Norwegian Ministry
of Justice and Public Security

Meld. St. 9 (2022–2023) Report to the Storting (white paper)

National control and cyber resilience to safeguard national security

As open as possible, as secure as necessary

Meld. St. 9 (2022–2023) Report to the Storting (white paper)

National control and cyber resilience to safeguard national security

As open as possible, as secure as necessary

Translation from Norwegian. For information only.

Contents

National control and cyber resilience to safeguard national security

As open as possible, as secure as necessary

Meld. St. 9 (2022–2023) Report to the Storting (white paper)

Recommendation of the Ministry of Justice and Public Security 9 December 2022, approved by the Council of State on the same day.
(Støre Government)

1 Summary

The current security situation requires powerful measures to safeguard national security. Russia's attack on neighbouring Ukraine on 24 February 2022 has created an entirely new situation in Europe. Hybrid threats affect society broadly, and safeguarding national security is increasingly demanding because today's risk and threat picture is complex and affects all areas of society.

In recent years, there have been several examples showing the importance of both regulatory instruments and long-term perspectives in order to ensure national control and national security. The sale of the Norwegian-registered company Bergen Engines AS in 2021 is one such example. The company was a manufacturer and supplier of motors and generators to both the civilian and defence sectors in Norway and other allied countries. One of the potential buyers was a Russian-controlled company. After considerable political and media attention, and an assessment of the sale in relation to the Security Act, the transaction was stopped. This case is an example of how important it is that the state has the toolbox to uncover and intervene when necessary. In 2014, it was suggested that the state sell some of its shares in Kongsberg Gruppen, an important actor in defence production. The case triggered political debate, and the sale was not completed.

These cases illustrate the importance of national control as a means of safeguarding national security. The government believes that the state must take an active role in ensuring national control, and safeguarding Norwegian security. This report to the Storting expresses this.

Concession legislation has a long history in Norway. In addition to securing ownership and using conditions that benefit society the most, it also contributes to settlement and long-term and good management of agricultural resources. The government believes that this legislation is necessary in a long-term perspective.

A short time ago, the state purchased Meraker Brug. With an area of approximately 300,000 acres, this was one of the country's largest privately-owned properties. The property makes up 90% of the land in Meråker municipality. Ensuring national ownership of certain properties is an important means of ensuring national control.

One of the government's most important tasks is to safeguard national security. In this report, the government will clarify strategic direction, priorities and measures for safeguarding national and cyber security in selected areas. The government's strategic direction is highlighted below. The measures mentioned in this report supports the strategic direction.

The government will use national ownership and control to strengthen national security

We face a more challenging risk and threat environment and we are challenged by states with security policy ambitions that do not correspond with our own national security interests. The government will strengthen efforts to increase society's collective resilience. National control in areas that are strategically important for national security is a vital part of this. National ownership is one of several means of achieving this. The government wants to increase national control in order to contribute to increased knowledge, predictability and trust, as a basis for value creation and future investments in Norway. Means of achieving various degrees of national control must be adapted and balanced against other important societal considerations in a democratic state. These can be considerations such as a free and open society, or knowledge, business, trade, economic and national security considerations. Risk acceptance will be a part of these assessments. The principle 'as open as possible, as secure as necessary' emphasises these balances.

The government will facilitate an increased overview of assets that are strategically important for national security

A fundamental prerequisite for safeguarding national security is that the authorities have an overview of which assets and companies are important for national security. The Security Act has its own methodology for mapping assets. The mapping of fundamental national functions gives ministries an overview of companies and assets that have decisive and significant importance to the state's ability to safeguard national security interests. The companies or assets that are of decisive importance are subject to the Security Act with requirements to implement preventive security measures. Mapping is complex, and shows extensive interdependencies between companies within and across sectors, and also shows that dependencies change relatively often. This is especially relevant to digital information systems and infrastructures. Targeted and effective preventive security work requires prioritising the work of updating and improving the mapping done in compliance with the provisions of the Security Act. In this work, preventive measures also have to be assessed and prioritised based on how costly and effective they will be. The government will prioritise the work of revising and updating overviews in all sectors of society.

The government will also assess how to gain a better overview of assets not covered by the Security Act, but which may still be significant to our national security. This can be physical, digital or other assets. At the same time, an overview of assets must be seen in connection with the risk and threat picture, in order to understand our own vulnerabilities and to be able to safeguard our own security. In this report, the government will present measures to further strengthen the overview of assets of importance to national security. A good overview of our assets allows the authorities to better assess relevant means of safeguarding national security, including through preventive security measures based on the Security Act, the use of other relevant legislation and national ownership.

The government will actively use regulation as a means to safeguard national security

The government sees it as important to ensure that the Security Act is adapted to the current risk and threat picture at all times, and will therefore put forward proposals for adjustments to the Act when necessary. The government also sees the need to review other relevant legislation to ensure that considerations of national security are included as an assessment criterion, where relevant. Furthermore, the government sees a need to strengthen the legislation in certain areas in order to safeguard national security, including in relation to cyber security and data centres. The government is considering putting forward a proposal for an act on cyber security to make companies accountable and ensure the implementation of national advice and recommendations. The government has also appointed a public committee to assess the need for regulations or a scheme to screen economic activity related to companies that are not subject to the Security Act.

The government will strengthen society's resilience and robustness through increased expertise and knowledge about national security and cyber resilience

Expertise and knowledge of risks, threats, vulnerabilities and effective countermeasures are a prerequisite for being able to protect our assets against unwanted incidents. The government will highlight society's need for expertise and facilitate long-term research of importance to national

security. The government will make sure that individuals, companies and authorities are aware of the security challenges and have the necessary knowledge of how they can meet them effectively. The measures presented in this report will contribute to increase the expertise and knowledge level in society.

2 Introduction

In this white paper, the government will clarify strategic direction, priorities and measures for safeguarding national security in selected areas. Special attention is given to strategically important companies, natural resources, infrastructures and technologies. The government will also highlight selected areas within cyber security. This report is delimited against the broad public security and preparedness perspective.

In this report, the government wants to reinforce efforts to strengthen society's collective resilience. Knowledge, expertise and awareness on all levels of society are essential to achieve this. It is about understanding risk and threat, why national security is important, how it affects the individual, and which relevant measures should be implemented. In Norway, we have a high degree of trust – for each other, and for the authorities. A high degree of trust makes us more resistant to disinformation operations from other states, which may aim to create political and social unrest. However, this trust can also be under pressure in Norway, and the level of trust can vary between population groups. We must therefore strengthen the entire population's understanding, knowledge and awareness of both threats and measures. If the state's actions are not understandable and predictable, and the population has insufficient knowledge, this can undermine trust in the authorities over time. In an open society like Norway, we must consider that various types of legal activity can be misused, including for intelligence purposes. Different considerations will need to be assessed and taken into account, and there will always be a residual risk.

In addition to initiation, developing and implementing measures through its own means, the Ministry of Justice and Public Security has a coordinating and driving role for preventive national security and cyber security on the civilian side. This means that the Ministry of Justice and Public Security must, among other things, design the government's policy, including establishing national requirements and recommendations, across various areas of society. The Ministry of Defence has overall responsibility for preventive national security and cyber security in the defence sector.

Below is a description of a more challenging risk and threat environment, as well as what is included in the concepts of national control and cyber security. Chapter 3 discusses the means for strengthening national control and building cyber resilience. National control of assets of importance to national security are discussed in Chapter 4. Chapter 5 discusses the economic and administrative consequences.

2.1 A more challenging risk and threat environment

We face a more challenging risk and threat environment and are challenged by states with security policy ambitions that do not correspond with our own national security interests. Increased willingness to confront non-Western states, Russian use of military power and energy as a weapon are examples of this. The invasion of Ukraine has created lasting changes in the relationship between Russia and Western countries.

Increased globalisation, great power rivalry and constant changes in the security situation greatly affect the national threat picture and present us with security challenges. The High North's increased strategic significance and our role as an energy supplier mean that Norway is particularly exposed to intelligence and sabotage activities, and other unwanted activity. Climate changes also affect national security over time. Furthermore, it appears from the Perspective Report that the annual budgetary scope for manoeuvre will be reduced in the coming decade, compared with the previous one.[1]

Traditional distinctions between peace, crisis and armed conflict have become blurred. State actors such as Russia and China often carry out activities that may be legal to promote their own strategic goals. This is part of the normal situation, but this activity can also harm our national

[1] Meld. St. 14 (2020–2021) *Perspective Report 2021.*

Figure 2.1 We are facing a more challenging risk and threat environment

Photo: Norwegian National Security Authority

security. We must take account of the fact that some states try to affect political decisions, public opinion and debate in Norway. Diplomatic, informational, military, economic, financial, intelligence and legal means from individual states can, individually or in combination, constitute hybrid threats directed at Norway. In recent years, the threats relating to foreign investments and acquisitions that can be used to access strategically important assets such as technologies and resources have been more visible.

More and more assets of importance to national security are managed and processed in the digital domain. Digitalisation and technology development bring about increased efficiency and renewal, but at the same time introduce new vulnerabilities, dependencies and concentration risks. This can be exploited by threat actors and must thus be handled. The rapid pace of development and the changes in the security policy situation make it increasingly difficult for companies to maintain a proper level of security throughout the entire spectrum of conflict.

Box 2.1 Hybrid threats

Hybrid threats are a term for strategies for competition and confrontation below the threshold of armed conflict, which can combine diplomatic, informational, military, economic, financial, intelligence and legal means to achieve strategic objectives. Hybrid threats can be found in security policy grey-zones with the aim of creating discord and destabilisation. The use of means can be widely distributed and can combine open, covert and hidden methods. The use of means can be aimed at specific activities or situations, or be designed more long-term to create doubt, undermine trust and thereby weaken our democratic values. Hybrid threats are, by their nature, complex, and challenge early warning, a common situational awareness as well as effective and coordinated handling.

Figure 2.2 Digitalisation introduces new vulnerabilities and risks.

Photo: Norwegian National Security Authority

2.2 National control and cyber security

National control

National control is not a goal in itself, but one of many means for safeguarding national security.

National control of companies and assets of importance to national security can be achieved through

- regulations in law, for example the Security Act and its regulations, which impose obligations on companies.
- complete or partial state ownership.
- complete or partial national ownership, which includes enterprises beyond the state, such as municipalities and county municipalities, in addition to private Norwegian ownership.
- sufficient overview by the authorities of assets that are important for national security, whether they are subject to the Security Act or not.
- public-private, civil-military and international cooperation.
- advice and guidance to actors who own assets of importance to national security.
- different combinations of the above.

The government will strengthen its national control through more active use of available means. The government will prioritise improving the overview of companies and assets which are of

Box 2.2 National security

National security, as the phrase is used in this report, is the state's ability to safeguard national security interests. Norway's national security interests are defined in Section 1-5 of the Security Act as the country's sovereignty, territorial integrity, and democratic system of government, and overall security political interests related to; a) the activities, security and freedom of action of the highest state bodies, b) defence, security and preparedness, c) relationships with other states and international organisations, d) economic stability and freedom of action and e) the basic functionality of society and the basic security of the population.

importance to national security, use means such as relevant legislation and national ownership, and increase society's level of knowledge of risks, threat actors and preventive security.

