a few cases has it been possible to trace such operations back to the government concerned.

Foreign intelligence services use a number of methods to identify activities, enterprises and infrastructure that are critical to Norway's security, such as:

- stationing intelligence officers in Norway
- sending intelligence officers on temporary missions to Norway
- supplying intelligence officers with a false identity and a false nationality
- exploiting their own country's nationals
- recruiting agents with a Norwegian or foreign identity
- exploiting insiders in Norwegian enterprises
- using aircraft, maritime vessels, motor vehicles and drones to collect information
- audio surveillance from mobile or stationary platforms in or outside Norway
- targeting computer network exploitation at devices connected to the internet
- targeting computer network exploitation at closed circuit systems
- collecting and systematising widely available information.

In the coming year all these methods will be employed against Norway, potentially damaging our capability for self-defence and crisis management.

The insider – the agent with direct access to Norwegian values

The recruitment or planting of spies inside Norwegian enterprises is a core task for foreign intelligence services. An insider in this sense is a person who exploits or intends to exploit their legitimate access to the values of an enterprise for unauthorised purposes.

An insider can inflict extensive damage on their own enterprise by compromising or manipulating information or through sabotage. Ex-employees may still possess valuable and sensitive information about the enterprise even after they have stopped working there, and can be particularly vulnerable to approaches by intelligence agents. Intelligence services sometimes find they have a better chance of succeeding if they approach former rather than current employees.

The recruitment or planting of spies inside Norwegian enterprises is a core task for foreign intelligence services.

PHOTO: JARLI&JORDAN

Research and development

Many research communities work closely with commercial actors. Research and development play a key role in a state's strategic ambitions, and some governments will go a long way to advance their own technology, for example by using their intelligence services to steal critical information and technology.

Norwegian researchers and the Norwegian private sector possess knowledge, competence, personnel and equipment that can be used by foreign states to develop their weapons programs. Norwegian research communities in the fields of physics, nuclear physics, chemistry, biology, toxicology, pharmaceutics, subsea and deep-water technology, control systems, management systems, autonomous ships, pattern recognition and artificial intelligence, engineering design, nanotechnology, satellite and missile technology, and Arctic technology are thus particularly subject to infiltration by foreign intelligence services. Many of these fields are also relevant for states with development programs for weapons of mass destruction (WMD).

In many states with WMD programs there are close ties between civilian research and weapons programs. Researchers may continue to maintain their relations with their own country's weapons program even while studying and doing research in Norway.

Several states' intelligence services have long experience of infiltrating foreign research institutions, and some authoritarian states even require their citizens by law to help the intelligence services when called upon. Research communities in such states are therefore under strong pressure from their country's services. In 2019 there were cases where researchers from countries of concern were involved in the unauthorised use of Norwegian research laboratories.

Thus Norwegian research institutions run the risk of contributing to activities that threaten the security of Norway and other like-minded countries. By obtaining Norwegian dual-use technology and expertise, authoritarian states will be able to strengthen their military capability, which they can then use either in Norway's neighbouring areas or in conflict areas in other

How secure is encryption?

Encryption is intended to make digital communication and information storage more secure. In an increasingly digitalised world, where almost all public functions depend on IT solutions, encryption is crucial to securing Norwegian values. Competence in this field is essential, not only for a state's own security and independence, but also for its capability for espionage, data manipulation and sabotage against foreign states.

Individuals and research communities in Norway with cutting-edge expertise in cryptology are therefore highly attractive intelligence targets. States that devote substantial resources to surveillance and computer network exploitation of Norwegian enterprises will also try to infiltrate groups of specialists in encryption in order to penetrate Norwegian protection mechanisms.

Cryptology and cryptology-related fields, such as information and communication security, cybersecurity, data science, physics, algorithms, quantum mechanics and quantum computing, are particularly liable to be targeted by foreign intelligence services. They are also likely to try to recruit future cryptologists who will be working with the encryption systems that safeguard the civil and military secrets of Norway and its allies.

parts of the world. States that conduct intelligence operations directed at Norwegian research and development have in recent years shown themselves ready and willing to employ military force and weapons of mass destruction against other states and their populations.

