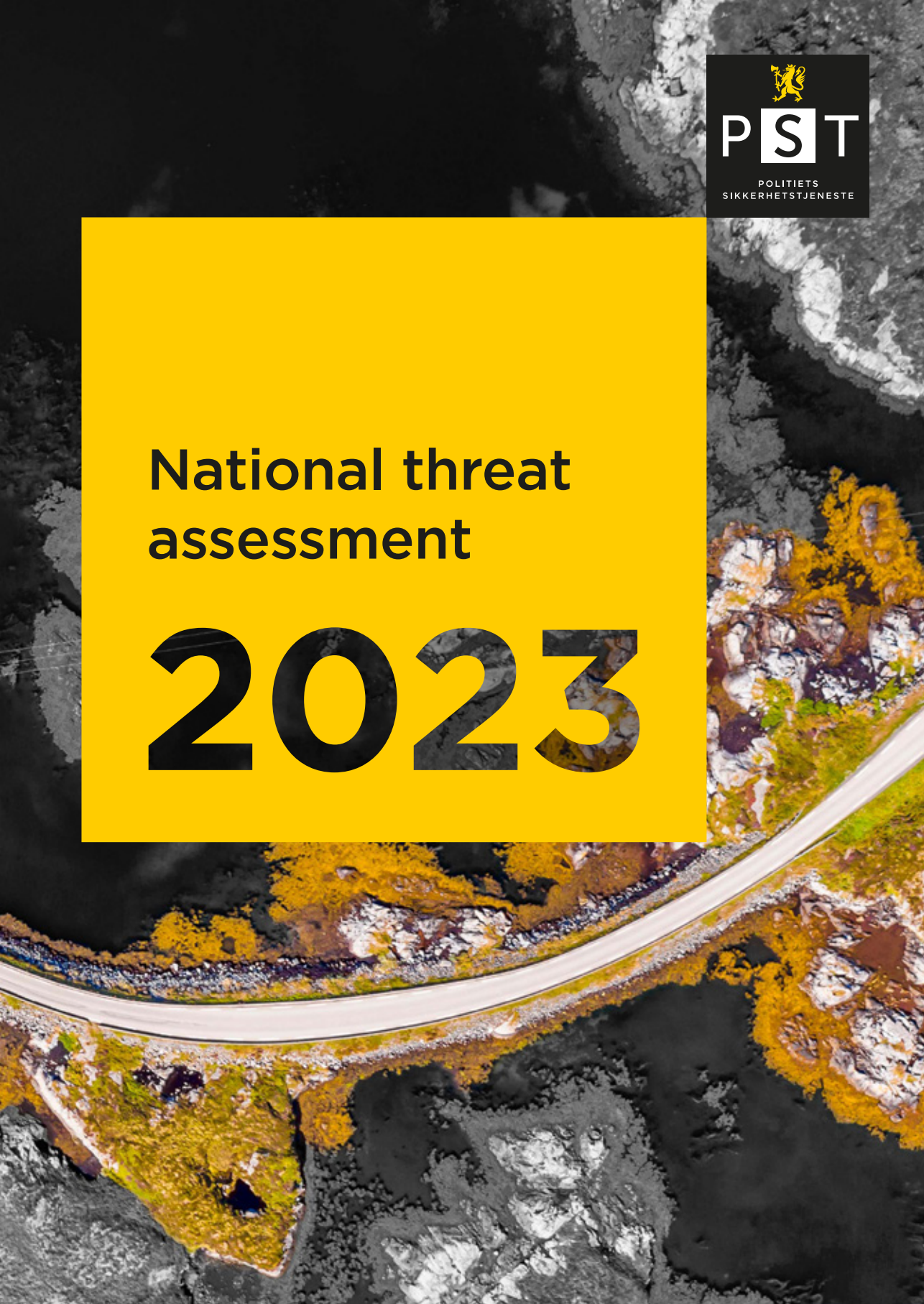


POLITIETS SIKKERHETSTJENESTE

National threat assessment

2023

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

The Norwegian Intelligence Service (NIS) is Norway's foreign intelligence service. Although it reports to the Chief of Defence, the service's areas of responsibility include civilian as well as military matters. NIS's main tasks are to supply information on external threats against 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, 'FOKUS' (FOCUS), is an analysis of the current situation and expected developments in thematic and geographical areas of particular relevance to Norway's security and national interests.

The Norwegian National Security Authority (NSM) is Norway's directorate for preventive security services. NSM strives to ensure that Norway can protect itself from espionage, sabotage, terror and hybrid threats. Through advisory services, research, oversight, testing and control activities, NSM helps ensure that undertakings protect civilian and military information, systems, objects and infrastructure of importance for national security. NSM also bears national responsibility for identifying serious cyber operations, warning about them and coordinating responses. A report entitled 'Risiko' (Risk) is NSM's annual assessment of the risks to Norway's national security. The report recommends measures and assesses how vulnerabilities in Norwegian undertakings and services affect risks in the light of the threat picture described by the Norwegian Intelligence Service and PST.

Introduction

In the National Threat Assessment (NTV), the Norwegian Police Security Service (PST) presents an unclassified review of the threats facing Norwegian society this year. The assessment focuses on the intelligence threat, devoting special attention to Russian and Chinese intelligence activities, as well as to the threat of terrorism and threats facing Norwegian dignitaries.

The NTV has been compiled during a time impacted by Russia's war of aggression against Ukraine, as well as by the shooting incident in Norway on 25 June 2022, which PST considers an Islamic extremist terrorist attack.

The war has profoundly altered relations between Russia and Western countries, including Norway. This impacts the threat posed by Russian intelligence services in Norway. However, the intelligence threat posed by other countries will continue to be characterised by continuity, and no major changes are expected during the current year.

A regards the terrorist threat, it will come from several different branches of extremism. In addition, the threat will be characterised by extremists being more prone to adapt their choice of ideology, mode of operation and choice of targets to their own preferences. This makes the threat more complex, and may make it even more challenging to detect radicalisation and potential terrorist plots.

NTV 2023 addresses a broad, widely diverse target group. On the one hand, the report is intended for members of the general public who seek comprehensive information on the status of and expected trend in the threat picture. On the other, the NTV is for the benefit of individuals and enterprises that require information for their own security efforts, but do not have access to classified assessments. Consequently, it is important that all those who read this report consider its content and make their own assessments of its relevance to and consequences for their own undertakings in the light of the assets they manage. Otherwise, please see *Using the National Threat Assessment* on the next page.

Vigilance and tips from the public are important for PST's efforts to avert terrorist attacks, threats against dignitaries, espionage, the proliferation of weapons of mass destruction, and refugee espionage.

If you have any tips,
contact us at:

PST.no/tips-oss

Using the national threat assessment

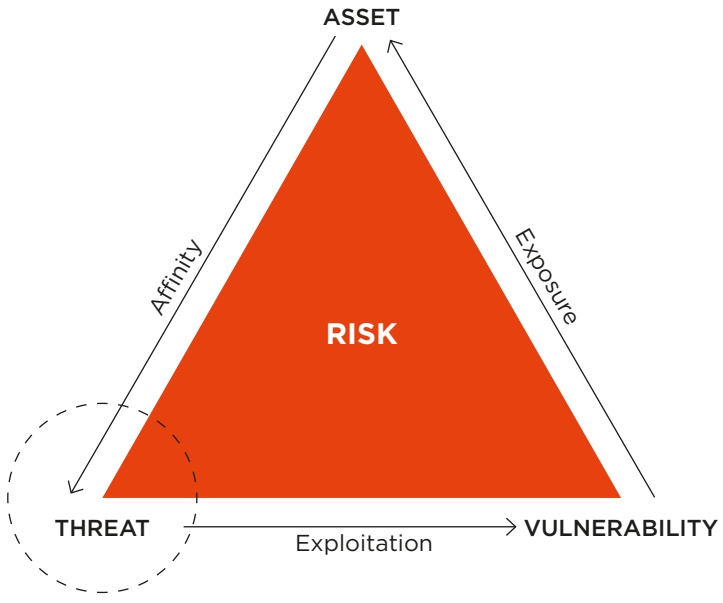
The national threat assessment is an analysis of expected developments in PST's areas of responsibility in the year ahead. It is intended to create awareness of the most serious threats facing Norway and to provide decision-making support in connection with the important preventive security measures for which enterprises are responsible. The enterprises must also take into account other threats that could affect their own undertakings, e.g. other types of crimes or other undesirable incidents.