National control as a means must be used in such a way that it promotes predictability and trust, and does not lead to unnecessary restrictions on value creation and foreign investments in Norway, or on Norwegian market access in foreign markets. National control which limits foreign activity in Norway can bring about political and economic costs for Norwegian society, and can affect foreign and trade policy considerations and cooperation with other countries. It is therefore important to have an approach that balances security and control against other important societal considerations, such as a free and open society or the need to provide companies with the best possible framework conditions and predictability. Cost-benefit and risk acceptance will be part of these assessments. The Security Act's purpose statement emphasises that 'security measures [must be] implemented in accordance with the fundamental legal principles and values of a democratic society.'

Cyber security

Digitalisation contributes to better services, more efficient use of resources and increased productivity in society. Digitalisation also brings the world closer together. The downside of digitalisation is that we become more vulnerable. Our society is dependent on critical societal functions working. This in turn requires that digital systems that support these critical societal functions work everywhere and at all times. But digital systems are becoming increasingly complex, and the rate of change is high. With a more challenging threat environment and an increased number of cyber attacks, preventive security work is all the more important. The government therefore wants to strengthen society's collective resilience against cyber threats.

Cyber security has gone from being a technical subject to become a global strategic issue.

Box 2.3 'The Bergen Engines case'

On 15th December 2020, Rolls-Royce plc alerted Norwegian authorities that they would start the process of selling the Norwegian-registered company, Bergen Engines AS. Transmashholding Group (TMH Group) was one of the potential buyers, and the purchase was planned to be carried out by TMH International AG, a Swiss-registered company that is 100% owned by Russian-registered TMH Group. On 4th February 2021, Rolls-Royce announced the signing of an agreement with TMH regarding the planned sale of Bergen Engines AS.

Bergen Engines AS is a manufacturer and supplier of engines and generators to both the civilian and defence sectors in Norway and other allied countries, including the USA and the Netherlands. A sale of Bergen Engines AS would involve the transfer of the company's technology, expertise, material, real property, customer portfolio and service and maintenance agreements. On the basis of the information about the transaction process, the Norwegian authorities started work to map all conditions related to the possible sale of Bergen Engines AS.

On 8th March 2021, Rolls-Royce was alerted by the National Security Authority that Norwegian authorities were considering whether the transaction should be stopped in accordance with the Security Act. Furthermore, the Norwegian authorities assumed that any transfer of knowledge in connection with due diligence and related activity was stopped until this had been clarified. On 12th March 2021, Rolls-Royce confirmed that both the transaction process and all knowledge transfer to TMH had been temporarily halted pending a final decision from Norwegian authorities. TMH confirmed the same on 15th March 2021.

On 26th March 2021, the Norwegian authorities decided on the basis of the first paragraph of Section 2-5 of the Security Act that Rolls-Royce plc and their subsidiaries were required to stop the sale of the shares in the Norwegian company Bergen Engines AS to TMH companies. The decision halted any transfer of shares, assets, property, industrial or technological information or other rights in Bergen Engines AS to TMH. Bergen Engines AS was later sold to the British company Langley Holdings.

Figure 2.3 NSM has recorded a large increase in the number of cyber attacks.

Photo: Shutterstock

Cyber security includes both technical and administrative security measures, and includes the protection of systems and the information in them. Cyber security is therefore about protecting 'everything' that is vulnerable because it is connected to or otherwise depends on information and communication technology.

On a strategic level, cyber security concerns security policy, where challenges must be largely solved through international, civil-military and public-private cooperation. The broad use of hybrid tools by certain states which can conflict with our national security interests highlights the significance of cyber security being an integral part of other security work.

The war in Ukraine and the gas pipeline explosions in the Baltic Sea are stark reminders of the importance of security work, including cyber security. As a result of these incidents, preparedness against cyber attacks, among other things, that could affect the petroleum sector or other critical companies has increased. Power and electronic communication are examples of infrastructures where cyber resilience is significant. When it comes to cyber security work, it is especially important to identify dependencies, work broadly with security and see measures in context. Strategically important infrastructure is crucial in this context and is discussed in more detail in Chapter 4.3.

Society's collective cyber security depends on the preventive work of each and every company. Company leaders are responsible for their company's ability to prevent and handle incidents. In line with the Ministry of Justice and Public Security's coordination responsibility for cyber security on the civilian side, the authorities provide national advice and recommendations and make resources available as far as possible when a serious incident occurs. The Norwegian National Security Authority (NSM) is the national agency for cyber security. The National Cyber Security Centre (NCSC) is a part of the NSM and contributes to protecting fundamental national functions, public administration and business from cyber attacks. The Norwegian Police Security Service (PST) and the police are also key actors, and the National Cybercrime Centre (NC3) at The National Criminal Investigation Service (Kripos) contributes to national and international work. The Norwegian Intelligence Service contributes in preventing, uncovering and countering foreign threats against Norway and Norwegian interests, including in the digital domain.

In recent years, a good cyber security knowledge base has been established, so that both companies and authorities are better able to implement the right measures. However, the NSM has registered a large increase in the

number of cyber attacks in recent years. The NSM has stated that around 80% of the incidents they deal with could have been avoided if basic security measures had been followed. It is therefore important to increase awareness-raising and strengthen preventive work. Companies and authorities must have expertise and capacity to uncover and handle unwanted incidents.

3 Means for strengthening national control and building cyber resilience

The state has a range of means for achieving national control and building cyber resilience. These means must be assessed individually and in context, and will vary depending on where you are in a spectrum of conflict, how much control is desirable in different contexts and any associated costs. Means for safeguarding national security must also be assessed in light of Norway's obligations under international law, including free trade agreements with third countries. As we strengthen our ability to withstand the actions of state threat actors, they will adapt their use of their means in a way that may affect our national security interests. Our means must therefore be adapted and developed over time to meet these challenges.

On a general basis, it is important to give sufficient priority to means with a preventive effect. Incident management is often more expensive and intrusive than prevention. The focus on preventive measures is important on all levels of society, from individuals to companies and authorities. The PST, the police and the NSM have a specific responsibility here. At the same time, society must have sufficient resources to deal with incidents once they have occurred.

Changing economic framework conditions place higher demands on priorities and effective resource utilisation. This means that prioritising the preventive measures becomes more and more important, and will result in having to balance between different considerations, needs and wishes. Means such as increased national ownership and control through the acquisition of strategically important companies, natural resources and infrastructures, for example, have a direct cost. The need for national control for reasons of national security can also result in costs for society and industry. For example, if increased reporting obligations were required or if restrictions on private ownership, access to international capital, business cooperation, and relations with other states were enforced. Norway has obligations through the EEA agreement and other international agreements, such as WTO regulations and free trade agreements, which must be safeguarded if ownership restrictions are to be introduced. Risk acceptance is another important element, including an assessment of adequate national control and cyber security. Society's use of resources and proportionality to achieve national control and digital resilience must be assessed against effectiveness. For this reason, cost-benefit assessments must be carried out. The many considerations mentioned here must be weighed against the consideration of safeguarding national security and together constitute a good decision-making basis.

Box 3.1 Cyber attacks cost NOK 20 million on average

A global study from IBM shows that 83% of the world's companies have experienced at least one cyber attack in the last two years. The cost of an average cyber attack on a company has increased by 13% in just 2 years. The cost averages NOK 20 million in the Nordic countries and NOK 40 million globally.

When Norsk Hydro was hit by a widespread cyber attack in 2019, the company was completely paralysed, and the costs of the attack were NOK 800 million. Another example is the Danish shipping company A.P. Møller-Mærsk. The company was hit by a cyber attack in 2017, the costs of which were estimated to be between 200 and 300 million US dollars.

3.1 Regulation must follow developments in society

Regulation is the primary means for ensuring national control, and is also cost-effective. Legal instruments usually consist of various injunctions

Figure 3.1 Satellite-based communication, surveillance and earth observation are among the fundamental national functions.

Photo: Shutterstock

or prohibitions, combined with the power to be able to grant permits, rights and obligations or exemptions linked to these. Regulation is a strong, but often necessary, tool. It creates predictability and is a prerequisite for equal treatment in a state governed by the rule of law.

3.1.1 The Security Act – our most important tool for safeguarding national security

The Security Act is uniquely positioned to safeguard national security. According to the Security Act, assets that are important to our national security interests must be designated and secured in line with the law's requirements. The ministries designate fundamental national functions and can decide that companies that are of vital importance for fundamental national functions shall be subject to the Security Act.[1] This asset mapping is a continuous process which covers all areas of society. This mapping work is complex and shows, among other things, that there are extensive mutual dependencies across areas of society, and that this dependency changes relatively quickly. There is a need to update and improve the overview in order for preventive security work to be as targeted and effective as possible. This will be prioritised across all areas of society in line with the Ministry of Justice and Public Security's leading and coordinating role within the work on preventive national security on the civilian side.

The government is interested in ensuring that the Security Act is adapted to the current risk and threat picture at all times, and will therefore put forward the necessary proposals for adaptations to the regulations. The law as a means of safeguarding national security is strengthened through revisions to the Security Act. See Chapter 4.2.1 for proposed changes to Chapter 10 of the Security Act about ownership control.

Companies that are subject to the Security Act must have sufficient expertise to follow up on the law's requirements. A shared security under-

[1] Fundamental national functions are defined in the Security Act as 'services, production and other forms of enterprise of such importance that a complete or partial loss of function will have consequences for the state's ability to safeguard national security interests.'

Box 3.2 Changes to the Police Act and the Police Databases Act

In Prop. 31 L (2022–2023), the Ministry of Justice and Public Security has proposed amendments to the Police Act and the Police Databases Act regarding the PST's intelligence mission and use of openly available information. The proposal suggests that the PST should prepare analyses and intelligence assessments about conditions in Norway that could threaten national security interests. Moreover, it is proposed that the PST processes openly available information if it is believed to be necessary for the preparation of analyses and intelligence assessments, even if the individual information in isolation is not necessary. These proposals will enable the PST to assess to a greater extent the likely future development of threats in Norway and the threat actors Norway will face in the future, and will be an important measure to safeguard national security.

standing, security culture and a basic securing of assets that are important to national security must develop over time. The Ministry of Justice and Public Security has asked the ministries to map their own security expertise during 2022, and will follow up with feedback to the ministries (see Chapter 3.4.1 for further discussion).

3.1.2 Practice of existing legislation

The government believes that many existing regulations in various areas of society can contribute to achieving national control, not just the Security Act.[2] Certain regulations do not include national security as an assessment criterion today, while other regulations already have provisions that take care of the security perspective. The government believes that there is room for manoeuvre for safeguarding national security in existing regulations in different areas of society, and that this room for manoeuvre should be better utilised.