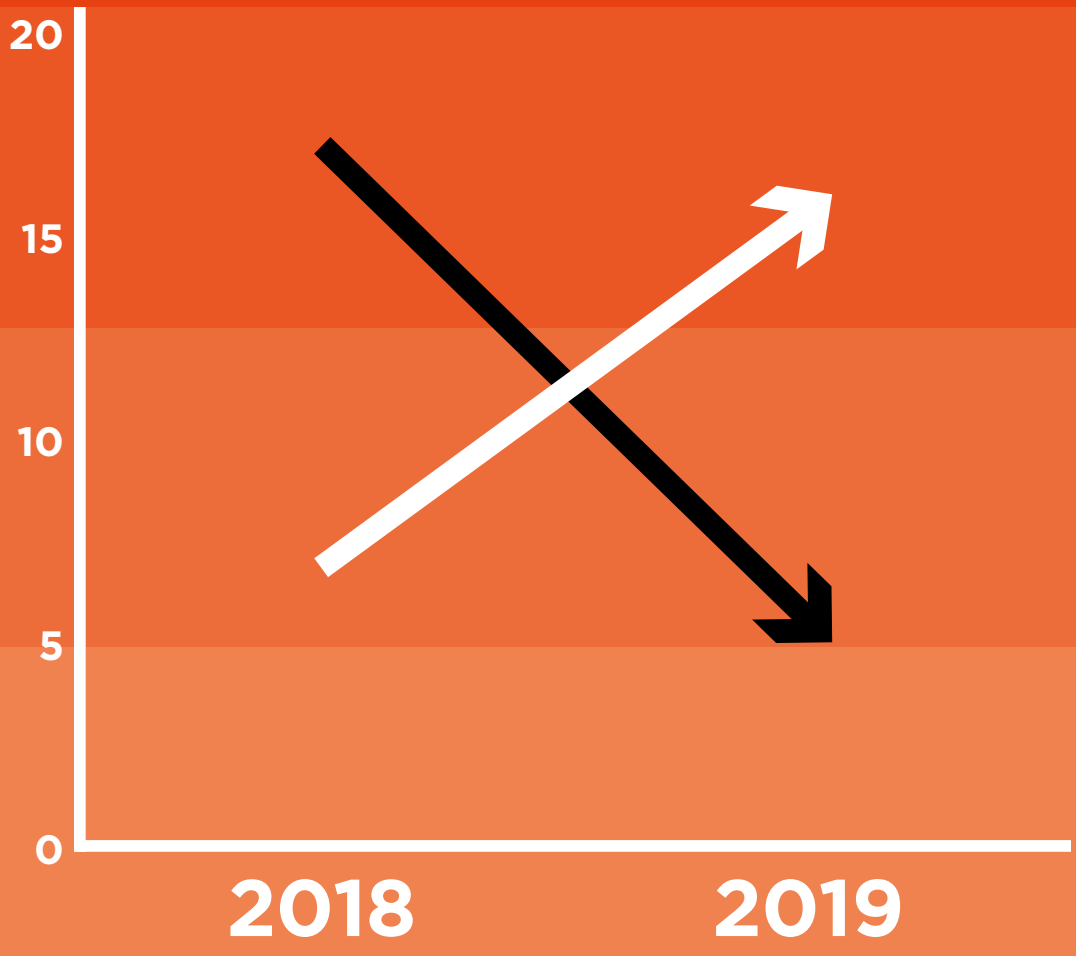
Some states that have or are suspected of having WMD programs also have close ties to terrorist organisations, so that knowledge, technology and equipment obtained in Norway may end up in the hands of a terrorist group.

Politically motivated violence

Extreme Islamism and right-wing extremism represent the two greatest terrorist threats to Norwegian security, and there is an even chance that one or more of their followers will try to carry out a terrorist attack in Norway in 2020. It is still highly unlikely that left-wing extremists will commit a terrorist act.