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

- Risk can be defined in several ways. In this context, risk is discussed as a combination of assets, threats and vulnerability, and the national threat assessment is intended to be used as a resource to inform decisions about potential risks.
- A good assessment of assets provides grounds for assessing relevant threats to a particular undertaking. Further, an assessment will highlight ways in which threat actors can impact an undertaking's assets. In this context, it is also important to examine any dependencies, including those outside the undertaking itself. This will provide a basis for the vulnerability assessment, which describes the extent to which the undertaking's assets are vulnerable to identified threats, which, in turn, forms the basis for introducing preventive and mitigation measures related to potential consequences.
- Based on this, a risk assessment must be carried out to determine whether the undertaking maintains an appropriate level of security.

In the work with preventive measures, you can also search for information on the following websites:

pst.no
politiet.no
nsm.no



Using degrees of probability

This assessment uses a set of standardised terms to designate degrees of probability. They are emphasised in the text in boldface. The purpose of this is to create a more uniform description of probability in the assessments and thereby to minimise the risk that they are unclear or could be misunderstood. The terms and the associated definitions of their importance have been compiled jointly by the police, PST and the Armed Forces.

Highly likely

Very good reason to expect.
More than 90% probability.

Likely

Good reason to expect.
60–90% probability.

Even chance

Equally likely and unlikely.
40–60% probability.

Unlikely

Little reason to expect.
10–40% probability.

Highly unlikely

Very little reason to expect.
Less than 10% probability.

PST's terrorism threat scale

PST's terrorism threat scale is intended to give a general impression of the terrorism threat situation. While the degrees of probability represent PST's assessment of the likelihood that the various forms of extremism will attempt to carry out an act of terrorism, this scale expresses the degree of severity of the situation.

X Extraordinary threat situation

4 High threat of terrorism

3 Moderate threat of terrorism

2 Low threat of terrorism

1 No known threat of terrorism

Determination of the level of a threat of terrorism is based on the threat assessment, along with the degree of severity of the situation, elements of uncertainty and the authorities' ability to implement countermeasures.

Summary

State intelligence activities
Pages 6–23

Several countries' intelligence services operate on Norwegian territory. In PST's opinion, Russian intelligence services will pose the greatest threat to Norway this year.

Foreign states' intelligence services employ a wide variety of methods and means in Norway, including computer network operations, the recruitment of sources, and covert procurement activities.

Computer network operations will account for a large part of Russian and Chinese intelligence activities in Norway. Cyber threat actors are developing increasingly more sophisticated methods and means for gaining access to sensitive information.

Russia, as well as other states, has intelligence officers stationed in Norway. They will persist in trying to recruit sources and contacts with access to the information they seek.

It is **unlikely** that Russia will carry out an act of sabotage on Norwegian territory in 2023. However, acts of sabotage could become a more relevant scenario if Russia's willingness to escalate the conflict with NATO and the West were to increase.

In 2023, Norwegian undertakings will be exposed to covert and clandestine attempts to procure goods and technology made by actors involved in foreign states' programmes for weapons of mass destruction and other military development. Norwegian research and educational institutions will be exploited for illegal transfer of knowledge. Actors with ties to Russia, China, Iran and Pakistan will pose special challenges.

Several authoritarian states will use their intelligence services to identify, monitor and influence their own nationals who are residents of Norway. Their intent is to restrain, undermine or eliminate political opposition.

Politically motivated violence – extremism
Pages 24–39

Islamic extremism and right-wing extremism are expected to represent the greatest terrorist threats to Norwegian society. PST believes there is an **even chance** that Islamic extremists and right-wing extremists will attempt to carry out terrorist acts in Norway in 2023.

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

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

PST considers it **unlikely** that anti-government extremists will try to commit acts of terrorism in Norway in 2023. Anti-government ideas and conspiracy theories will nonetheless still result in the radicalisation of certain individuals, and such notions may be perceived as justification for the use of violence and non-democratic means.

PST considers it **highly unlikely** that left-wing extremists or extremists motivated by climate-related, environmental or nature conservation issues will try to perpetrate terrorist acts in Norway in 2023. Our assessment is nevertheless that issues related to the climate, the environment and nature conservation do have a potential for radicalisation.

Threats to dignitaries
Pages 40–43

PST considers it **unlikely** that dignitaries will be the target of serious acts of violence in Norway in 2023. However, demanding economic times could escalate threat activity. Threats and harassment against politicians constitute a serious challenge to democracy since the collective pressure on multiple dignitaries and politicians could lead some to withdraw from public discourse or to refrain from running for office.

State intelligence activities

Russia is still waging war against Ukraine. This has profoundly altered Russia's political, diplomatic and economic relations with Western countries, including Norway. The new security policy situation has consequences for the threat picture in Norway.

PST's assessment is that at this juncture, Russia has more to gain and less to lose by running intelligence activities in Norway. Recently, individuals suspected of illegal intelligence activities on behalf of Russia have been arrested in Norway and several other European countries. However, Russian intelligence activity is hardly a new phenomenon in Norway. In many ways, the activity we expect in 2023 will be consistent with what we have been seeing for quite some time. This also applies to other states' intelligence activities, e.g. China, Iran and North Korea.

In the following, PST provides a general assessment of how state actors, especially Russia and China, will present a threat to Norwegian interests in 2023.

Sign upon entry into Barentsburg on Svalbard.
Photo: Erin Schaff/The New York Times/NTB

PST expects that Russian intelligence services will be interested in information about actors involved in Norway's administration of Svalbard

Russian services will present the greatest threat

Russian services will present the greatest intelligence threat to Norway in 2023. Norway's NATO membership and close cooperation with the USA, our strategic location, and our border with Russia, as well as our abundant natural resources and competitive technology are among the reasons why Russian intelligence services have been and continue to be highly active in Norway.

Over the past year, relations between Russia and Norway have deteriorated significantly. Norwegian and Russian authorities are meeting in fewer arenas than before. Moreover, economic sanctions have weakened trade relations, investments and economic cooperation between the two countries. This means that Russia's access to information about conditions in Norway is no longer as easy as it once was. To compensate, Russian authorities must rely on their intelligence services to a greater extent to cover their need for information in Norway. This tends to exacerbate the Russian intelligence threat in Norway.

Another consequence of the deteriorating relations between Norway and Russia is that Russia has less to lose if the country's intelligence operations in Norway are exposed. PST therefore believes that Russia may be willing to accept higher risk in respect of its intelligence activities in Norway.

PST expects that Russia's war of aggression against Ukraine and conflict with the West will only to a limited degree impact the general goals of Russian intelligence activities in Norway. The new security policy situation will, however, entail some changes in Russia's priorities as regards its need for information in Norway.

Russian intelligence services in Norway will continue to try to gather information about Norwegian political processes that have, or could have, a bearing on Russian interests.

What is more, Russia will continuously strive to obtain an overview of all military capacity that could have an impact on Russia's security and freedom of action. Inasmuch as Norway is a member of NATO, Norwegian and Allied activities and their presence in Norway will inevitably be important intelligence targets for Russia.

Further, the High North is of great strategic importance to Russia. It will be decisive for Russia to maintain the understanding of the situation in the region. Russia will also try to gain an overview of Norwegian and multilateral processes for the future development of the Arctic and the High North.

Every change in or uncertainty about Norway's policy in the High North will be of interest to Russian intelligence services.

PST expects Russian intelligence services to be interested in information about actors involved in Norway's administration of Svalbard (Spitsbergen). In 2022, Svalbard was designated a separate customs territory. Historically, there has been no control of the goods imported to and exported from Svalbard, or of whether they are imported or exported in contravention of embargos and restrictions. Accordingly, we expect that Russia will track Norway's control activities on the archipelago.

Information that could impact the war in Ukraine will be of particular interest to Russia in 2023. Among other things, Russian intelligence services will devote attention to the response of Norway and the West to Russia's warfare. Information about what military support Norway and other Western countries are planning to provide, as well as information about political and economic sanctions against Russia, will probably have high priority.

This year, we also expect that Russian intelligence services will need new political and military intelligence related to the consequences of NATO's enlargement in the Nordic region. Swedish and Finnish NATO membership could escalate the overall importance of the Nordics for Russian intelligence services, leading Russia to give higher priority than before to intelligence activities against the Nordics as a whole.

Further, Norway's role as an energy supplier to Europe has assumed even greater security policy importance as a result of the war in Ukraine. Over the past year, we have seen the emergence of Russian ambitions to exert pressure on European energy security. PST therefore expects that in 2023, Russia will try to gather intelligence about most aspects of Norway's oil, gas and energy sector.