The practice of different regulations cannot be seen in isolation, but must be seen across areas of society. Different permit schemes and management perspectives can create blind spots, which can be exploited by foreign states at the expense of national security interests. Our ability to protect national security is therefore dependent on the individual sectors and the authorities being jointly aware of the threat picture, their own assets and dependencies, within and across areas of society. The principle of cooperation ("samvirkeprinsippet") is important in this regard. In addition, the Ministry of Justice and Public Security and the Ministry of Defence are important drivers of cooperation between the civilian and military sides.

The government will go through relevant existing legislation to ensure that consideration of national security is included as an assessment criterion where appropriate.

With regard to strategically important assets, companies, property, infrastructure, natural resources and technology, relevant regulations that can be assessed in more detail include concession legislation, the Planning and Building Act, the Waterfall Rights Act, the Energy Act, and the Ports and Waters Act. This does not mean that considerations of national security will always weigh more heavily, but that it must be considered as a minimum. The purpose is to make demands on those who administer legislation, and those who must comply with it in order to prevent unwanted actors from gaining insight, control and influence over assets that are of importance to national security. It is appropriate to make any adjustments in the relevant regulations as part of another review of the law. The legislation must also be seen in context with other legislation, to avoid unnecessary double regulation.

3.1.3 Export control

The Export Control Act[3] and related regulations[4] apply to the export of specified goods, technology, including intangible outputs, technical data packages or production rights for goods, as well as certain services. The aim is to ensure that exports that can be used for military purposes, or as weapons of mass destruction, do not contribute to conventional, military capacity building in countries of concern, and to ensure that export is in accordance with Norwegian foreign and security policy interests.

[2] Certain relevant regulations will be discussed in chapter 4.

[3] Act relating to the Control of the Export of Strategic Goods, Services, Technology, etc.

[4] Regulations concerning the export of defence material, multi-purpose goods, technology and services.

The control of the export of strategic goods and technology is increasing in complexity in line with security policy developments and changes in the threat picture to Norwegian interests. Countries with which we do not have security cooperation with seek strategic goods, technology, services and knowledge from Norway to strengthen their military capability. This covers conventional military capacity building and programs for weapons of mass destruction, as well as equipment that can be used for intelligence activities or mapping of critical infrastructure in Norway. Norwegian technology communities are constantly exposed to attempts to circumvent export control regulations.

The government wants to clarify and strengthen export control regulations, and clarify the practice of control of knowledge transfer in and from Norway. This includes clarifying what export control-regulated knowledge transfer is, and introducing a provision on license obligations for knowledge transfer in the export control regulations.

In spring 2022, the Ministry of Foreign Affairs conducted a general hearing of proposals for changes to the export control regulations. The Ministry of Foreign Affairs is in the process of assessing these proposals and will follow up the regulatory work further in 2023.

3.1.4 Proposal for a new Norwegian cyber security Act

The government is considering putting forward a proposal for an act on cyber security. Central to this is making companies accountable and ensuring the implementation of national advice and recommendations.

The government plans for the bill to apply to operators of essential services within the areas of energy, transport, health, water supply, banking services, financial market infrastructure and digital infrastructure. Furthermore, it will also apply to the providers of digital services, more specifically providers of cloud services, digital marketplaces and digital search engines. The regulations will also clarify what is required for a business to be considered an operator of essential services. The Norwegian cyber security act will require companies to implement security measures and notify of serious cyber incidents. This applies to certain areas of society which have an essential important role in maintaining critical social and economic activity. As the act is further developed, particular attention will be paid to expanding its scope, and to ensuring that national advice and recommendations are followed up by companies to a greater extent. The act will facilitate the introduction of the EU's NIS Directive.[5]

The government will continuously assess regulation to ensure that companies that support important functions in society have sound cyber security. Among other things, the EU's revised NIS Directive will be significant in deciding how the Norwegian Cyber Security Act is further developed. Other relevant EU legislation includes the EU's Cybersecurity Act, which deals with the mandate of the European Union Agency for Cybersecurity (ENISA), and a common European framework for voluntary certification of IT products, services and processes. Efforts are being made to incorporate this regulation into the EEA agreement. The EU has also recently launched the Cyber Resilience Act which sets minimum requirements for cyber security in products and services. A draft legislation on digital operational resilience for the financial sector, the Digital Operational Resilience Act, is also being considered in the EU. The goal of this legislation is to ensure that all participants in the financial system have the necessary measures in place to reduce the danger of cyber attacks and other unwanted incidents. The draft builds on the NIS Directive and will take precedence over the NIS Directive's rules where applicable once it has

Box 3.3 Long-term strategic work

Norwegian authorities have worked strategically with cyber security over a long period of time through major studies, reports to the Parliament ("Storting"), strategies and the development of measures. Norway was the second country in the world to produce a national strategy for cyber security in 2003. In 2019, Norway became the first country to publish a fourth strategy. Internationally, Norway is considered to be a mature country in this area and for many, an attractive partner for collaboration. This report to the Storting further builds upon long-term work where strengthened advice and guidance and the need for further regulation have been identified as important areas.

[5] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Box 3.4 The EU's proposal for a revised NIS Directive

In November 2022, the EU agreed to a new directive, NIS2. The scope of the directive has been extended compared to the NIS Directive by adding new sectors and entities. Entities to which the regulations will apply will be classified based on their importance and divided into two categories: essential or important entities and, respectively, subject to different supervisory regimes. The new directive also strengthens the security requirements for companies with a list of basic measures that must be applied as a minimum, and gives more precise provisions for the reporting of incidents. Furthermore, security in supply chains and supplier relationships is addressed. EU member states are given a deadline of 21 months to introduce the directive nationally, at which time the current NIS Directive will be repealed.

entered into force. The proposed regulations are considered to be EEA-relevant.

3.2 National ownership to ensure national control

In some areas, national ownership contributes to ensuring national control. This applies, for example, to energy and natural resources, important infrastructure and strategically important elements of Norwegian private sector. National ownership includes state ownership, county municipal ownership and municipal ownership, as well as private Norwegian ownership. Due to complex value chains and ownership structures among other things, national ownership does not necessarily imply national control.

'State ownership' refers to the state's direct ownership of companies. Since 2002, a white paper on ownership policy has been presented to the Storting in each parliamentary session about the state's overall direct ownership of companies. The ownership report explains why the state is an owner, what the state owns and how the state exercises its ownership. The current ownership report[6] lists public security and preparedness as reasons why state ownership can be an appropriate measure. The following appears in the ownership report:

> "Regulation is the primary policy instrument used for safeguarding considerations relating to national security, civil protection and emergency preparedness. Examples of such regulation are the Business and Industry Preparedness Act, the Power Contingency Regulations, the Security Act and the Electronic Communications Act. State transfers to manufacturers, contracts with private actors or other forms of cooperation with business actors that are administered and managed through the respective sector ministries are examples of other policy instruments.
>
> In special cases, the State may consider it necessary to prevent undesirable interests from obtaining access to information, influence or control over companies that are of importance to national security, civil protection or emergency preparedness. This can be achieved by, among other things, making the companies subject to the Security Act or by owning a specific stake in certain companies."
>
> "State ownership based on civil protection and emergency preparedness normally suggests that the State should own more than half the company. This helps to prevent outside interests from acquiring majority shareholding or gaining influencing through positions on the board."

Public ownership (state, county municipal or municipal ownership) can provide the public with large revenues, and facilitate the desired social development and democratic control. At the same time, public ownership can be resource-demanding, can have economic costs, require significant follow-up and be politically sensitive. National control can be achieved through various means and is not necessarily the same as public ownership. Having control can include preventing undesirable actors from gaining control of or possibly acquire property, resources or infrastructure that can give them insight or influence, or reduce our own political or economic room for manoeuvre. This can also be achieved through private Norwegian ownership of companies, property or other assets.

Checking to identify the real owners of e.g. infrastructure, natural resources or property of importance to national security is important. The

[6] Meld. St. 6 (2022–2023) *A greener and more active state ownership – The state's direct ownership of companies.*

Box 3.5 State ownership as a means for public security and preparedness

Public security and preparedness have for a long time been justifications for state ownership. The state operated its own production of defence material through Kongsberg Våpenfabrikk, Horten Verft and Raufoss Ammunisjonsfabrikker. These companies were established in the 19th century under the auspices of the Norwegian Armed Forces, and were spun off in 1947 into separate, independent companies. The companies eventually also entered into other industrial production. The state has continued ownership of the ammunition business through Nammo, and of the production of other military material through the Kongsberg Group.

government wants a better oversight of this. It will provide insight into whether ownership can be a challenge for national security. Information about foreign ownership is registered by a number of institutions, both Norwegian and international, but the information is currently not systematised to a large extent. This therefore requires extensive national and international cooperation. The need for oversight of strategically important areas is more closely discussed in Chapter 4.

3.3 National and international cooperation

Cooperation and information sharing across society, services, sectors, public-private and across international borders is crucial in the work on national security. For example, various private and public actors have much relevant information that can contribute to increased insight and common understanding of the risk and threat picture. This contributes to a better basis for decisions and an adapted use of our means, and makes us better able to protect assets of importance to national security in peace, crisis and armed conflict. Increased expertise and involvement at all levels of society must be an integral part of meeting the risk and threat picture. By strengthening individual security, we contribute to strengthening our collective security.

3.3.1 Collaboration between intelligence and security services

Extensive cooperation and information exchange between our intelligence and security services is fundamental for national security. Information

Box 3.6 Intelligence and security services

The Norwegian Police Security Service (PST) is Norway's national domestic intelligence and security service, subject to the Ministry of Justice and Public Security. The PST is tasked with preventing and investigating serious crimes against the nation's security. As part of this, the service must i.a. identify and assess threats related to unlawful intelligence activities, the proliferation of weapons of mass destruction, sabotage and politically motivated violence or coercion. These assessments will contribute to policy development and support political decision-making processes.

The Norwegian Intelligence Service is Norway's foreign intelligence service. The service is a part of the Norwegian Armed Forces, but the work covers both civilian and military topics. The Norwegian Intelligence Service's main task is to notify of external threats to Norway and prioritised Norwegian interests, support the Norwegian Armed Forces and defence alliances in which Norway participates, and support political decision-making processes with information of special interest to Norwegian foreign, security and defence policy.

The Norwegian National Security Authority (NSM) is a national competent authority for preventive security in accordance with the Security Act. Among other things, the NSM gives advice on the protection of and supervises the safeguarding of critical national information, information systems, objects and infrastructure. The NSM is also national specialist hub for cyber security and is responsible on a national level for updating, warning and coordinating the handling of serious cyber attacks.

Figure 3.2 The PST is Norway's national domestic intelligence and security service.