There was a marked increase in the number of terrorist attacks made by right-wing extremists in the West in 2019 compared with the previous year. On the other hand, the number of attacks by extreme Islamists continued to decline.

Terrorist acts by right-wing extremists
Terrorist acts by extreme Islamists



Right-wing extremism

There is an even chance that right-wing extremists will attempt to commit a terrorist act in Norway in 2020. The number of right-wing terrorist acts in the West more than doubled from 2018 to 2019. In Norway the threat from right-wing extremism also increased in 2019, and resulted in one terrorist attack. The number of Norwegian supporters of right-wing extremism terrorist acts has also risen.

At present there is an even chance that a terrorist act will be carried out by right-wing extremists and by extreme Islamists. In the past year right-wing extremist ideology and networks have become more transnational and more terror-oriented. The March 2019 attack in New Zealand will continue to serve as inspiration for right-wing extremists in the coming year.

Greater support for right-wing extremism in 2019

In 2019 there was more widespread support in Norway for right-wing terrorist acts than in 2018. Right-wing extremism falls into two main groups: those inspired by traditional Neo-Nazism and those who are anti-Islam and anti-immigration. However, although the number of right-wing extremists rose in 2019, it is expected to remain stable in the coming year.

In recent years the most conspicuous Neo-Nazi group in Norway has been the Nordic Resistance Movement, whose goal is to abolish democracy and establish a Neo-Nazi Nordic state. However, this has very little support among the Norwegian public, and the movement is not expected to recruit more members or sympathisers in 2020.

At present anti-immigration and anti-Islam groups still have few members and are unlikely to mobilise any more supporters for public demonstrations, mainly due to the low level of immigration in Norway. However, the groups will continue to spread their message: a ban on Islam and the expulsion of non-Western immigrants. Some individuals are also convinced by conspiracy theories about how Muslims and Jews are plotting to take over power in Norway and Europe.

The internet – an important arena for radicalisation

In 2020 the internet will continue to be a significant means of spreading right-wing extremist propaganda, inciting terrorism, and expressing anti-Islam and anti-immigration views. Although these persons ostensibly deny that they support violence, those who take an active part in online forums post hate speech, threats and abuse against minorities, politicians and other opponents of their views.

Right-wing extremism is becoming increasingly transnational, and the internet is a major factor in this development.

PHOTO: JARLI&JORDAN

Radicalisation[2] to right-wing extremism and incitement to violence take place mainly on social media, through propaganda and anonymous communication between individuals with the same views, together with the anonymity and lack of censorship in this arena allow these extremists to use language that goes well beyond the boundaries of what is acceptable. In addition to promoting violence, these individuals also make use of memes, references to the films and games world, irony, sarcasm and ideological symbols, which can sometimes make it difficult for outsiders to penetrate the real meaning of what is being said. Although people who threaten violence rarely act on their threats, a few may be inspired to move from words to action.

[2] 'Radicalisation' refers to the process whereby an individual develops an attitude of acceptance of or willingness to support or take part in violent acts to achieve a political or ideological goal.

> **In 2020 the internet will continue to be one of the main arenas for spreading right-wing extremist propaganda and incitement to terror**

Like other extremists, right-wing extremists often make use of encryption and closed online forums for communicating and sharing propaganda. This ensures that all opposing views and arguments can be ignored or excluded.

Right-wing extremists will continue to use online communication to create transnational networks. Their goal is to safeguard the 'white' European culture and race through violence. Several extremist networks have members who want to start a race war. The terrorist attacks in 2019 demonstrated the radicalisation potential of the internet. However, the actual planning, reconnaissance and other practical preparations for new attacks are mainly done offline.

The potential for greater radicalisation

There are several indications that radicalisation to right-wing extremism and extremist activity will increase in 2020. Any further major international terrorist acts will encourage other terrorists.