Part of Russia's need for intelligence in 2023 will also focus on how Norway handles crises, and how we would deal with any acute situation involving Russia. For that reason, the EOS services, the police and the rest of the civilian emergency preparedness system in Norway will continue to be valuable targets for Russian intelligence operations.

Western technology is coveted by Russia's civilian and military industries. Russian industry used to find it easier to procure this technology legally. In 2023, the expanded sanctions regime and stricter export restrictions will heighten Russia's need for western goods, technology and related expertise. For that

Sweden's former Prime Minister Magdalena Andersson (Swedish Social Democratic Party) and NATO's Secretary General Jens Stoltenberg meet in Harpsund for talks about Sweden's application for NATO membership. Photo: Peter Wikström/TT/NTB

This year, we expect that Russian intelligence services will need new political and military intelligence related to the consequences of NATO's enlargement in the Nordic region

reason, PST expects Russia to carry out covert and clandestine attempts to make procurements in and through Norway this year.

Persistent intelligence threat from China

PST expects no major changes in the intelligence threat posed by China in Norway. China will continue to constitute a significant intelligence threat against Norwegian interests this year. Chinese intelligence will employ a wide variety of means to obtain advanced technology, expertise and sensitive information from Norwegian undertakings and institutions. China will also be interested in intelligence about Norwegian policy making, especially as related to international cooperation and the High North.

In March 2023, Norway will assume the presidency of the Arctic Council. Strategies and processes related to the High North are among the most vulnerable intelligence targets in Norwegian politics. China will continue actively to strive to obtain information and to influence Norwegian processes related to development in the North. We expect China to continue to give priority to its long-term positioning in the High North, especially in relation to the future exploitation of natural resources. China will also try to purchase or establish businesses on strategically located properties in the High North. A stronger Chinese presence in the High North could challenge Norwegian security interests by facilitating intelligence operations and creating economic dependence that is vulnerable to exploitation.

The Chinese state does not operate with clear distinctions between the state sector and the private sector, but uses a wide variety of actors to achieve its political objectives. According to the Chinese Intelligence Act, every Chinese citizen, business and organisation is duty-bound to assist the intelligence services if asked to do so. One consequence of this is that it is impossible to distinguish private actors from actors who contribute to illegal intelligence activities for the state of China. Chinese companies or students that may initially have legitimate intentions can be ordered to spy on behalf of the party-state. The upshot of this is that visits from delegations and other travellers are important recruitment platforms for Chinese intelligence services. The lifting of Covid-19-related travel restrictions means that the intelligence threat associated with Chinese delegations will see an upswing this year.

PST observes that several European countries have been subjected to pressures and threats from China in recent years, in attempts to change or influence decisions made by these countries. China will continue to take advantage of economic dependence and use its intelligence services to target countries with which it has diplomatic conflicts.

Taiwan's representative office in Vilnius, Lithuania.
Photo: Andrej Vasilenko/The New York Times/NTB

China resorts to pressure and threats in diplomatic conflicts

In January 2022, Lithuania was subjected to a comprehensive hybrid reaction from Chinese authorities when the country allowed Taiwan to open a representative office in Vilnius. Lithuania was subsequently made the target of a coercive campaign and multiple cyber attacks. In addition, the country was subjected to heavy pressure on supply chains, the suspension of services, and other formal and informal sanctions. At the same time, Lithuanian companies had trouble procuring Chinese parts and components. Chinese authorities also pressured businesses in other European countries to get them to restrict their dealings with companies from Lithuania.

Which methods and means will foreign states use in Norway?

Foreign states' intelligence services employ a wide variety of methods and means in Norway. In the following, we examine what methods we expect to be used or what we believe might be relevant in 2023. These include:

- Computer network operations
- Recruitment of sources
- Digital and physical sabotage
- Influence operations
- Covert procurement activities and illegal transfer of knowledge
- Monitoring and threats

State actors will use computer network operations for covert activities in Norway

Computer network operations represent a persistent, serious threat to Norwegian assets. Cyber threat actors adapt to current security policy situations, developing increasingly more sophisticated methods and means for achieving their goals. Several intelligence services include cyber threat actors that operate in cyberspace, and computer network operations are one of their most important tools for gaining access to sensitive and classified information. The computer network operations against the Storting (Norwegian Parliament) in 2021 are examples of extremely serious incidents in Norway.

Computer network operations and digital espionage are cost-efficient and entail little risk compared with other methods for gathering intelligence. A computer network operation can be mounted with few resources while enabling the actor to strike many targets. Using advanced techniques to conceal their identities, actors enjoy a high degree of anonymity. This makes it difficult to attribute the attacks to a particular actor, engendering few consequences for those state actors that avail themselves of this method for gathering intelligence.

When state actors mount computer network operations, they generally do so to achieve espionage and intelligence goals. Among other things, PST expects intelligence services to track and obtain information on Norwegian undertakings. At the same time, we expect to see computer network operations that can be described as disruptive by nature, such as denial-of-service attacks.

A broad range of methods

Cases that have come to light in recent years illustrate the broad range of methods employed by foreign intelligence services that operate in Norway. Among the most serious cases, we find PST's apprehension of a guest lecturer at the University of Tromsø (UiT), suspected of being a Russian illegal. In addition, we have seen Chinese and Russian computer network operations aimed at private and public undertakings, and Russian recruitment of an insider in a major Norwegian private enterprise, as well as several breaches of Norwegian export control legislation for the benefit of countries like Iran and Russia.

In Norway, the largest threat actors in the digital domain are Russia and China, but other countries, such as Iran and North Korea, also engage in computer network operations in Norway. PST expects that these countries will try to strike Norwegian targets in 2023.

Over the past year, PST has seen that several state intelligence services, or threat actors operating on their behalf, have carried out so-called supply chain attacks. These are computer network operations aimed at weak, more peripheral points in an undertaking's supply chain, e.g. subcontractors. Undertakings with robust data security systems and routines are vulnerable if their subcontractors do not have corresponding security measures. PST expects several computer network operations of this type in 2023.

Cyber threat actors continuously try to cover their tracks on the Internet. To make it more difficult to trace them, they use computers in different countries as hop-points. A hop-point is an intermediate step in a computer network operation, i.e. it is not a final target. The primary target is often hit from a computer located in a third country. On several occasions over the past year, PST has discovered infrastructure in Norway being used by Russian and Chinese threat actors as hop-points for operations against other countries, including Norway's allies.

In the coming year, a larger share of computer network operations will exploit digital infrastructure in Norwegian homes. In such cases, the threat actor will gain access through home electronics linked to the Internet, e.g. PCs, routers and smart TVs, taking advantage of them as hop-points. Such units generally have rather weak data security, making it easy to exploit them as a link in computer network operations/cyber attacks.

Denial-of-service attacks

A denial-of-service attack entails overloading a website with traffic to prevent it from being accessible to users. Denial-of-service attacks do not usually cause long-term damage, but they can be disruptive. A successful denial-of-service attack ensures that a website cannot be used. If there are important functions on the website, this means that users cannot access these services for as long as the website is down. Most websites have measures in place to protect them against denial-of-service attacks.

In 2021 and 2022, there were several instances of criminal actors being driven by the same intention or goal as state actors. We are observing this mode of operations in several countries. One example is Killnet, a 'hacktivist' group that identifies itself with Russia; it has carried out denial-of-service attacks against several government institutions and undertakings in Europe. There are also instances of intelligence services and criminal actors working together on cases involving ransomware, and cases in which intelligence services' own cyber threat actors are seeking to commit crimes for profit.

Norwegian undertakings can take simple measures to mitigate vulnerabilities

Cyber threat actors are continuously searching for vulnerabilities that might allow them access to their targets. One similarity shared by many successful computer network operations is that the threat actor has exploited vulnerabilities which, in retrospect, would have been easy to eliminate. This includes, e.g. the re-use of weak passwords, the lack of two-factor authentication and outdated software.

A computer network operation is usually initiated using data retrieval. If the target is an undertaking, the threat actor will seek to get an overview of the undertaking's assets, employees and technical infrastructure. The goal is to identify vulnerabilities that can be exploited to gain access to the undertaking's digital assets.

So-called phishing attacks will continue to be the easiest, most commonly used method for gaining access to information about a person or an undertaking. Phishing involves duping an employee into clicking on a link in an e-mail received from a seemingly trustworthy source. Cyber threat actors may also exploit vulnerabilities like weak passwords, outdated software and the lack of two-factor authentication to gain illegal access to information. Both methods can potentially allow the cyber threat actor to large volumes of sensitive information.