Photo: Ministry of Justice and Public Security

about and understanding of the risk and threat picture is vital for ensuring that various actors can identify their own vulnerabilities and safeguard their own security. A prerequisite for this is appropriate frameworks and tools, especially for the handling and dissemination of highly classified information.

In order to contribute to increased information exchange and coordination between the Norwegian Intelligence Service and PST on specific cases, the collaboration was further strengthened in the summer of 2021 through the establishment of a Joint Intelligence and Counter-Terrorism Centre. In November 2022, the government established the National Intelligence and Security Centre (NESS). The PST, the Norwegian Intelligence Service, NSM and the police will collaborate in NESS to strengthen our national ability to detect and understand hybrid threats – and our own vulnerabilities – as well as to ensure good decision-making support for the authorities. This collaboration builds on the enhanced collaboration between PST and the police established in February 2022, in order to develop national hybrid threat picture. This measure emphasises the government's prioritisation of work against hybrid threats.

The Joint Cyber Coordination Centre (FCKS) is a permanent, co-located professional environment consisting of representatives from the NSM, the Norwegian Intelligence Service, PST and Kripos. The work done by FCKS helps to increase our national ability to protect ourselves against serious cyber attacks and maintain a comprehensive risk and threat picture for cyberspace. Furthermore, they contribute to important analyses at strategic level, which forms a basis for the government's decision making.

3.3.2 National Cyber Security Centre at NSM (NCSC)

Through the National Cyber Security Centre, the NSM has established an arena for national and international collaboration for detection, handling, analysis and advice related to cyber security. The Centre includes partners from business, academia, defence and the public sector who actively contribute to mutual cooperation for a more robust digital Norway. Around 50 companies cur-

Figure 3.3 National Cyber Security Centre in the NSM.

Photo: Norwegian National Security Authority

rently participate, with more and more joining. The partner program will be strengthened, both to open up for more partners and to facilitate more information sharing.

With more partners, the need to divide the partner network into target groups increases. This is important in order to build trust and share information internally in the network, and to reach out with better adapted information to individual companies in a more efficient way. The National Cyber Security Centre is an important part of the NSM's work with advice and guidance, detection and incident handling (see points 3.5 and 3.6).

To strengthen research, innovation and expertise within cyber security, Norway is following up on the EU's regulation on the establishment of a network of national coordination centres for cyber security. In this context, a centre will be established, in order to build up and coordinate the national part of the European expert community within cyber security and generally stimulate research, innovation and competence development nationally. An important task for the centre will be to promote and give guidance to applicants to the European investment programmes DIGITAL and Horizon Europe's cyber security-related calls. The centre is also expected to be able to allocate EU funds and national co-financing to third parties. DIGITAL and Horizon Europe are EU investment and research programmes, in which Norway already participates.

The Ministry of Justice and Public Security is working to enable the NSM and the Research Council of Norway to establish Norway's national coordination centre for cyber security. The centre will collaborate with other cyber security communities in Norway.

3.3.3 International cooperation

In an international economy and a digitalised society, where dependencies, means and threat actors are not limited to national borders, international collaboration is important to achieve national control. This includes working for responsible government behaviour in the cyber space and seeking to use existing channels, such as the EU's framework for foreign direct investment screening, for access to information about economic activity which could threaten our security.

Experience from our allies, NATO, the UN and the EU can give useful insight on best practice across international borders and help adapt national regulations to have a common approach, where appropriate. In light of Finland's and Sweden's NATO applications, it will be particularly relevant to seek common Nordic solutions where possible, given our similar governance systems, values and risk and threat picture. By taking a clear role internationally and being able to point to national initiatives and priorities, Norway could also be perceived as a predictable and reliable ally and partner, which is important for our position in international cooperation.

A main priority for Norway at an international level is to work for strengthened compliance with current international law among UN member states. In 2021, Norway published its national positions on selected international law issues in cyberspace to contribute to a strengthened common understanding of how international law applies. The services and products we use are often completely or partially produced and developed in other parts of the world. This requires collaboration on international standards from a security perspective.

The government wants Norway to work towards a close, binding and predictable international cooperation on national security and counter hybrid threats together with allies, partners, NATO, the UN and the EU.

The government wants Norway to actively participate internationally for strengthened compliance with current international law. Norway will contribute to the work on the preparation of international voluntary norms and standards within cyberspace. The government will also strengthen collaboration with international partners to create an open, secure, stable and peaceful cyberspace.

3.4 Competence and awareness raising

3.4.1 Security competence in society

Competence about threats, vulnerabilities and effective countermeasures are a prerequisite for being able to protect assets against unwanted incidents. A lack of competence about risk and know-

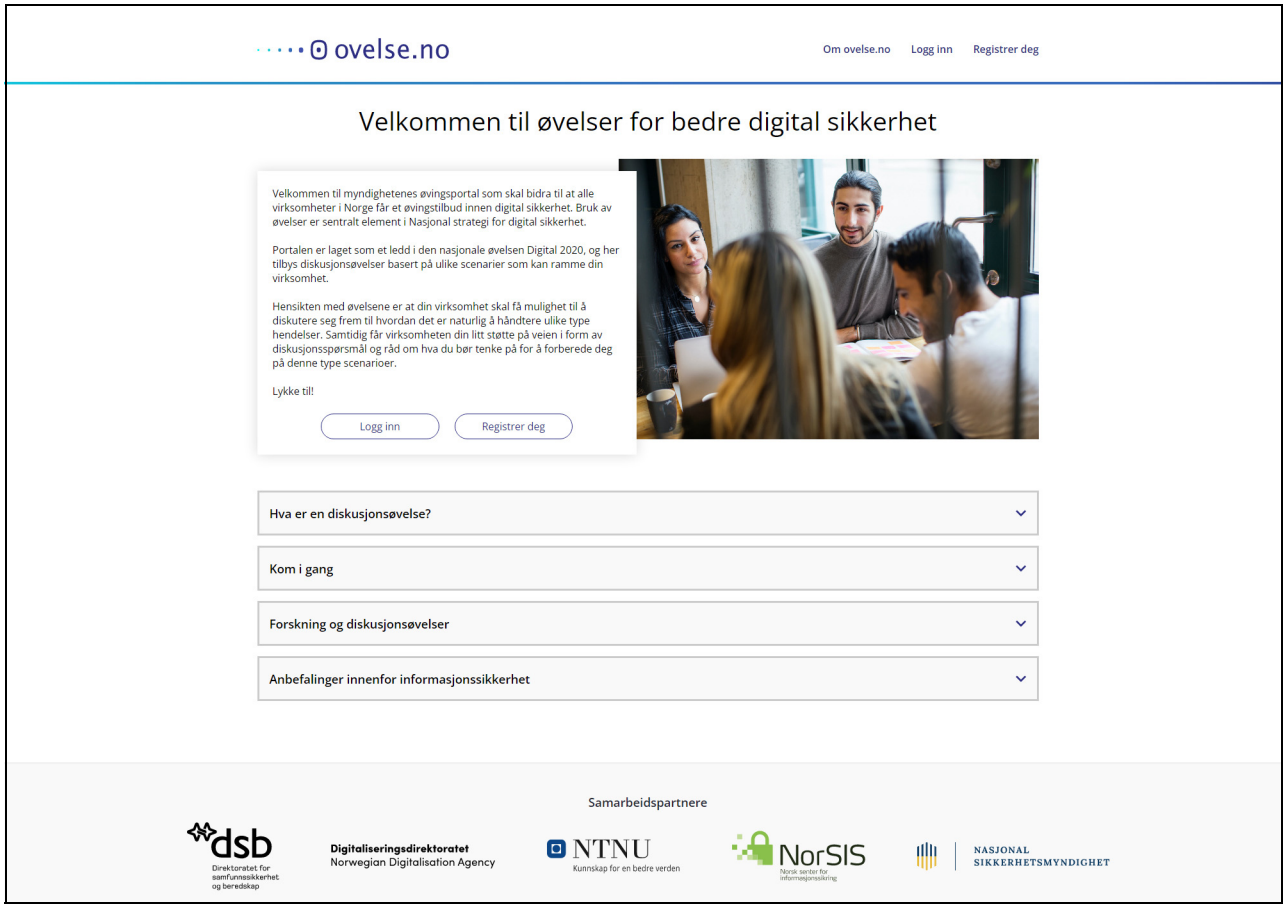

Figure 3.4 The ovelse.no platform is the authorities' training platform, to help all companies in Norway to access free training in cyber security.

Screenshot: ovelse.no

Box 3.7 Media literacy

Media literacy is important for the population's resilience. This is a highly prioritised area for the Norwegian Media Authority, which conducts a survey on media literacy in the population every two years. The mapping includes exposure to and handling of disinformation and fake news, knowledge of differences in editorial and commercial content, privacy, knowledge of sources and trust in the media. The Norwegian Media Authority implements measures and advice to ensure that the population is well equipped to navigate and understand the media. Tenk, which is the educational department of the fact-checking service Faktisk.no, develops teaching programs which cover critical media use and source awareness for use in schools.

ledge of our own assets and vulnerabilities leads to reduced security management and a weaker connection between the actual risk picture and measures that reduce risk. There are many examples where the combination of a lack of understanding of assets and a culture of openness has led to information about e.g. property and infrastructure of importance to national security being openly available on the internet, i.e. risk and vulnerability analysis or an overview of socially critical infrastructure. Companies and public bodies that manage assets of importance to national security must assess the consideration of national security to a sufficient extent when such information is made available.

Technical security measures alone cannot stop potential threat actors. It is therefore necessary to build a good security culture across all of society. This assumes that everyone – individuals, companies and authorities – is aware of the security challenges and has the necessary basic knowledge of countermeasures that are relevant to them. This increases robustness, but also the individual's awareness and understanding of security. It is particularly important to strengthen the understanding of assets and competence about threats, vulnerabilities and effective security measures among top level managers and decision-makers. A good security culture is expressed through each company's overall security behaviour.

Box 3.8 National strategy for cyber security competence

The national strategy for cyber security competence from 2019 facilitates a long-term build-up of competence, including the national capacity in research, development, education and awareness raising measures aimed at the population and companies. The strategy has been developed by the Ministry of Justice and Public Security in collaboration with the Ministry of Education and Research.

NorSIS coordinates National Cyber Security Month every year in October on behalf of the Norwegian authorities. This is an example of an awareness raising measure in society at large. The aim of this campaign is to strengthen the cyber security competence of companies and individuals. Another example is the national training portal, ovelse.no, which offers all Norwegian companies free training in cyber security.

In order to facilitate good follow-up of the Security Act, the Ministry of Justice and Public

Box 3.9 National public information campaign

On behalf of the Ministry of Justice and Public Security, NorSIS will, cf. Prop. 78 S (2021–2022). carry out a national public information campaign on cyber security. The aim of the campaign is to increase security awareness and competence in the population. The campaign will be implemented in collaboration with relevant actors such as the NSM and the police. The campaign is directly targeted at the population and small and medium-sized companies, and will have a style and message that are easy to understand. One of the themes that will be promoted is measures to contribute to increased cyber security in the population, such as two-factor authentication for various services. In order to reach as many people as possible, it is planned that the campaign will largely take place on social media. The campaign will start in December 2022 and will continue throughout 2023.