The terrorist responsible for the attack against two mosques in New Zealand in March 2019 will continue to prove an especially great inspiration for extremists in the coming year. The terrorist was

«Chans»

Right-wing extremists often use anonymous websites like the chans to discuss ideology and spread propaganda. In 2019 the websites were used to post manifestos and notice of attacks shortly beforehand.

applauded by right-wing supporters for the high casualty rate and the broad media coverage due to the fact that the perpetrator posted his manifesto and a video clip of the attack on the internet. The manifesto set out the reasons why such attacks are necessary, and encouraged the reader to do the same.

It is likely that in the coming year members of anti-immigration and anti-Islam groups in Norway will take actions that are perceived as insults to Islam. The aim will be to criticise Islam, provoke Muslims to violence and attract attention to the views of these groups.

Right-wing extremists and anti-Islam and anti-immigration supporters are expected to take advantage of any rise in immigration and any public controversies about integration and minority protection to strengthen support and justify terror.

It is also likely that right-wing extremists will take advantage of any rise in the number of terrorist acts by extreme Islamists in the West in 2020 to justify new acts of revenge. Some acts by right-wing extremists in recent years have been motivated by revenge.

The Bærum attack

On 10 August 2019, a right-wing extremist carried out a terrorist attack in Bærum municipality. One of the sources of inspiration for the attack was Brenton Tarrant, the man who committed the New Zealand attack. The Bærum attack was the first act of terrorism committed by a right-wing extremist in Norway since 2011.

> Right-wing extremists are becoming more willing to use terror to achieve their goals

Terrorist acts committed by lone actors

The threat from right-wing extremism is more likely to come from an individual than a group. Any potential terrorist attack in 2020 will probably be directed at a meeting place for Muslims or non-Western immigrants so as to kill or injure as many as possible. Norwegian dignitaries and politicians who are perceived as facilitating immigration and destroying the Norwegian way of life and culture are also potential targets, in addition to Jews, individuals with a non-Western appearance, lesbians, homosexuals, bisexuals and transsexuals, and any others considered to be strongly opposed to right-wing ideology.

Experience from the past year indicates that the most likely weapons will be firearms, improvised explosive devices and vehicles.

PST's role in preventing radicalisation and extremism includes informing and advising the police and other local partners.

PHOTO: JARLI&JORDAN

Extreme Islamism

There is an even chance that extreme Islamists will try to carry out terrorist acts in Norway in the coming year. However, the extent of radicalisation to extreme Islamism in this country is expected to remain limited in the current year. There has also been a dramatic decline in the number of terrorist attacks by extreme Islamists against the West since the peak year 2017.

There are several factors that could intensify the threat posed by extreme Islamists in 2020, such as repeated incidents that are perceived as insults to Islam.

Certain developments, like the growth of network-building among extreme Islamists in Europe, also have the potential to aggravate the situation in Norway. Despite the further weakening of ISIL in 2019, the organisation and its sympathisers still intend to strike at Western countries.

> For the last few years there has been no cause powerful enough to mobilise extreme Islamists in Norway

The limited scale of radicalisation and small number of terrorist acts

We expect the extent of radicalisation to remain limited in 2020. Extreme Islamism still has few supporters in Norway, and few active radicalisers. There is little activity among radicalised individuals, and none of the organisations in Norway promote extreme Islamist ideology in a physical public setting. The existing activity takes place in religious arenas, in prison and online. Online activity is anonymous and encrypted, which means that threats are hard to discover but also that fewer people come in contact with the propaganda and indoctrination.

ISIL is expected to go on being the greatest inspiration for extreme Islamists in Norway. The West has been defined by ISIL and al-Qaeda as the stereotypical enemy, since they perceive Western countries as being at war with Islam and Muslims in the West and in Muslim countries. While Norway plays a relatively small part in this enemy stereotype, it occupies a central place in the minds of the extreme Islamists who live here.

Factors that could rapidly alter the threat picture

In recent years there has been little activity among extreme

Islamists in Norway, due to lack of a cause powerful enough to mobilise them, and this trend is expected to continue. ISIL adherents seem to be fairly resigned about the gradual weakening and fall of the caliphate, but events perceived to be an insult to Islam could trigger more radicalisation, activity and violence. Norwegian military operations in Muslim countries, the strengthening of ISIL's position in Syria, and circumstances surrounding the return of foreign fighters could also provoke a reaction and encourage radicalisation.