Individuals are more vulnerable to computer network operations

Political decision-makers, researchers, military personnel, dissidents and diaspora communities are increasingly being exposed to computer network operations staged by foreign states' intelligence services. This differs from earlier years when the threat actors primarily targeted institutional networks.

Among other things, this is because access to commercial malware makes it easier for countries with limited cyber capacity to carry out computer network operations. However, the threat from these countries also comes from countries with the ability to develop their own network capacity, for example, China and Russia.

The consequence of a computer network operation aimed, for example, at members of the refugee diaspora may be that the threat actor gains access to all their correspondence, plans, contact information and contact networks. This gives the threat actor unique insight. For instance, such information can be used to facilitate computer network operations against others in the same network, or to build a case against an individual in his/her homeland.

Foreign intelligence officers will attempt to recruit sources in Norway

Several states have stationed intelligence officers under diplomatic cover at their official representative offices in Norway. Their core task is to identify, cultivate and attempt to recruit individuals in Norway.

In PST's opinion, Russian intelligence officers in Norway experience a more challenging operational environment now than prior to Russia's invasion of Ukraine. One reason for this is that certain types of sources of information have become less accessible due to the political climate and greater vigilance among the members of the general public in response to the threat from Russia. To maintain access to information in the new political climate, Russia has no resort but to increase the use of covert acquisition, including the use of insiders and other agents. Russia's increasingly authoritarian use of power may also mean that Russian nationals in Norway with access to sought-after intelligence will be subjected to threats or pressure to get them to cooperate with Russian security and intelligence services.

For foreign intelligence officers, individuals with access to sensitive and classified information will be high-priority targets. At the same time, there are also many others who could potentially help intelligence officers by responding to their need for information. It can take many years to develop potential sources. For example, intelligence officers will seek out young people who they believe might eventually gain relevant influence and access to information.

Illegals

Russian authorities are known for using their intelligence services to engage in espionage and collection of information using illegals. This method was established by the Soviet Union as early as in the 1920s, and it is still in use. Illegals are intelligence agents who operate in a different country, using a different identity than what they had at birth. Their identity might be taken from a deceased person, for example, preferably from a country that has an inadequate central national population registry or is lacking one altogether.

In October 2022, PST arrested a Brazilian national, and charged him with engaging in illegal intelligence activities in Norway. He is suspected of being a Russian illegal working for a Russian intelligence service. During his time in Norway , he worked under the guise of being a visiting researcher at the University of Tromsø (UiT). There, he participated in research communities and networks that have in-depth knowledge of the High North and Arctic politics, Norway's total defence, and hybrid warfare. These topics are of considerable interest to Russian intelligence services.

For many years, intelligence officers have taken advantage of conferences and seminars in Norway to identify and approach individuals who could potentially be future sources. The first contact will typically seem completely innocent and might involve no more than exchanging contact details. One typical approach would be for the intelligence officer to subsequently take contact by email to request a meeting, possibly to discuss a topic that falls within the expert purview of the contact. Following an assessment of their suitability, attempts will be made to recruit these contacts to be clandestine sources who will do work for the intelligence officer.

For several years, PST has observed that Norwegian research and educational institutions have been used by foreign states to identify potential sources. An attempt to recruit a Norwegian researcher

may seem innocent and legitimate to the person in question. One classic Chinese method is to invite relevant individuals to China. This may start with the researcher being invited to write a well-paid article for a Chinese think tank. Then perhaps the person in question would be invited to attend conferences in China, all expenses paid. The relationship-building process may then continue in different social contexts. In reality, the goal is to get the person to share sensitive information.

The recruitment of a source could do formidable harm to Norway. The source could provide unique information about what public undertakings, political institutions, companies or individuals are doing or planning to do. The person could be asked to find vulnerabilities that could be exploited by an intelligence service, e.g. regarding an enterprise's routines, security measures and digital infrastructure. A source could also be instructed to work covertly to influence decisions or to obtain information about other potential sources.

Foreign intelligence officers will also engage in other inappropriate activities in Norway. Among other things, they will engage in domestic travel to identify critical infrastructure and monitor Norwegian and Allied military activity in Norway. Intelligence officers may also use different technical tools, from a vehicle, for example, to collect technical data and monitor communications systems in Norway.

Foreign intelligence officers will engage in inappropriate activities in Norway. Among other things, they will engage in domestic travel to identify critical infrastructure and monitor Norwegian and Allied military activity in Norway

Unlikely that there will be Russian acts of sabotage in Norway

PST considers it **unlikely** that Russia will carry out any act of sabotage on Norwegian territory in 2023. If Russia's willingness to escalate the conflict with NATO and the West were to increase, however, acts of sabotage against strategic targets in Norway will become a more likely scenario. In the current security policy situation, PST considers the petroleum sector to be a particularly vulnerable target. However, other essential service functions could be relevant targets for sabotage, e.g. infrastructure connected with the power sector or the e-communication sector.

Any act of sabotage could be perpetrated physically or digitally, and will most likely be performed in a manner that makes it challenging to attribute the act to the actor behind it.

Several states will carry out influence operations

Several of the foreign intelligence services that operate in Norway have been tasked with influencing political decisions and public opinion in Norway. So far, PST is not aware of any widespread propaganda or disinformation campaigns that are targeting political processes in Norway. We must nevertheless be prepared for foreign intelligence services, especially those from Russia and China, to try to influence decision makers and the people of Norway in 2023.

Attempts to exert influence can take a variety of forms. For example, foreign intelligence services will use traditional media, alternative media and social media to disseminate their messages. These media can be used to spread disinformation, to initiate harassment campaigns, and to spread rumours and half-truths. In Norway, certain foreign intelligence officers will also work in a goal-oriented manner to get people with political influence to sway the outcome of individual cases.

For many years, Russia has demonstrated the desire and ability to carry out influence operations in Western countries. PST expects that once again this year, Russia will try to sway Norwegian decision makers and the people of Norway regarding matters of great importance to Russia. For instance, Russian authorities would have a great deal to gain by splitting Western unity in respect of further military support for Ukraine and financial sanctions against Russia.

In previous years, Russia has attempted to influence democratic processes and elections in several countries. So far, PST has not discovered any such attempts to exert influence in Norway.

China is expected to engage in influence activities aimed at individuals in Norway who openly criticise what China considers to be its core interests.

Norwegian enterprises will be exposed to covert procurement attempts

In 2023, Norwegian enterprises will be subject to covert and clandestine attempts to procure goods and technology, as well as attempts to perform illegal transfer of knowledge. The purpose will be to circumvent sanction regimes and export control regulations. States with which Norway has no security cooperation represent the greatest threat. Russia, China, Iran and Pakistan are expected to be the main actors involved in illegal

procurement activities for national programmes for weapons of mass destruction and other military development. Moreover, we expect that Syria and North Korea will try to obtain sensitive technology for their military weapons programmes.

Norwegian enterprises develop, manufacture and sell goods and technology that can have both civilian and military applications, i.e. a dual-use potential. Such civilian technology is coveted by foreign states for the development of weapons of mass destruction, means of delivery and other military systems. The export of sensitive goods, services and technologies is strictly regulated. For that reason, actors in countries of concern try to circumvent export control regulations using a variety of covert methods. Norwegian undertakings will thereby be subject to attempts to obtain illegal procurements of the above-mentioned goods and technologies. Procurement attempts cover a number of fields of technology, including sensor and detection technology, maritime technology, semiconductor technology, space and satellite technology, as well as drone and communication technology.

Examples of new emerging technologies:

- 3D printers
- Quantum computers
- Artificial intelligence
- Maritime autonomics
- Biotechnology
- Advanced surveillance technology

Emerging new technologies are sought after by state actors to ensure military capability, political influence and economic growth. These include goods and technologies that also have military applications. Norwegian enterprises that are leaders in emerging technologies are expected to be popular intelligence targets. In addition, fields of research at Norwegian universities and university colleges that are exploring emerging technologies are attractive targets. China is an especially relevant threat actor in this regard.

The Chinese authorities pursue an explicit strategy of exploiting private actors to ensure rapid military modernisation. The paramount objective is that civilian technology can readily be adopted by the military sector, provided it has dual-use value for the military.