Security has asked the ministries to map management positions that have roles and responsibilities linked to the ministries' fundamental national functions. These managers need security clearance and expertise of security management, risk assessment, asset assessment and basic cyber security.

The Ministry of Justice and Public Security has also recommended that all ministries, in accordance with the Security Act, map which management positions in underlying companies require security clearance and security expertise. Results are to be submitted to the Ministry of Justice and Public Security by the end of 2022. The ministry will then assess the need for further competence measures on public companies to safeguard our national security interests.

3.4.2 Adequate national specialist expertise

Surveys of supply and demand show a need for more graduates in cyber security. In recent years, a number of measures have been implemented to reduce the skills gap. Several long-term measures are considered. For example, the full effect of increased admission to IT-related subjects has not yet come in the form of number of graduates.

The government will map the need for cyber security expertise and will assess measures based on the needs of the workforce.

Within certain areas of significance for national security, there is a need for personnel with specialist expertise at doctoral level. Personnel must be able to lead research and development in areas where they process information that could have decisive consequences for national security if the information becomes available to unauthorised parties.

A sufficient number of graduates at master's level is a prerequisite to ensure more graduate researchers and others highly competent personnel with security clearance in the fields of cyber security and cryptology. 90% of students of 'science subjects, craft subjects and technical subjects' were Norwegian in 2021. The proportion of foreign students on programmes relating to cyber security varies between study programmes, but in total it was just 5% in 2021.[7] Increasing the admission to cyber security and other IT studies will therefore contribute to increasing the proportion of researchers and other highly competent people who will be able to obtain security clearance.

Any changes in student admissions are assessed in the annual state budgets. At the same time, the government expects universities and university colleges to assess the scope of cyber security in their study portfolios themselves, based on the needs of the workforce and the wishes of their applicants, as they must do for all their educations, including doctoral educations.[8]

Recruiting doctorate candidates who can be given security clearance is already currently a challenge in various technological areas. In the last ten years, well over 60% of those who completed a doctorate in technology at a Norwegian educational institution have had foreign citizenship.[9] The proportion of foreign nationals applying for recruitment positions in mathematics, natural sciences and technology was close to 90% in the period 2016–2018.[10] This is a development that must be taken seriously.

The government will continue with earmarked funds for the Research Council's industry PhD and public sector PhD schemes aimed at cyber security and cryptology. These funds are available for all qualified applicants who have security clearance.

Recruiting candidates who can be given security clearance for doctoral education in cyber security and cryptology will also require targeted efforts from universities and university colleges. As mentioned above, the government expects educational institutions to determine the scope of their doctoral education according to the needs of the workforce and the wishes of applicants. In the case of employment in recruitment positions where the employee will be in situations that require either security clearance, access clearance or authorisation, universities and university colleges must ensure that the appointed person receives the necessary clearances, as required by the Security Act.

---

7 Higher education statistics from the Norwegian Directorate for Higher Education and Skills.

8 Recommendation 425 S (2020–2021) and Meld. St. 19 (2020–2021) Management of state universities and university colleges.

9 Statistics Norway 2022. Article: Rekordmange utenlandske statsborgere blant de nye doktorene i 2021 [Record number of foreign citizens among new PhD graduates in 2021].

10 NIFU 2019. Søking, rekruttering og mobilitet i UH-sektoren sektoren [Attractive academic careers? Searching, recruitment and mobility in the HE sector]. Report 2019:10.

Box 3.10 The balance between a still open and internationally oriented education and research sector and increasing emphasis on security considerations

Increased internationalisation has for a long time been a goal of Norwegian higher education and research policy, and an important instrument for increased quality and relevance in Norwegian education and research. Good facilitation of long-term cooperation with strong professional environments in other countries is crucial for the further development of Norway as a nation of knowledge, and for Norwegian contributions to solutions to the challenges we as a society face. This also includes countries with which we do not have security cooperation.

In Norway, as in other like-minded countries and in the EU, OECD, etc, there are discussions as to how to facilitate a good balance between a still open and internationally oriented education and research sector and increasing emphasis on security considerations. In line with this, 'responsibility' has been introduced as a fundamental principle in the current strategy for higher education and research collaboration with priority countries outside the EU.[1]

Several measures have been taken to facilitate collaboration within higher education and research in priority areas while safeguarding national interests. This includes a permanent round table for academic cooperation with China, which is coordinated by the Ministry of Education and Research, and 'Møteplass Kina' [Meeting Place China], which is organised by the Research Council and the Norwegian Directorate for Higher Education and Skills. The round table is aimed at strategic management, while 'Møteplass Kina' is aimed at those who work more operationally with higher education and research collaboration at Norwegian universities, colleges and research institutes. In addition, work is underway to develop national guidelines for responsible international cooperation, which will be available during the first half of 2023.

[1] The Panorama Strategy (2021–2027) regjeringen.no.

Box 3.11 Public-private collaboration on security testing and critical system investigations

Norway must have the expertise and capacity to verify and validate equipment and systems that are integrated into systems that are critical to society's ability to function. Over several years, NTNU, in close collaboration with the power industry, has worked to build up such a capacity that can be used for security testing and investigations of hardware and integrated systems. Statkraft, Statnett, Eidsiva, Kraft-CERT, NVE, NSM and Energy Norway have been driving forces behind this public-private collaboration initiative. Together with partners, NTNU is now making an investment of approx. NOK 15 million to establish a laboratory environment to meet this need. The investment is made in connection with Norwegian Cyber Range.

Most PhD candidates in technological subjects will not need security clearance during their doctoral education, but they may need security clearance in the job they go to after completing their doctorate. In some subject areas of importance to national security, it will therefore be desirable to ensure that a sufficient number of doctoral candidates who can get security clearance after education. With the current regulations for security clearance and employment in government positions, it is unclear how universities and colleges can regulate the intake of research fellows in order to fulfil the desire to train doctoral candidates who can get security clearance. At the same time, the workforce's need for doctoral candidates who can get security clearance is unclear. Before the government starts assessing the regulations, the need should be assessed.

The government will examine the workforce's need for doctoral qualifications for positions where a security clearance is required.

3.5 Advice and guidance – the user in focus

A high level of common understanding of security, the risk and threat picture, from individuals to companies and public enterprises, is important for national security and national control. This also includes why national security is important, what instruments the authorities have at their disposal, what requirements are placed on various public and private actors and how it affects the individual. The sum of individual measures contributes to greater resilience in society against unwanted events.

3.5.1 The establishment of a national portal and support tool for cyber security

The government will launch a national portal for cyber security and a support tool for all Norwegian companies to make national advice and recommendations available in line with Prop. 78 S (2021–2022).

Advice and guidance on cyber security is often not well known and is only to a limited extent systematically followed up and prioritised by companies. The portal will be a common gateway for different user groups, but will be designed so that everyone receives uniform advice adapted to their user group. This should not require prior knowledge of roles and responsibilities within the area.

Box 3.12 National advice and recommendations on cyber security are not used enough

In 2021, The Ministry of Justice and Public Security and the Ministry of Defence conducted a survey among Norwegian companies about the national strategy for cyber security and awareness of national advice and recommendations for cyber security. The results show that those companies that are aware of the national recommendations in the strategy and NSM's basic principles use these to a large extent in their operations. This applies to both the public and private sectors, regardless of the size of the company. Only a small number of companies have followed up on all recommendations. The main reason is stated to be a lack of time, but also that the companies are unsure of how to proceed.

The work of developing a portal started in autumn 2022 with a planned launch during 2023. The portal's contents will be developed by central actors with roles and responsibilities related to cyber security. NSM leads the work, and will establish, manage and run the portal.

Increased security in individual companies is an important contribution to society's collective security. In order to contribute to more systematic work with cyber security, NSM will offer a support tool to all Norwegian companies through the national portal. The tool will make it easier for companies to evaluate their own security maturity level and contribute to national advice being better known and implemented by companies.

3.5.2 Merging government guidance resources

Several state authorities provide advice and guidance about cyber security, and the authorities' work in this area can appear fragmented and uncoordinated to the outside world.[11] The portal and the support tool described in Point 3.5.1 will contribute to better coordination and making advice and guidance more available. The government will consider further measures to strengthen coordination at authority level and make it easier for the end user.

The government will map user needs and experiences with the current organisation of guidance in cyber security. This is to assess tasks, responsibilities and organisation, and whether merging of government guidance resources will be able to produce efficiency gains.

3.5.3 A secure digital network architecture ('Zero Trust')

During the last decade, the work on a secure network architecture has increasingly taken as its starting point the fact that one cannot have more trust in machines and services in a company's internal network than one has in arbitrary machines and services on the open internet. A consequence of this is that digital identities, authentication and access management have become central tools for establishing a secure network architecture. This approach has been called 'Zero Trust' architecture.

[11] NOU 2018: 14 *IKT-sikkerhet i alle ledd* [ICT Security at Every Stage].

The government will ensure that Norwegian recommendations on secure network architecture are updated in line with the development of international standards in this area.

3.6 National detection capability and incident management

3.6.1 National incident management

A large proportion of the threats against Norway occur in cyber space. Over time, NSM has experienced a sharp increase in cyber attacks. According to the NCSC, this is a trend that is expected to continue in the future. The cyber attacks on the Storting in 2020 and 2021 were attacks on our democracy and show the seriousness of the cyber risk picture. For the first time, Norway took the step of making a public attribution to another state. It was announced that Russia was behind the attack. The following year, it was announced that the second data breach against the Storting was carried out from China.

To help meet this challenge, the NSM has been granted NOK 15 million in 2022, cf. Recommendation 270 S (2021–2022) to Prop. 78 S (2021–2022). The grant will expand the number of positions in the NCSC and will improve the ability to coordinate, analyse and handle incidents and provide practical assistance to affected companies.

Sector-specific response communities are an important measure to ensure the sharing of information and support for handling cyber attacks.

Box 3.13 The Oil Fund experiences cyber attacks every day – cyber attacks are the Fund's biggest concern

Norges Bank Investment Management has the daily task of managing the Norwegian Government Pension Fund ('the Oil Fund') and makes a major effort to reduce the likelihood and consequences of cyber incidents on its own operations. The number of attacks they experience is increasing, and attackers are constantly using more advanced methods and means. Thus, cyber security has become one of the biggest concerns for the fund's manager.

Box 3.14 Team Norway

Commissioned by the Ministry of Justice and Public Security and the Ministry of Defence, NSM and the Norwegian Cyber Defence Force coordinate Norwegian participation in the international cyber exercise Locked Shields. The purpose of Norwegian participation is to train response communities in incident management in the civilian and military sectors. Through the establishment of 'Team Norway', the NSM and the Norwegian Cyber Defence Force have followed up the strategy of extensive public-private and civil-military cooperation to meet cyber threats.