Repeated incidents that are perceived as insults to Islam will also be a potential cause of radicalisation, since even moderate Muslims may find them offensive. Violent responses to the offensive behaviour will not necessarily be limited to the geographical region where it has taken place, since photos and videos of the incident will be rapidly spread via the internet.

Any new incidents of offensive behaviour in Norway will be widely disseminated via the internet and foreign media. It is likely that repeated desecration of the Koran will trigger progressively stronger protests and reactions, and acts in other European countries will reinforce the response in Norway and against Norwegian interests abroad. Repeated incidents will potentially also make Norway a more important enemy target for extreme Islamists outside the country, which means that a terrorist act in Norway could well be planned abroad.

Extreme Islamism – a latent threat

Despite being considerably weakened, ISIL is still active in Syria, Iraq and other parts of the world, and still determined to strike at Europe.

In the coming year developments in European networks that sympathise with ISIL will have a decisive impact on the threat posed by these extremists in Norway. No other extreme Islamist terrorist organisation has ever had so many sympathisers in Europe. It is likely that the many foreign fighters and convicted terrorists who will be released in the next few years will set up physical and online networks, which are likely to be used to radicalise individuals, encourage terrorism and plan physical terrorist attacks across borders.

The threat posed by European networks of extremists will also be influenced by whether these extremists are inspired or guided by, or cooperate with, organisers of terrorism. There is also an even chance that an increase in the number or scale of terrorist acts in other European countries will inspire terrorist activity in Norway by local extremists.

Al-Qaeda will continue to be motivated by their fight for a future caliphate and by what they perceive as the West's war on Muslims. Although the organisation still intends to attack Europe, it is not expected to pose the same threat as ISIL in 2020. The existence of Norwegian extremists who are primarily

Tips from the public are very important for our ability to identify, clarify and reduce threats to Norwegian security from left-wing extremists.

PHOTO: JARL I&J ORDAN

engaged in regional conflicts in Asia and Africa is another factor that influences the threat picture. While these extremists have no intention of attacking targets in Norway, they collect funds and support other activities from here.

Isolated terrorist acts are still the most likely form of terrorism

Any attempted terrori st act by extreme Islamists in Norway in 2020 is expected to involve only one or two people. Both ISIL and al-Qaeda encourage their supporters to commit attacks singly in order to avoid discovery.

Both symbolic[3)] and general[4)] targets are potential objectives for any extreme Islamist attack. A general target is likely to be a crowded venue with low security. The most likely symbolic targets are ideological opponents, individuals who insult Islam and uniformed police and military personnel who are out in the public arena. Police and military personnel are perceived as key representatives of the state and defenders of Western efforts to oppress Muslims and wage war on Muslims in conflict areas.

The most likely weapons are edged weapons and blades, vehicles, firearms and simple improvised explosives. The first of these are particularly suitable because it is difficult to find out whether they will be used for terrorism.

3) 'Symbolic targets' refers to targets related to these extremists' core ideology.

4) 'General targets' refers to targets without particular ideological significance apart from representing or being located in the West.

Left-wing extremism

It is highly unlikely that left-wing extremists will try to carry out a terrorist act in Norway in 2020. However, we expect them to use violence against their opponents, usually during demonstrations. It is unlikely that left-wing extremist groups will recruit more members the coming year.

A stable level of left-wing extremism

The left-wing extremist groups in Norway are small and few. In recent years, however, some have become more active, and have shown a greater tendency to use violence against political opponents. We expect this situation to continue in the coming year.

Left-wing extremist causes in 2020 will be the same as before: combatting fascism, racism, homophobia and anti-feminism. In the long term, their goal is to establish a classless society without government or hierarchies. Other issues that engage

them are capitalism, climate and the environment, the Israeli-Palestinian conflict, asylum and immigration policy, and opposition to NATO and foreign military forces on Norwegian territory. Controversial events in any of these fields may trigger more activity from extreme left-wing groups.