State actors use a wide variety of methods to circumvent control mechanisms and secure access to technology and expertise from Norwegian enterprises. This includes the use of insiders, computer network operations and strategic acquisitions. Third-party states, including also other European countries, are often used to approach Norwegian enterprises. The means to accomplish this include using false documentation, complex corporate structures, nominee companies and front companies, as well as supply chains.

NTNU, Norwegian University of Science and Technology.
Photo: Gorm Kallestad/NTB

Iranian-German NTNU professor found guilty

In November 2022, a former Iranian-German professor at the Norwegian University of Science and Technology (NTNU) was found guilty of several breaches of Norway's Export Control Act, including hacking into systems containing data subject to export control, and sharing information about listed and militarily relevant materials with a group of visiting Iranian researchers, as well as giving them access to university laboratories at NTNU. The judgment was not yet legally binding when NTV went to press.

Several foreign states also employ different financial instruments to gain access to sensitive technology and information about conditions in Norway. Such activities include investments in companies and the acquisition of property. While this activity is not necessarily illegal, it may in certain cases be used to achieve many of the same goals as illegal intelligence activities.

A large proportion of the procurements and attempts at procurements in Norway go through middle men in different transit countries and shell companies. Norway may also be used as a transit country for deliveries. Actors engaged in clandestine and covert procurement activities aimed at western technology and equipment for Russia's military complex will to a greater extent than before use neighbouring countries that border on Russia, or countries that have not endorsed the sanctions regime, for their procurement activities. As one of the countries that has not endorsed the sanctions, China will be used as a transit country in 2023.

Western technology is the preferred alternative for Russia's civilian and military industry. The expanded sanctions regime and stricter export restrictions will nonetheless entail changes in Russia's covert procurement activities in 2023. Restrictions against Russian fishing vessels in Norwegian ports limit opportunities for covert procurements and breaches of the sanctions regime via the sea. We expect that actors that previously used the sea route from Norway to circumvent or breach the sanctions regime, will find alternative transport pipelines while nonetheless taking advantage of any freedom of action available to them in or through Norway, whether it involves transport by air, land or sea.

Research fields of particular interest to foreign states:

- Metallurgy
- Nanotechnology
- Cyber security
- Cryptography
- Robotics and autonomics
- Biotechnology
- Chemistry
- Micro-electro-mechanical systems (MEMS)
- Acoustics and nuclear physics

Norwegian research and educational institutions are vulnerable intelligence targets for illegal transfer of knowledge from several countries with which Norway does not have security cooperation. These research communities maintain a high international calibre, have good funding schemes and enjoy access to advanced laboratory facilities and other research infrastructure. Some countries have a strong interest in exploiting this access and the advantages of Norwegian universities and research institutions.

In particular, higher education personnel with links to foreign universities that are relevant for military capacity-building represent a threat in respect of the illegal transfer of knowledge.

In 2022, we registered a growing number of cases at Norwegian research and educational institutions in which the background, expertise and disciplines of visiting foreign researchers/professors could lead to Norwegian technology and expertise being used in ways that violate the export control regulations. This trend will continue in 2023.

Espionage against refugees and dissidents in Norway will continue

China, Iran and several other authoritarian states use their intelligence services to register, monitor and influence their own nationals who reside in Norway. Refugees and dissidents engaged in opposition activities are particularly vulnerable targets. The authorities' goal is to restrict, undermine or eliminate political opposition. These activities can have grave consequences for those involved, and pose a threat to democratic values in Norway.

For example, several states keep track of events, meetings and associations for exile communities in Norway. Certain countries use their official representative offices in Norway for this work, while other countries use visiting intelligence officers, organised criminals or individuals who report on diaspora communities.

Refugee espionage will take place in parallel in the digital domain, through everything from monitoring social media to hacking digital devices. Among other things, computer hacking can result in access to personal data, correspondence, plans and networks of contacts. Such data can be used either to threaten a person or as a gateway to espionage against members of the person's network.

Norwegian undertakings that administrate data about refugees may also be vulnerable targets. Several foreign intelligence services would have considerable interest in gaining access to relevant registers and databases, e.g. agencies involved in the administration of immigration, the police and the Norwegian Labour and Welfare Administration (NAV).

Certain states may be willing to go to great lengths to silence political adversaries living in exile. Several of them will be the targets of threats and harassment, either physical or digital. Dissidents may also be pressured into returning to their home countries, e.g. if family members still remaining in their country of origin are threatened or imprisoned. In recent years, we have seen examples of dissidents and those in opposition being murdered or subjected to attempted murder in several European countries. In 2021, a Norwegian-Iranian national was found guilty in Denmark for having colluded on plotting the murder of an Iranian in exile on behalf of the Iranian intelligence service.

Politically motivated violence – extremism

The terror threat level in Norway has returned to a moderate level. Islamic extremists and right-wing extremists are still expected to represent the greatest threats of terror against Norway. PST believes there is an **even chance** that both Islamic extremists and right-wing extremists will attempt to carry out terrorist acts in Norway in 2023.

It is **unlikely** that anti-government extremists will attempt to carry out terrorist acts in Norway in 2023. It is **highly unlikely** that left-wing extremists or extremists associated with the climate, the environment or nature conservation will try to carry out terrorist acts in Norway in 2023. Our assessment is nevertheless that issues involving the climate, the environment and nature conservation may be potential arenas for radicalisation.

The threat from Islamic extremism

PST believes there is an even chance that Islamic extremists will attempt to carry out terrorist acts in Norway in 2023. The threat of terror comes mainly from individuals who are inspired by the ideology and message of the terrorist organisations ISIL and al-Qaeda. These people can be motivated to act by statements or deeds perceived as insults or oppression of Muslims and the religion of Islam.

ISIL and al-Qaeda are the foremost examples of terrorist organisations that have a global or transnational Islamic extremist agenda. They contend that the West is at war with Islam, both in and outside the West. Western military intervention in Muslim countries and what they perceive as oppression and insults against Muslims in the West are used as justification for terrorist attacks. Since Western countries elect their own leaders, the entire population is held accountable and is therefore perceived as a legitimate target.

According to PST, the term **'extremism'** implies acceptance of the use of violence to achieve political, religious or ideological goals. While extremists accept the use of violence, they do not necessarily engage in violence themselves.

The term **'radicalisation'** refers to the process whereby an individual develops an attitude of acceptance for or a willingness to actively support or take part in violent acts to achieve political, religious or ideological goals.

Few Islamic extremists in Norway, but nonetheless serious acts of terrorism

Support for Islamic extremism in Norway is considered low at present. However, since much of today's radicalisation is expected to take place through encrypted digital platforms, it is challenging to detect. That being said, we have no physical openly extremist communities in Norway at the moment, like the ones we had some years ago. All the same, there is little to corroborate that known Islamic extremists have been de-radicalised. At times, Islamic extremists may be less active, but they could be re-motivated by relevant banner issues or events.

In June 2022, Norway fell victim to what PST considers an Islamic extremist terror attack.

PST has also averted several attacks by Islamic extremists in recent years. In some of these cases, the perpetrators were young, and the networks in which they operated were digital. The attack in June 2022 and the attacks that were averted indicate that the threat of terror in Norway is real.

Last year's attack could still inspire others who intend to commit terrorist acts. Even though direct inspiration is reduced over time, we see that past terrorist attacks may continue to inspire potential terrorists for many years.

Examples of averted terrorist attacks

In 2021, a young boy was arrested and found guilty of planning a terrorist attack in Norway. Through online networks sympathetic to ISIL, he had downloaded instructions for how to make poison and explosives. At the time he was arrested, he had tried to make nicotine poison.

In 2022, a Norwegian man in his 20s was found guilty by the Supreme Court for aiding and abetting acts of terrorism in other European countries. The man had played an active role in online networks sympathetic to ISIL.

Minister of Culture and Equality Anette Trettebergstuen (Labour Party) and Minister of Justice Emilie Enger Mehl (Centre Party) laying wreaths at the site of the shooting incident in downtown Oslo. Behind them are Prince Sverre Magnus, Crown Prince Haakon, Crown Princess Mette-Marit and Prime Minister Jonas Gahr Støre (Labour Party). Photo: Javad Parsa/NTB

Shooting incident in Oslo

On 25 June 2022, a man in his 40s opened fire on people outside of several bars in downtown Oslo. Two individuals lost their lives and more than 20 were injured. The accused has refused to be interrogated by the police. In autumn 2022, the Oslo Police District charged three additional individuals with aiding and abetting the terrorist attack. At the beginning of 2023, the case is still under investigation.