Most sectors have established such communities or have entered into various forms of cooperation in this regard. These response communities are the link between the NSM and individual companies in various sectors. On behalf of the Ministry of Justice and Public Security, an external evaluation of sectoral response community scheme has been carried out. The overall impression is that cooperation between the various actors works well, that there is a good exchange of information, methods, experiences and competence across the communities, and that the system of sectoral response communities has provided a more unified security environment in Norway. A main conclusion is that the national effort should be combined to secure fundamental national functions. Moreover, preventive cyber security should be included to a greater extent in the national model for incident management and balanced against operational work. Given the lack of expertise within cyber security, it is also important that the national model for incident management is sustainable over time.

The government will further develop the national framework for managing cyber incidents. This is to ensure a sustainable incident handling model in line with society's needs.

3.6.2 Digital resilience in the municipal sector

Unwanted cyber incidents in municipalities can have large consequences on services for citizens, and can result in large costs for the municipalities and for the Norwegian society. Although

Figure 3.5 Norway has frequently participated in the international exercise Locked Shields.

Photo: NATO CCDCOE, Ardi Hallismaa

cyber security in the municipalities is handled within public security, a hybrid threat picture makes it necessary to work towards better digital resilience also from a national security perspective. In a challenging economic situation, it will however be difficult for the municipalities to set the necessary priorities and acquire cyber security expertise.

In February 2022, over 200 municipalities attended a meeting with the Minister of Justice and Public Security and the Minister of Local Government and Regional Development. The purpose of this meeting was to raise awareness of cyber security in the municipal sector, inform about a changed risk and threat picture and enter into dialogue with the municipalities about how the state can contribute so that they are better equipped to prevent and handle unwanted cyber incidents. As a follow-up to the municipal event, the government wants municipalities to have a permanent response community that meets the municipalities' needs.

The government will contribute to the prevention of unwanted cyber incidents in the municipal sector and will designate a sectoral response community that can meet the municipalities' needs.

Box 3.15 Østre Toten municipality exposed to ransomware virus

On 9th January 2021, Østre Toten municipality was exposed to ransomware, which put large parts of the municipality's network back to manual management for a long time. The actor had stolen significant amounts of data. The municipality's operational ability was greatly reduced when most of the municipality's digital services were down. The situation worsened further on 29th March, when parts of the stolen data were published on the dark web. The municipality had to handle sensitive personal data that had been stolen, and inform and support people who were affected. In practice, the incident meant that the alarm system at nursing homes was replaced with bells, the locking system in the municipality's buildings did not work, and that the health centre's records were inaccessible. The incident has cost the municipality around NOK 34 million.

3.6.3 Establishing next-generation national detection capability

'Advanced persistent threats' are the defining threat to national cyber security. The actors behind them are often considered to be government actors who work systematically over time to create access to relevant systems.

The early warning system for digital infrastructure (VDI) functions as a 'digital burglar alarm' to detect attacks. VDI is a network of sensors that are deployed at selected public and private enterprises that have critical infrastructure. The sensors make it possible for the NSM to detect and verify cyber attacks.

In order to increase the effectiveness of the system, the number of companies participating in the VDI collaboration and the analysis capacity to handle larger amounts of information will have to increase. The NSM has been granted NOK 30.3 million for this initiative, cf. Recommendation 270 S (2021–2022) to Prop. 78 S (2021–2022). Next-generation VDI will be expanded with several different components that are designed to work together and overall will be more efficient than today. The expansion is also an important contribution to seeing the totality of and the work with a national situation picture in the cyber domain.

One of the government's ambitions is to further develop national detection capabilities. Development in this area will require long-term investment, which also includes infrastructure. Central to this is the further development of VDI and any requirements for VDI sensors for important suppliers that support key functions in society. Increased analysis capacity and technical capacity in the NSM will be considered in order to detect incidents which could threaten our security.

4 National control of assets of importance to national security

It is important to ensure national control of assets of importance to national security.[1] Examples from recent years show that the use of economic means against assets such as infrastructure, companies, property, natural resources and technology can represent a security risk, and this is a particular challenge.

State actors can use economic means to exploit vulnerabilities, strengthen the effect of other means of power or help to legitimise these means of power. This comes in conflict with our national security interests. Investments and acquisitions can, for example, be used as a means of gaining insight into sensitive information relating to emergency arrangements, critical infrastructure or political decision-making processes. Economic means can also grant access to technology and resources of strategic significance.

Research-based expertise about the use of economic means which could threaten our security is crucial in order to take the right measures to strengthen resilience against this activity. The Ministry of Justice and Public Security has given several research assignments to the Norwegian Defence Research Establishment (FFI) and the Norwegian Institute of International Affairs (NUPI). The assignments include foreign investments and ownership in Norway.

4.1 Overview of assets and value chains

4.1.1 Mapping companies and assets

A fundamental prerequisite for safeguarding national security is that the authorities have an overview of assets and companies that are important for national security. Such an overview is necessary in order to be able to assess which of the measures described in chapter 3 are relevant and appropriate for ensuring national control. There is a need for a better overview of foreign ownership in companies and property, among other things. The need for new tools, such as the development of registers, access to and use of databases and analysis tools, must be assessed in more detail. The use of such tools must not violate confidentiality considerations.

The Security Act has a proper methodology for mapping assets of decisive and significant importance to the state's ability to safeguard national security interests (fundamental national functions). This mapping shows that national security is safeguarded by a large amount of companies in all areas of society, and that there are extensive dependencies both within the same sector and across sectors. This mapping is complex, and the dependencies change relatively often. The government therefore wants to prioritise this mapping so that it is sufficiently updated and detailed, in order for the use of means to be as accurate as possible.

The government believes that there is also a need for a better overview of companies and assets to which the Security Act does not apply, but which may nevertheless be of importance to national security. This will concern companies and assets that have less than decisive importance for national security, but which, as part of a total or in a given context, could have such importance that it may be appropriate to take measures. This can be physical, digital or other assets, such as e.g. research information and knowledge, infrastructure, companies, property and natural resources. An overview of such assets can give central and local authorities insight into assets of importance to national security within their area of responsibility, and will supplement the overview that central authorities have from mapping in accordance with the Security Act. Based on this overall picture, the authorities can assess relevant instruments to safeguard national security, including national ownership and control. How the overview is to be followed up, for example related to responsibilities and roles, instruments and regulations, must be assessed in more detail. It will be necessary to see such an overview in context with other relevant work, such as changes to the Security Act and the screening of economic activity against

[1] In such assessments, different considerations will always have to be weighed, as discussed under point 2.2.

Figure 4.1 The power supply is an important part of Norway's infrastructure.

Photo: Shutterstock

companies that are not subject to the Security Act. The government will intensify this work.

The government will assess how to appropriately gain a better overview of companies and assets that are not covered by the Security Act, but which may still be of importance to national security.

4.1.2 Increased overview of our dependencies and value chains

Central services and functions in society are largely dependent on long and partly blurred value chains. A value chain can be explained as a structure of deliveries between companies. The value chain represents a dependency between companies to deliver services or products. Value chains can include physical infrastructure, digital dependencies, ownership and sub-suppliers. Value chains are often complex and opaque with many dependencies, which often cross international borders.

Failures in value chains can have major consequences. The Covid-19 pandemic and the war in Ukraine have shown us how vulnerabilities in international value and supply chains can challenge security of supply. If the power supply fails, large parts of society will come to a standstill. Outages in the digital infrastructure lead to the unavailability of digital services in the affected area. Outages in satellite-based services will have consequences for e.g. the Armed Forces, rescue services, shipping, aviation and parts of the financial industry.

Threat actors can exploit vulnerabilities in value chains which are important for national security, and/or gain control over central parts of value chains through e.g. ownership. Vulnerabilities in a value chain can result in activity which could threaten our security being carried out against subcontractors in the value chain, either as a goal in itself or as part of achieving goals higher up in the value chains.

Norway has an open economy and is a digitalised society. This means that we have many complex and cross-border value chains, over which it is difficult to have control. Digital value chains have received a lot of international attention through value chain attacks in recent years (see text box 4.1 about SolarWinds). Individual companies are responsible for having an overview of and

Box 4.1 SolarWinds

In December 2020, the American IT company SolarWinds was exposed to a supply chain attack. The attack was a sophisticated and extensive cyber operation in which the threat actor managed to establish a backdoor in one of SolarWinds' programmes. The backdoor was then included in an update of the programme that SolarWinds itself distributed to its customers, over 18,000 companies worldwide. US authorities later stated that the actor behind the attack probably had Russian origins.

Some of the severity lay in the type of programme that was affected. It is designed to carry out network monitoring and will therefore usually have wide access to the company's infrastructure. By infiltrating this, the actor gained a very favourable starting point for getting into the network and bypassing security mechanisms.

The case had extensive consequences for those affected, including US government agencies and large technology companies such as Microsoft. After gaining access to companies that had installed the update via the backdoor, the actor strengthened their capabilities against designated targets. It indicated that the actor did not exploit all the access it had obtained, but rather prioritised certain companies that were exposed to more targeted methods for further compromise.

NSM worked closely with national and international collaboration partners to map the scope of the incident. Recommendations from the Cybersecurity and Infrastructure Agency in the US (CISA), FireEye and Microsoft were followed, and NSM encouraged all companies that used the software in their infrastructure to familiarise themselves with the available documentation. Many of SolarWinds' customers in Norway had installed a compromised version of the programme. The major consequences did not occur because the backdoor was not used. Still, this type of supply chain attack is something that NSM expects more of in the future, with potentially significant consequences for Norwegian targets.

control over their value chains, to the extent possible. Increased provision of services requires better follow-up of suppliers, including companies having sufficient ordering expertise and making sufficient security assessments.

We depend on international collaboration in order to achieve national control over value chains, both physical and digital. Norway will work to maintain close, binding and predictable international cooperation to identify value chains that are important for national security and to reduce failures in these value chains.

The government will initiate a collaborative project between the Ministry of Local Government and Regional Development and the Ministry of Justice and Public Security to assess the need for measures within risk management of digital value chains.

In this project, a mapping of selected value chains linked to critical digital infrastructure that is of importance to national security will be carried out, which will form the basis for the establishment of effective guidance and appropriate regulation for Norwegian companies. Mapping will also contribute to developing measures and lay the basis for a revision of the NSM's basic principles for IT security. Moreover, such a survey will be able to contribute to the work of designating fundamental national functions and their critical

Box 4.2 Emergency stockpile for medicines

A resilient health preparedness must be adapted to the challenges and the current security situation. The Covid-19 pandemic has also highlighted international dependencies and vulnerabilities. A national emergency stockpile for infection control equipment has been set up, where regional health organisations own inventory, are responsible for purchasing, rolling out and developing stock. The government will continue the stockpile in 2023, and it includes respiratory protection, masks, gloves, eye protection, surgical gowns and full-coverage suits and has a volume equivalent to six months of pandemic consumption.