> In the last few years left-wing extremists have physically attacked persons they define as right-wing extremists

Left-wing aggression will continue to be directed at right-wing extremists and anti-immigration and anti-Islam groups and individuals

In 2020 the cause most likely to trigger violence by left-wing extremists will be right-wing extremism. The degree of activism and recruitment to left-wing groups will therefore mirror that of right-wing extremists and anti-immigration and anti-Islam groups. Left-wing extremists are likely to identify, harass and try to commit violence against these groups.

There is an even chance that police officers who are on guard during left-wing demonstrations will be attacked by the demonstrators, since left-wing extremists regard the police as an enemy who protects and facilitates fascism and capitalism.

Norwegian left-wing extremists are in contact with individuals and groups abroad who may have a lower threshold for violence. There is an even chance that this will radicalise Norwegian groups and inspire them to more violence against their opponents.

PHOTO: JIŘÍ HAVRAN

Threats against dignitaries

Hate speech, harassment and threatening incidents will continue to be directed at Norwegian dignitaries in the coming year. In the case of some dignitaries, the abuse will be so extensive that it will make them reluctant to participate in the public debate.

Threats against dignitaries

Dignitaries [6] are the highest-ranking individuals in the state and government. Norway's most vital constitutional and democratic values therefore depend on maintaining their security and room for action. They also deal with sensitive and confidential information and their decisions can have national and international significance.

Dignitaries will continue to receive threats in the coming year. However, the nature and intensity of the threats will vary considerably. Some positions are particularly liable to become intelligence targets for foreign states, especially in cases where these states have strategic interests that are in conflict or in competition with Norwegian interests (see the section on state intelligence services).

Although not all dignitaries or politicians fit into the enemy stereotype of Norwegian extremists, those who deal with sensitive topics like immigration are likely to be targeted by right-wing extremists (see the sections on right-wing extremism and extreme Islamism). However, the greatest threat is the lone individual who does not belong to any group. Such people's motives are just as often rooted in personal grievances or political discontent as in ideology or politics, which makes it difficult to identify potential perpetrators of violence.

Dignitaries in Norway are and will continue to be safe, but this safety is becoming compromised. Abusive language and the use of violence against politicians are now a source of concern. Hate speech, harassment, online shaming and threatening language against individual dignitaries on social media are an everyday occurrence. Young politicians and those engaged in immigration, environmental and taxation policy are particularly exposed. Sometimes even local issues or issues that have ramifications for only a few individuals can result in pressure, threatening language and/or unlawful acts directed at the person of the dignitary or politician.

The accumulation of negative attention and behaviour has become a heavy burden for certain dignitaries. Ultimately this means that some of them will refrain from putting themselves up for election, leave politics altogether or be pressured into making decisions they would not otherwise have made. It can also lead to a situation where a politician declines invitations to take part in public debate on subjects they know to be inflammatory. This constitutes a threat to democracy.

[5] Government ministers and members of the Royal Family, the Government, the Storting and the Supreme Court.

PHOTO: JIRI HAVRAN

Some dignitaries are particularly liable to be targets of intelligence activity and pressure from foreign states.

How does PST arrive at its conclusions?

The purpose of the national threat assessment is to convey what we believe to be the most likely developments in the threat picture in the coming year, and to indicate those factors that are expected to change. Our analysts use a number of structured analytic methods to quality assure the conclusions and to identify factors where the level of uncertainty is highest, and why.

The analysts monitor developments within a fixed framework of factors, or indicators, that influence the threat picture. These may be located inside the country or abroad. Our assessment of developments abroad is based on information from cooperation partners like the Norwegian Intelligence Service, and our assessment of developments inside Norway is largely based on our own reconnaissance.

Some of the indicators we study are quantifiable, while others require a qualitative evaluation. The trends in the various indicators are followed over time and viewed in relation to each other. It is extremely rare that a particular trend on its own significantly alters the threat picture.

DESIGN: CREUNA PRINT: STAPLES

The Police Security Service
vww.pst.no