The networks in Europe are less active than they were some years ago. However, they are currently far larger than they were before ISIL was established. Online and physical contact between individuals in Norway and these communities could increase the danger of terrorism. This is because it brings them into contact with individuals and communities that radicalize others and are able to provide guidance regarding attacks.

Several released convicted terrorists in Norway and other European countries will continue to exert an adverse impact on the threat of terror. Islamic extremists convicted of terrorism have experience of and the capacity to carry out terror-related acts; many still have ideological beliefs, and several also have ties to international extremist communities. They can help radicalise or guide others to carry out terrorist attacks, while they themselves may also constitute a threat.

In 2023, we expect that Islamic extremists in Norway will have limited opportunities to participate in foreign fighter activities. This is because there are few areas in which terrorist groups accept foreign fighters. Those who go will have ties to the area or the group from earlier. Contact between Norwegian extremists and these groups will occasionally contribute to escalating the danger of terrorism.

ISIL and al-Qaeda are still expected to give priority to building up branches and affiliated groups in countries outside Western Europe in which they have gained a footing, rather than carrying out terrorist acts against the West. The exception is ISIL in Afghanistan, which seeks to strike targets in the West as a step in the group's work to undermine the Taliban as the ruling power, isolating them in the international arena. The organisations are also believed to be taking advantage of the opportunity to guide and inspire attacks in the West. ISIL and al-Qaeda will continue to encourage sympathisers to initiate and carry out attacks in the West.

Online propaganda is an important source of radicalisation and terrorist inspiration

Radicalisation to Islamic extremism will take place both through physical relationships and online networks.

On encrypted platforms, users will have opportunities to act and communicate anonymously. They can build relationships and develop trust among themselves, which is essential for terrorist planning and support. Extremists share propaganda and instructions for home-made explosives, and they can receive guidance on how to carry out a terrorist attack.

The propaganda made by ISIL and al-Qaeda sympathisers in the West is expected to become an increasingly more important part of the threat picture. Sympathiser-created propaganda includes new, recirculated and updated historical propaganda. Sympathisers tailor propaganda based on their own assessments and not necessarily based on group affiliation.

The propaganda is inserted into a western context of current interest to support and explain ideological questions and issues, and to encourage attacks in the West. The material is published in different European languages. Propaganda is often also designed for the purpose of capturing the attention of minors and young adults on platforms on which they are active. This type of propaganda will contribute to self-radicalisation as well as to radicalisation through relationships.

The distinction between digital and physical networks will often not be absolute. In the year ahead, we expect that radicalisation will also take place through physical relationships among friends and family, at school, in religious arenas and in prisons.

Perceived insults against Islam can motivate actions

Terrorist organisations have repeatedly encouraged attacks as revenge for what they perceive as insults against Islam. Matters experienced as provocations, desecrations or oppression of Muslims or the religion of Islam may contribute to radicalisation and, at worst, motivate terror-related activities in Norway. We have observed this in particular in countries such as Denmark, Sweden and France, where the production of and teaching about the Mohammed caricatures have led to several completed and averted terrorist attacks.

Matters experienced as provocations, desecrations or oppression of Muslims or the religion of Islam may contribute to radicalisation and, at worst, motivate terror-related activities in Norway

Burning and desecrating the Koran are also examples of incidents we see being experienced as offensive or provocative. In Norway, we expect that such events will also occur in 2023. Debates and events in Norway that are perceived as hampering the exercise of religion will also exacerbate the perception that the West is at war with Islam. When such incidents take place in Norway, they increase the likelihood of radicalisation and, in their ultimate consequence, the plotting of terrorist acts against Norway.

ISIL and al-Qaeda continue to be of the opinion that they are at war with the West. Among other things, the organisations encourage revenge as a reaction to the killing of several of their leaders in recent years. Western military involvement in Muslim countries will continue to motivate acts of terrorism and foreign fighter activities.

All the attention devoted to the topics of insults and how the West is waging war could motivate some individuals to carry out terrorist acts. Experience has shown that retaliatory actions in response to incidents experienced as provocative or offensive can occur a long time after the incident per se.

Less guidance from the terrorist organisations could make more targets relevant

In 2023, any Islamic extremist act of terrorism in Norway will probably be committed by a lone individual. It is assumed that the perpetrator would have been in contact with other extremists in the run-up to the act, either online or in person.

ISIL has inspired a far higher number of attacks in the West than al-Qaeda. ISIL's portrayal of the enemy implies that everyone except ISIL sympathisers themselves are legitimate targets in the West.

The most relevant targets for Islamic extremists will continue to be civilian crowds, institutions or individuals perceived as having insulted the religion of Islam, and uniformed police and military personnel in public areas. Religious meeting places are also deemed likely targets. In addition, different types of infrastructure may also be targets.

While individuals and institutions perceived as violating ISIL's moral code have rarely been the targets of attacks in the West so far, they are considered legitimate targets. In the wake of the terrorist attack in Oslo last year, LGBTQ+ meeting places have become more likely targets. ISIL's stereotype of the enemy encompasses everyone who does not share their interpretation of Islam. However, attacks against those who practice other forms of Islam have rarely occurred in the West to date.

Since the propaganda is being produced by sympathisers to an ever-greater extent , it is expected that terrorists will increasingly be inspired by local factors, as well as by guidance provided by ISIL and al-Qaeda centrally. For that reason, there may be a greater number of relevant targets than before, including targets that have been less common in the West thus far.

As regards means of attack, this is discussed in a separate sub-chapter (page 35).

The threat from right-wing extremists

PST believes there is an even chance that right-wing extremists will attempt to carry out terrorist acts in Norway in 2023. The threat will largely be represented by the young adults and minors who are radicalised through right-wing extremist digital arenas. Experience from Norway and other countries indicates that some of them may develop an intention to engage in terrorism.

Extreme right-wing ideology has the idea of ethnic nationalism as its common denominator. The state and the people are to be a single unit, based on the notion of a common 'race' or shared cultural characteristics. Groups that do not belong to this community are considered a threat. Further, right-wing extremists are anti-democratic, viewing groups of people as fundamentally different and not of equal value. Conspiracy theories are also of paramount importance to right-wing extremists.

The greatest challenge is propaganda on digital arenas

Radicalisation to right-wing extremism continues. Right-wing extremist digital arenas will continue to pave the way for radicalisation to right-wing extremism. They use platforms that either allow or fail to delete right-wing extremist material.

The ideology of glorifying violence is presented with humour, through memes and references to gaming and pop culture. Even though most people who participate in such fora are primarily driven by the desire to push limits and to have fun, repeated exposure to such ideas can normalise attitudes that glorify violence. Further, the algorithms used for online searches and social media may lead people to more extreme content. One-sided bias based on the messages conveyed in such fora may contribute to radicalisation.

The majority of those who are radicalised on digital fora are expected to be young adults and minors. PST has found that several of them struggle with loneliness and mental health issues. The sense of belonging imparted by the digital arenas is often instrumental in ensuring that participants remain active in such networks.

Radicalisation will continue to take place face to face, primarily through right-wing extremists who try to radicalise people close to them and acquaintances. We do not expect physical right-wing extremist groups in Norway to have the ability to radicalise and recruit others on a large scale.

Telegram Messenger, Instant Messenger App.
Photo: Valentin Wolf imageBROKER/NTB

Online extremism

Individuals can be exposed to extremist propaganda on open platforms like TikTok, Instagram, Telegram and different gaming platforms. The message is adapted to avoid being censored on these platforms. The posts often contain links to encrypted platforms where the content may cross the line and glorify violence. Telegram is used frequently because it offers a stable platform and features little censorship. Telegram consists of channels for publishing propaganda for a broad audience in addition to channels for user-driven chat groups with fewer members.

Accelerationism and earlier terrorist acts can motivate terror

The threat of terror primarily comes from right-wing extremists who participate in online accelerationist networks. Accelerationists claim that they are trying to save 'the white race' by accelerating what they believe to be an imminent racial war while whites still have a demographic majority in the West. This racial war is being accelerated inter alia through the escalation of conflicts, polarisation and other factors that could lead to a faster collapse of society. Terrorism is recognised as a useful tool for destabilising society and igniting racial wars. Participants in the networks are urged to commit acts of violence and terrorism, and it is emphasised that time is of the essence. Such networks have persuaded several right-wing extremists to plot acts of terrorism in the West in recent years.