Box 4.3 Supply chain security in the power supply

In 2021, an investigation carried out by the Norwegian Water Resources and Energy Directorate (NVE) showed that cyber attacks primarily affected administrative IT systems in the power industry and that attacks could move to companies via suppliers that had been attacked. NVE has statutory requirements for deliveries of operational control systems to the most critical facilities, and recommends that the industry familiarise themselves with the risk and threat reports from PST, the Norwegian Intelligence Service and the NSM, as well as to assess land risks. NVE also collaborates with trade organisations in order to raise the knowledge base and further develop relevant guidance material.

Box 4.4 Foreign states increase their expertise and technology through acquisitions

In the 'Bergen Engines case', acquisition as a means for appropriating technology was brought to the fore. In Royal Decree 21/1898, the decision that halted the sale of the Bergen company, states: 'Norwegian industry and Norwegian knowledge and research institutions are targets for Russian intelligence activities. Russia shows particular interest in companies that have unique expertise and technology, including within the defence industry and maritime sector. The Western sanctions regime is causing Russia to seek alternative methods to acquire critical technology and expertise in order to further develop its own military capabilities. The use of private actors is an example of such a method, and is something which makes it more challenging to detect and prevent covert procurement.'

digital dependencies, as well as to the work of designating socially important and essential services as part of the work on the Cyber Security Act. The framework for risk management of digital value chains will be included as a knowledge base in this work.[2]

4.2 Strategically important companies

Norway has an open economy that is closely integrated with the world's economy. Openness to foreign investment is positive for economic growth and prosperity, but at the same time makes us vulnerable to foreign states with hostile intentions. PST's national threat assessment for 2021 listed unwanted acquisitions as a significant threat to Norwegian interests. The concern was repeated in the threat assessment for 2022 and was supported by risk and threat assessments from the other intelligence and security services.

The Norwegian state already uses a number of means to ensure national control over strategically important companies. The Security Act has provisions on ownership control in companies subject to the act, and state ownership is used as a tool in some cases. The reasons for state ownership are also apparent from the white paper on ownership policy, and are discussed in section 3.2. There is a need for a better overview and control of ownership structures in strategically important companies in Norway in order to identify any activity which could threaten our security. Examples of strategically important companies include the defence and security industry, including those that are not subject to state ownership. Even though much work is being done in this area, and the government is further strengthening opportunities to gain a better overview and control, there will always be a residual risk that must be managed.

4.2.1 Ownership control and screening mechanisms based on the Security Act

Chapter 10 of the Security Act gives the authorities the opportunity to control ownership in companies that are subject to the Security Act. The provision set out in Section 2-5 grants the authorities the right in extreme circumstances to intervene in the economic activities of companies that are not subject to the Security Act under specific conditions. However, Section 2-5 of the Security Act is intended to act as a safety valve.

Norway has a screening mechanism based on the Chapter 10 and Section 2-5 of the Security Act.

[2] Risk management in digital value chains. Norwegian Directorate for Civil Protection (dsb.no).

Figure 4.2 Companies within the defence and security industry are examples of strategically important companies.

Photo: Frank Holm

The mechanism consists of an interministerial network, led by the Ministry of Justice and Public Security, as well as an agency network led by the NSM. In 2021, the NSM was appointed as the national contact point for notifications related to security-threatening economic activities. The process and criteria for handling cases under Chapter 10 are described in the Act, while in 2022, guidelines were drawn up for the ministries' handling of cases concerning possible security-threatening activity in companies that are not subject to the Security Act and where it may be appropriate to use Section 2-5. The Norwegian authorities aim to have the opportunity to detect, assess and possibly intervene in economic activity that could threaten national security. At the same time, it is important that Norway's obligations under international law are safeguarded and that unnecessary or disproportionate burdens are not placed on business or restrictions on trade with other countries. This is challenging since the management of security-threatening economic activity hits the intersecting point between security interests and commercial, foreign policy and trade policy considerations. The different ministries therefore work closely together to evaluate and weigh the various considerations against each other.

The government aims to put forward proposals for changes to Chapter 10 of the Security Act, on ownership control etc., in early 2023.

The main purpose of the proposal is to strengthen the ability to protect our national security interests against other states' use of financial instruments by increasing the authorities' access to information about changes in ownership in the companies that are subject to the Act. The purpose is also to clarify rules on the suspension of acquisitions, etc., so that the law does not limit Norwegian companies' opportunities to attract investment beyond what is necessary to protect national security interests.

The proposal means that the ministries are given increased opportunity to make the provisions in the Security Act, including the provisions on ownership control in Chapter 10 of the Security Act, applicable to more companies than today. Furthermore, it is proposed to lower the thres-

hold for the acquisition of companies to be reported to the authorities, and that both the transferor and the company, in addition to the acquirer, are obliged to send a notice of acquisition.

This will strengthen the authorities' ability to intervene in cases where an actor's attempt to gain control or significant influence over a Norwegian company is considered to be in conflict with national security interests.

4.2.2 Screening of economic activity against companies that are not subject to the Security Act

The national screening mechanism has been established on the basis of Chapter 10 and Section 2-5 of the Security Act. There will however be cases of economic activity against Norwegian companies which potentially could threaten our security that are not captured through the reporting obligation under Chapter 10 for companies subject to the Security Act. There is therefore a need to look more closely at a possible mechanism to capture potential security-threatening economic activity for companies to which Chapter 10 does not apply. Section 2-5 is, as mentioned under 4.2.1, intended to function as a safety valve, not as a basis for ordinary processes. The regulations therefore do not provide details about sectors, criteria or the process for processing cases of potential security-threatening economic activity.

The government has appointed a public committee to investigate the need for regulations, or a scheme to screen economic activity against companies that are not subject to the Security Act. This must be seen in the context of the current screening mechanism and the proposal for changes to the Security Act's provisions on ownership control. The committee will deliver a Norwegian Official Report (NOU) in December 2023.

The committee must look at how relevant countries handle screening cases and take this into account in their assessments. The committee will also look at the work of an interministerial working group set up by the Ministry of Foreign Affairs, which is considering the future organisation of export controls.[3] A survey carried out by NUPI (2021) of a selection of countries' screening mechanisms shows that there is great variation in how different western countries' screening mechanisms are set up, but that several EU countries are in the process of harmonising their regulations and mechanisms against the requirements set in the EU screening regulation from 2019.[4]

4.2.3 The need to strengthen the national control of properties of security relevance

In their risk and threat assessments, The Norwegian Intelligence Service, PST and the NSM have pointed out that foreign ownership of properties in certain geographical areas may pose a threat to national security interests.

Certain properties may be of security relevance because they are located near critical infrastructure, such as ports, defence facilities or power supplies. This can include commercial properties, holiday homes, agricultural and forestry properties or other types of property. A 'property of security relevance refers to a property which, due to its location, can facilitate

Box 4.5 New legislation in Finland cuts down on who can own property

FFI report 22/00426 on 'Russian economic statecraft – implications for Norwegian security' mentions new Finnish legislation: 'In Finland, in 2018, the authorities raided several Russian-owned properties with extensive surveillance equipment installed on the property. The properties were located near strategically important ports and waterways in the Baltic Sea, and the ultimate owner was hidden through companies registered in tax havens. While the properties may be linked to non-state, criminal activity, Finnish security and intelligence services generally point to properties in Finland purchased by Russian actors being used for military purposes. It is the concentration of properties near strategically important locations that arouses the suspicion of the security and intelligence services.'

In 2019, the Finnish authorities introduced a law making it obligatory to apply for permission for the purchase of certain properties. The law is administered by the Finnish Ministry of Defence.

[3] See more about the export control work under 3.1.3.

[4] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union.

Figure 4.3 Foreign ownership of properties can pose a threat to national security interests.
Photo: Robert Bye/Unsplash

security-threatening activities against a critical national object or infrastructure.

In the Bergen Engines case, the property's location was emphasised in the justification for stopping the sale:

> 'The property is strategically located by the northern approach to Bergen and defence installations of security importance for Norway and allied nations. Russian intelligence activities against Norwegian aims and interests may result in the property appearing as an interesting platform for Russian services.'

Foreign ownership interests in property can be represented in Norway via foreign private individuals who live here, via enterprises they control or have shares in, or as investments in property without any other form of registered activity in Norway. Information about who owns properties is only to a small extent systematised in ways that provide an overview of foreign ownership interests, despite the fact that a lot of relevant data is collected. Information about owners is often recorded in ways that do not differentiate between Norwegian and foreign actors.

When assessing ownership of property and the use of property, it is important to assess the scope in extant regulations, for example to systematise extant data, and give relevant authorities access to information on ownership of properties.

The aim is to present proposals for changes to the Security Act's ownership provisions, etc. early 2023. Proposals for changes to Section 7-3 of the Security Act are being considered to specify that companies' risk assessments must identify specific properties with locations that can allow for security-threatening activities against critical national objects and infrastructure. This could increase the vigilance and awareness of companies, and lower the threshold for notifying the security authority when companies receive information about activities related to properties that may pose a risk. The proposal also suggests that

the security authority should have an oversight of properties of security relevance where risk cannot be reduced by security measures.

In order to strengthen the authorities' ability to detect security-threatening activities related to the ownership and use of property, the government wishes to give Kartverket (the Norwegian Mapping Authority) and the NSM the task of arranging a system that would generate a necessary overview of property of security relevance. Such access can be granted on the basis of Section 4, third paragraph, letter h) of the regulations on the disclosure, further use and other processing of information from the land register.

Hidden ownership of real property can have consequences for national security interests if the properties are used for security-threatening activities. As part of strengthening national control/checks into hidden ownership, the government has begun work to map challenges related to hidden ownership in real property.

The government will strengthen checks of hidden ownership of properties of security relevance, and is considering:

- *proposing changes to the Security Act which specify that company owners have a duty to undertake risk assessments which identify specific properties with locations that can allow for security-threatening activities against critical national objects and infrastructure.*
- *giving the security authorities electronic access to the land register in order to have an oversight of properties of security relevance.*
- *mapping challenges associated with hidden ownership of real property, including a possible registration obligation.*
- *taking a closer look at how being obliged to apply for permission to purchase certain properties can possibly be regulated.*

4.2.4 Emphasise national security in spatial planning

The area part of municipal master plans must, to the extent necessary, show considerations and restrictions that are significant for the use of the area. National security is not currently a factor that is considered in current provisions. The government will consider changing this.

The state and regional bodies concerned can raise objections to proposals for the spatial and zoning plan of municipal master plans in matters that are of national or significant regional importance, or which are of significant importance to the relevant body's area of expertise. Through the rules on the right to object, a system has thus been established for checking current provisions. Furthermore, it is delegated to the state administrators to guide the municipalities in spatial planning, among other things related to the provisions on public security. This guidance role is important, as it contributes to increasing the municipalities' expertise in spatial planning.