Although few right-wing extremist terrorist attacks were carried out in 2022, among right-wing extremists in particular, we see that attacks committed several years ago are still sources of inspiration. Multiple terrorist actors have published manifestos in connection with their acts of terrorism. There have also been several instances in which terrorists have tried to film their attacks. Attacks are filmed and manifestos are published to inspire and encourage others to commit similar acts. In two of the attacks last year, the perpetrators had published manifestos declaring that they had been inspired by terrorists like Anders Behring Breivik and Brenton Tarrant.

Non-western immigration is a factor that influences right-wing extremists because they see it as support for their perception of the 'White race' as being threatened. During surges in non-Western immigration, we see that this topic attracts attention and may contribute to radicalisation. Lately, there has been little non-Western immigration to Norway. Most immigration has come from Western countries. If there were to be an upswing in immigration from non-Western countries in future, we would expect it to result in more radicalisation to right-wing extremism.

Certain Norwegians who are affiliated with right-wing extremism chose to participate in the war in Ukraine in 2022, despite the fact that the war has no clear ideological applicability for right-wing extremists in Norway. None of the combatant groups in the war have terrorist attacks outside of Ukraine as a strategic objective. However, it is expected that right-wing extremists who choose to take part in the war could enhance their weapons capability, lower their threshold for violence, expand their extremist networks, and get traumas of war.

Persistent hatred of minorities and the Norwegian authorities

Any extreme right-wing terrorist acts in Norway will most likely be committed by a lone individual, and will be aimed at targets that fit right-wing extremists' stereotype of the enemy. The form of attack could be an attempt to carry out a mass casualty attack or a targeted assassination of an individual.

The stereotype of the enemy held by right-wing extremists in Norway will still encompass minorities and the Norwegian authorities because the extremists believe that they pose threats to the survival of the nation, the culture or the 'race'. Examples of potential targets include Muslims, individuals with a non-western appearance, Jews, politicians, traditional media and members of the LGBTQ+ community.

The stereotype of the enemy held by right-wing extremists in Norway will encompass minorities in particular and the Norwegian authorities because the extremists believe that they pose threats to the survival of the nation, the culture or the 'race'

There are indications that members of the LGBTQ+ community will assume a more vital role in right-wing extremists' stereotypes of the enemy in the years ahead. The reasons are the occasional strong focus on members of the LGBTQ+ community in the media, and expressions of support for violence against LGBTQ+ individuals among Norway's right-wing extremists, as well as the multiple terrorist acts carried out against LGBTQ+ meeting places in the West in 2022.

In recent years, certain right-wing extremist plans of attack in Europe have targeted lower and upper secondary schools. Since the everyday routines of young adults and minors largely revolve around school, schools may be an easily accessible target for young right-wing extremists' plotting of attacks. In addition, several previous school shooters, especially the perpetrators behind the Columbine massacre, have been celebrated in the propaganda.

The police have been referred to as enemies in accelerationist propaganda and in certain manifestos, chiefly because they are considered protectors of the existing 'establishment'. This may influence future right-wing extremist terrorist actors to also consider the police as targets for terrorist attacks.

Means of attack that can be adopted by Islamic extremists and right-wing extremists

Since there are many similarities in terrorists' choices of means of attack, these are dealt with collectively.

The choice of means of attack is influenced by the actors' motives, skills, networks and how available the means of attack are. Averted attacks in the West indicate that an exceptional number of potential terrorists would like to use firearms and/or explosives, but that they often end up using means of attack that are more readily accessible for them. For example, a threat actor with ties to criminal networks may find it easier to obtain firearms than an actor without such ties. A potential terrorist whose family hunts or who hunts himself may have access to legal weapons.

Simple means of attack

In recent years, many attacks have been carried out using simple means. The term 'simple means of attack' refers to objects that are in daily use, readily accessible, and call for little or no previous knowledge. Examples include axes, knives, machetes, hammers or vehicles. A vehicular attack can lead to a great many fatalities, even though it is a simple means of attack.

Simple means of attack are expected to be used by both Islamic extremists and right-wing extremists, often in combination with firearms and/or explosives.

Other means of attack/firearms and explosives

While firearms may also be readily available to certain actors and groups, they usually call for more expertise than what vehicles require, for example. Firearms are invariably attractive as a means of attack and will be used by threat actors if they have access to them because of the potential scope of the damage they can do. Firearms used for terrorist attacks can be procured by either legal or illegal means. Deactivated weapons that have had their functionality restored can also be used.

Historically speaking, improvised explosive devices (IEDs) are the weapon of choice for completed and averted terrorist attacks. It must therefore be expected that threat actors will try to develop and use IEDs if they have access to components and possess the expertise needed to make them. If attempts are made to use IEDs, they will most likely have a relatively simple structure and mode of operation, and they will be incendiary devices, e.g. Molotov cocktails.

In many Islamic extremist terror attacks, the perpetrators themselves wanted to be killed by the police while committing the act. Fake bomb belts or the like have been used by Islamic extremists on several occasions to provoke a lethal response from the police. Such devices can also be used to stall for time, increasing the likelihood of doing greater damage.

The threat from anti-government extremists

PST considers it unlikely that anti-government extremists will try to commit acts of terrorism in Norway in 2023. Anti-government ideas, especially conspiracy theories about the 'deep state' and the notion that the State is not legitimate, will continue to lead to radicalisation.

Anti-government extremism is a general description of ideas and conspiracy-like theories that involve an element of violence. These ideas are largely anchored in conspiracy theories that contend that everything is related and nothing happens by chance. These theories refer to the enemy as something so evil and so dangerous that resistance and violence will eventually be considered necessary.

Distrust of the authorities is a unifying factor. The different anti-government theories overlap to a great extent, and we see that conspiracy theories are constantly taking on new forms and adapting to current events and global development trends. A perpetual anti-government mentality includes the notion that the State does not have a legitimate platform for its exercise of power. Violence can be considered legitimate if someone is convinced that legislation and regulations violate individual citizens' civil liberties and sovereignty.

Violence can be considered legitimate if someone is convinced that legislation and regulations violate individual citizens' civil liberties and sovereignty

Conspiracy theories offer easy explanations in times of uncertainty

The rhetoric touted in anti-government fora indicates that some people have a narrow, one-sided perception of reality that offers no latitude for alternative explanations. Those who hold opposing views are portrayed as though they are not truthful, and like they have a hidden agenda. This is a means of demonising individuals whose opinions differ from their own. This is often a key step in the process of radicalisation. In its ultimate consequence, anti-government and conspiracy theories may be perceived as justification for the use of violence and undemocratic means.

Less focus on Covid-19 has led to a reduction in incidents of anti-government violence in the West. An upsurge in the Covid-19 pandemic, for example, or other events that support anti-government conspiratorial ideas, could elevate the threat in the year ahead.

Economic downturns and the tense political situation in Europe are examples of events that engender unrest and fear among the members of the general public. This could reinforce the need for simple explanations and provide fertile ground for conspiracy theories. This is especially relevant among individuals who are already inclined to believe conspiracy theories.

'The Deep State'

The notion that authorities and public figures conspire with, or work for, a secret network or a hidden elite that seeks world domination.

Disinformation campaigns on the part of state actors will continue to exert influence and thus to maintain anti-government convictions that could radicalise individuals in Norway. There will continue to be some overlapping between anti-government and right-wing extremist mentalities. The threat relating to politically motivated violence in Norway could thereby become more complex.

Infrastructure and individuals that fit the stereotype of the enemy are the most vulnerable targets

For the time being, it is unlikely that anti-government extremists will carry out a terrorist attack. Targets associated with core anti-government issues and that play a key role in current conspiracy theories will be the most relevant targets for any potential attack. Critical infrastructure and dignitaries are examples of this. There are several cases in which dignitaries or others who are perceived as representatives of the establishment have been made the targets of planned acts of violence in the West.

The threat from left-wing extremism

PST considers it highly unlikely that left-wing extremists will try to carry out acts of terrorism in Norway in 2023. The left-wing extremist groups in Norway are expected to remain small.

Left-wing extremists' ideological convictions will continue to be grounded in various forms of Communism, anarchism and anti-fascism that glorify violence.

The fight against right-wing extremism – still a common core issue

The fight against right-wing extremism will continue to be the most unifying issue for these groups in Norway. We expect that certain left-wing extremists will commit acts of violence against individuals they believe to be right-wing extremists.

Left-wing extremists will primarily engage in activities that can be considered disturbances of the peace, making them the responsibility of the ordinary police.

Extremism associated with the climate, the environment and nature conservation

PST considers it highly unlikely that individuals associated with the climate, the environment or nature conservation will try to carry out terrorist acts in Norway in 2023. However, we expect to see an increase in activities involving the use of illegal acts such as vandalism and disturbance of the peace. Eventually, this could help radicalise individuals.

This topic has the potential to radicalise

We expect that activists in Norway motivated by the climate, the environment and nature conservation will primarily use non-violent methods to promote their causes. Political influence will mainly take place through democratic channels.

However, some will also resort to illegal means, such as vandalism and disturbance of the peace, to attract the attention of politicians and others. These are the responsibility of the ordinary police.

Nonetheless, our assessment is that issues involving the climate, the environment and nature conservation do entail a potential for radicalisation. This refers in particular to climate-related challenges, which may engender existential fears among certain individuals who feel that time is of the essence when it comes to finding solutions. If they also happen to be of the opinion that politicians are not doing enough to solve climate-related challenges, it may be easier for them to accept the use of violent means.

Further, individual issues related to the climate and nature conservation may create quite a sensation, not least locally, leading some individuals to develop an intention to resort to violence to support or achieve political objectives.

Violence is expected primarily to target infrastructure and property considered to be sources of emissions that exacerbate environmental challenges.

PHOTO: 2016 STORTINGET/PETER MYDSKE

Threats to dignitaries

PST considers it **unlikely** that dignitaries will be victims of serious acts of violence in Norway in 2023. However, demanding economic times could escalate threat activity. Threats and harassment against politicians constitute a serious threat against democracy since the collective strain impacting multiple dignitaries and politicians could lead some of them to withdraw from public discourse or to refrain from running for office.

Dignitaries are defined as members of the Royal family, the Government, the Supreme Court and members of parliament. However, the NTV also covers certain politicians who do not fit the definition of dignitaries, but who are in a vulnerable position by virtue of being politicians.

Most of the people who threaten dignitaries are driven by personal motives. The threats are largely associated with individual issues. What is more, many threat actors have mental health issues. Very few of the people who make threats genuinely intend to engage in violence.

Threats against dignitaries can also come from extremists. PST's assessment, however, is that targets other than dignitaries are more prominent in extremists' stereotype of the enemy.

Challenging economic times could escalate threat activity

Deteriorating financial circumstances due to price hikes, higher interest rates and inflation have exacerbated many Norwegians' feeling of being powerless. In some cases, growing frustration is aimed at the authorities. This is generally expressed through slander and harassment against politicians on social media and online platforms.

If the authorities implement initiatives that are perceived as particularly invasive in respect of individuals' privacy, this could generate further threat activity and, in certain cases, confrontations in the public sphere.

Threats and harassment against politicians constitute a serious challenge against democracy

Serious incidents over the past year raise the likelihood of threats against dignitaries. The murder of Japan's former prime minister Shinzo Abe and the murder of psychiatrist Ing-Marie Wieselgren during Almedal Week in Sweden are examples of this. The leader of the Swedish Centre Party, Annie Lööf, is said to have been the original target of the man who killed Wieselgren. She subsequently chose to withdraw as party leader, not least as a result of the hate rhetoric to which she was subjected as a politician.

The collective strain on several Norwegian dignitaries and other politicians has become so great that some of them are withdrawing from public discourse, refraining from running for office or leaving politics. This presents a serious challenge to Norwegian democracy. One of the assumptions underlying our democracy is that all Norwegian citizens should feel safe and secure when taking part in politics, at every level.

Threats and harassment against politicians constitute a serious challenge to democracy, and could lead some to withdraw from public discourse or to refrain from running for office

In connection with the municipal and county council elections in autumn 2023, there is reason to expect more incidents of slander, harassment and threats against local politicians and young politicians. If this impacts their political participation, it also represents a serious challenge to democracy.

The intelligence threat against Norwegian dignitaries

The war in Ukraine and the tense security policy situation between the West and Russia have consequences on the intelligence threat in Norway. Several foreign states, especially Russia, will continue to pursue the goal of gathering intelligence about Norwegian political processes that could have a bearing on their interests. This implies that a number of Norwegian politicians, and people who work in the system surrounding them, may be targets for foreign states' intelligence and influence activities in Norway in 2023.

Reference is made to the chapter "The threat from foreign intelligence services in Norway" for further information about the intelligence threat in 2023.

Report tips to us

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

If you have any tips, contact us at:

PST.no/tips-oss

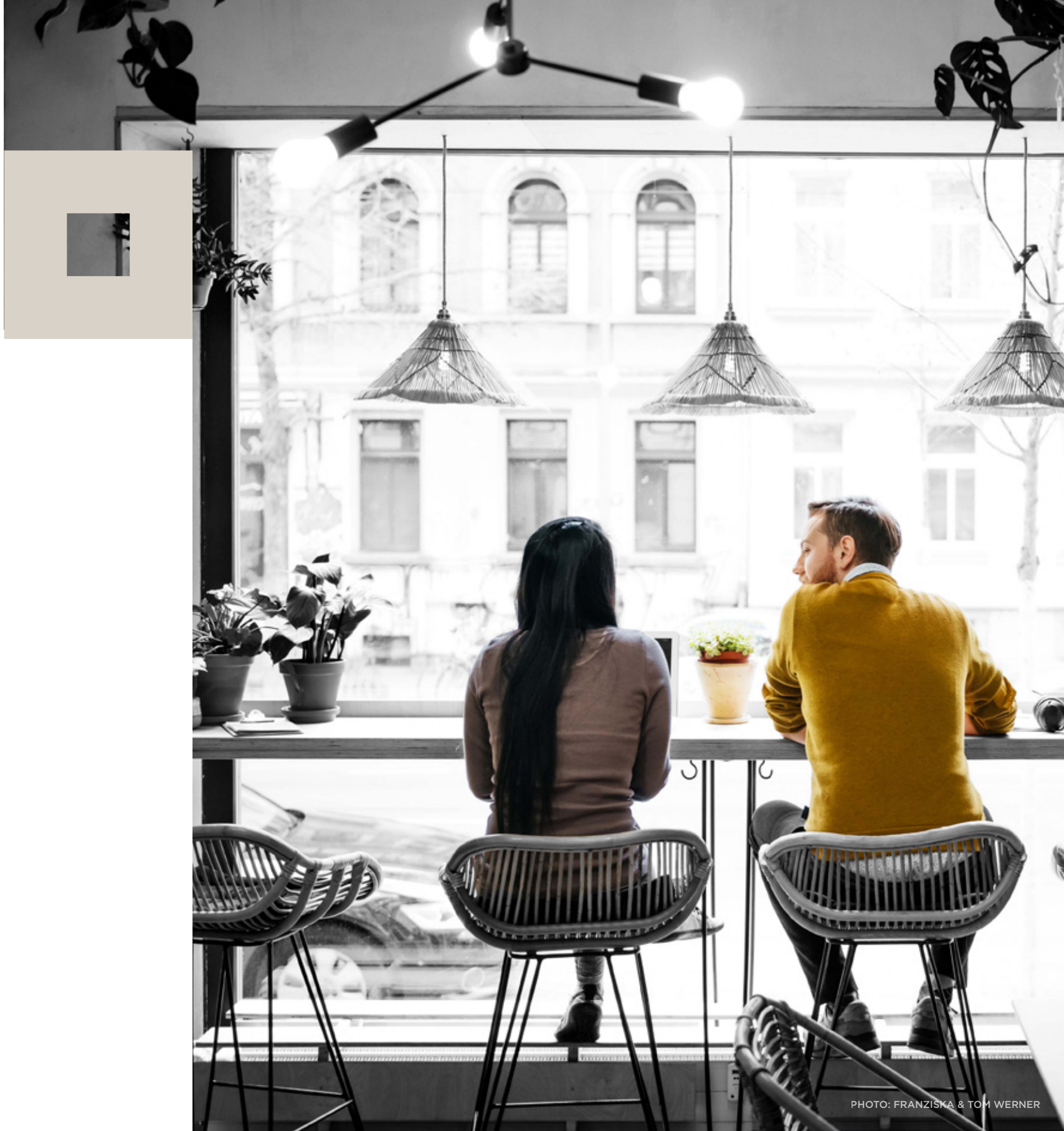


PHOTO: FRANZISKA & TOM WERNER

DESIGN: KNOWIT / COVER PHOTO: ANTON PETRUS/GETTY IMAGES

PST
POLITIETS SIKKERHETSTJENESTE

The Police Security Service

pst.no