The Government will take a closer look at the provisions in the Planning and Building Act to ensure that national security is emphasised in spatial planning. Furthermore, the government will consider expanding the rules on the right to object, so that the state has the right to object in areas related to national security. The government will also consider expanding the state administrator's duty of guidance towards the municipality in relation to national security.

4.2.5 Safeguarding national security concerns in concession legislation

The Concession Act aims to regulate and control the sale of real property in order to achieve effective protection of agricultural production areas and conditions of ownership and utilisation that are most beneficial to society.[5] The Act applies to the acquisition of real property, but not to indirect transfers such as the acquisition of shares or impersonal companies that own real property. In addition to acquisitions, the Act provides authority for checks if e.g. long-term rights of use are established on a property that would require a concession in the event of a transfer. Such rights are subject to a concession regardless of the size of the area seized by the rights. The Act stipulates that this applies to all acquisitions, but exceptions to this have been made in the Act and in regulations. In practice, exceptions have meant that checks are usually only relevant when someone acquires a property that is to be used for agricultural purposes, or when acquiring property located in municipalities with a reduced concession limit, and where the purpose of acquisition is to use the property for purposes other than year-round housing.

Municipalities can grant concessions, set conditions for concessions, or reject applications. In each specific case, there is a broad interpretation of which conditions of ownership and utilisation that are most beneficial to society. This means that various societal considerations and interests

[5] Act relating to concession in the acquisition of real property (28th November 2003).

can be included in the assessment of the concession application. As a consequence, the Concession Act can also be linked to national security since it provides an overview of who acquires property. It may be desirable to regulate the acquisition of certain properties, for example based on a value survey, as discussed in 4.1.1.

The government will take a closer look at the practice of the Concession Act, so that national security considerations are assessed before concessions are granted, where relevant.

The purpose of this is to prevent unwanted actors from gaining insight, control and influence over properties that are of importance to national security.

4.3 Strategically important infrastructure

An infrastructure can consist of physical elements, such as water supply, underwater infrastructure, installations at sea, ports, airports, or outer space (ground-based and satellite-based). Infrastructure can also consist of digital and more high technology elements such as algorithms and sensors. Mapping, acquisition of and investing in important infrastructure can create opportunities for infiltration, surveillance and sabotage. This can enable attacks or disturbances in the social functions supported by that infrastructure. Furthermore, import of technology from foreign companies can make critical infrastructure vulnerable to future cyber attacks. In today's security environment, it is important to assess different instruments to secure strategically important infrastructure, of significance for national security.

Box 4.6 Critical Entities Resilience (CER) – a new directive from the EU

The EU is working on a new directive (the CER directive) to increase the security of member-states' ability to deliver critical goods and services, and to ensure that populations have access to these in crisis situations. The directive includes services such as drinking water, energy, health, transport, digital infrastructure, public authorities, outer space and the finance sector. The directive is meant to strengthen EU countries' societal resilience.

Ensuring national control over critical infrastructure that crosses Norway's national borders is challenging, but important. The current security environment emphasises this. For this type of infrastructure, Norway is dependent on international cooperation in order to achieve national control.

The government will map strategically important infrastructure in order to identify which allies and close partners we are most dependent on in order to secure national control, and will establish a close, binding and predictable collaboration with them.

4.3.1 National cloud service

Many Norwegian companies choose to buy cloud services from large commercial, multinational companies. This usually helps to increase companies' security as they can phase out outdated IT solutions and access secure infrastructure and professional security environments. At the same time, the government is concerned with the overall national dependencies on foreign cloud suppliers, and the consequences of this dependencies in the event of potential crises and conflicts. For some companies, the use of cloud services should therefore be assessed against the need for national control and national preparedness.

More and more companies are choosing public cloud services to meet the need for new and improved IT solutions. However, for several state enterprises, it is a challenge that there is no access to functional and cost-effective cloud services with a sufficient degree of national control. It can lead to increased risk if such solutions are nevertheless chosen. The alternative is that companies may choose local solutions, which can lead to higher costs and limited access to new technological tools. This problem is expected to grow in the future.

The government will consider the establishment of a national cloud service to ensure increase national control over critical IT infrastructure, and to protect important information.

In November 2021, NSM was commissioned to investigate the need for a national cloud service. A number of central actors are involved in this work. The investigative work is extensive, complex and addresses several fundamental and cross-sectoral issues, including technological, security-related, organisational, legal and financial issues. The alternatives that are assessed must be based on the national processing and storing of

Box 4.7 Other countries' national cloud services

Many of our nearest neighbouring countries have activities related to national cloud services. Sweden has not yet established a state service, but has carried out several investigations and clarifications. Denmark has established 'GovCloud' which is run by the Danish Agency for Governmental IT Services, and which allows which for applications to be submitted in a publicly owned and operated cloud service. Germany has established 'Die Bundescloud' which is a closed cloud service which is developed, owned and run by the state. The United Kingdom has a 'G-Cloud' which helps to make procurement easier, with standardised framework agreements and approval of suppliers.

data. Security challenges that may arise if a supplier is subject to the jurisdiction of foreign states are included in this assessment. The same applies to the ownership model, for example if the national cloud service is to be owned and operated by the state itself, but using expertise and innovative power from the private sector. This investigation must be delivered by the end of 2022, so that quality assurance can be carried out by the summer of 2023.

4.3.2 Data centres

A data centre is an infrastructure which stores and carries digital services and data, and forms an important part of the digital foundation, in line with infrastructure for electronic communication. Meld. St. 28 (2020–2021) *Our shared digital foundation* refers to the growing fusion of traditional electronic communication and IT, cloud and data centre services, where third-party providers are being more closely integrated into electronic communication providers' solutions.

Today, many critical digital services are delivered from data centres, and companies are increasingly dependent on them. Some examples of services carried by data centres are mobile services, such as calls and data, payment services, health and welfare services, critical communication services, TV and radio distribution (DAB), the Norwegian Armed Forces' communication services and future emergency and preparedness communication.

The government will specify requirements for security and preparedness for data centres, and has submitted a legislation proposal for consultation. This proposal suggests setting requirements for appropriate level of security for data centre services, as well as introducing a registration obligation for data centre actors, which will enable the authorities to have a better overview of the data centre industry in Norway. The defence sector is exempt from the regulation of data centre operators.

Data centres and anonymous leasing can be abused by criminal and state actors. Ultimately, such leasing challenges national security, as cyber attacks can be carried out from Norway without the Norwegian authorities having the opportunity to locate owners or equipment.

The government will investigate current measures to uncover and combat the leasing and use of data centres for criminal and security-threatening purposes. The consequences of current measures for the data centre industry and national data storage capacity must be assessed. The investigation will start when the new Electronic Communications Act is presented to the Storting.

The government also wishes to carry out a survey of which data centres provide services of importance for critical societal functions. Such a survey will reveal whether sectors and their redundancy are concentrated in a small number of data centres, and whether this poses a concentration risk. This survey will cover data centres within and outside of Norway. For data centres in Norway, the survey will include dependencies to electronic communication networks and power supplies that supply the data centres. It will also be relevant to know the reason why certain companies use foreign data centres, and what it would take for them to switch to using data centres in Norway. Based on this survey, the Ministry of Justice and Public Security, in collaboration with relevant ministries, will assess measures in this area. In accordance with the established division of responsibilities between the civilian sectors and the defence sector, a corresponding survey and follow-up for the defence sector will be carried out by the Ministry of Defence.

For reasons of national security, it is very important in some areas that we have control over stored data and that this is available in various parts of the spectrum of conflict. The government wants the functions upon which society is most dependent to be delivered from data centres in Norway, or close allies and partners. An appro-

Figure 4.4 Lefdal Mine Data Centre is built in a disused mine between Måløy and Nordfjordeid.

Photo: ABB

priate level of security is required at these data centres. Operation and storage of information of importance to national security interests was one of the issues that was highlighted in connection with discussions about IT infrastructure in health institutions after the events in Helse Sør-Øst in 2018.[6] At the same time, the war in Ukraine has made it clear that it can be precarious to have all such infrastructure located in one's own country. For Norway, this means that we need sufficient redundancy, including through international cooperation and agreements. The police opened a new data centre in 2021, where other actors in the justice sector are also present. The police are also working on choosing a concept for a corresponding data centre to ensure redundancy.

Box 4.8 Operation and management of IT solutions in state enterprises

On behalf of the Ministry of Local Government and District Affairs, an external survey has been carried out to map the extent to which the current organisation of operation and management of state IT solutions is suitable for solving future demands and challenges in terms of cost efficiency and secure development, operation and management of the state's IT solutions. This survey shows that a significant proportion of state enterprises have not drawn up a sourcing or cloud strategy. This can lead to vulnerabilities at national level, as it is possible to lose track of the value chains upon which Norway is dependent, and where specific data is stored. However, the survey shows that 65% of enterprises comply to a high degree (54%) or to a very high degree (11%) with the basic principles for security management drawn up by NSM.

6 Recommendation 386 S (2017–2018) Recommendation to the Storting from the Health and Care Services Committee.

4.3.3 Solutions for classified communication

We currently have a range of systems for classified communication. Many of these systems are developed, operated and managed by the defence sector. There is currently no common actor who is responsible for looking after the needs of civilian sectors in this work from a total defence perspective. Several systems are currently being developed, phased in or phased out. Another challenge is the fact that many of the solutions have different operating and management models on the civilian side.

The government will assess which environment and which actor are best suited to take care of the civilian sectors' needs for solutions for classified information. This is to ensure a more consistent delivery of classified systems in civilian sectors, and effective interaction between civilian sectors and the defence sector.

4.3.4 Digital communication infrastructure

Digital infrastructure carries increasingly valuable and critical services for Norwegian society. It is clearly stated in the government's political platform that the cases in which the state should take ownership of digital infrastructure, in order to secure these assets, will be assessed. The government is therefore setting up an expert committee to assess how the state can ensure national control over critical digital communication infrastructure. The Ministry of Local Government and Regional Development is coordinating this work.

Undersea fibre cables make up an important part of the digital infrastructure. New technology can detect possible threats to undersea fibre cables, for example by analysing acoustic signals. The government is strengthening telecom preparedness on the Norwegian continental shelf. Means of doing this include, among other things, a support scheme for the purchase of new technology that enables identification of threats to undersea fibre cables, funds to carry out investigations of important undersea fibre cable stretches and the purchase of equipment that can detect disturbances to satellite-based services, e.g. GPS on the Norwegian continental shelf.

4.3.5 Space activity of importance to national security

The intelligence and security services have increasingly highlighted the importance of space activity for national security and national security interests in recent years. This has been strengthened by changes to the European and global security environment, especially in the last year. Preventive security will thus become increasingly important in this area, both in outer space and ground-based installations. Norway is an important space nation, and our geographical position is attractive for space activities, including launching satellites and deploying ground-based sensors.

The government considers space activities in outer space and on the ground to be of strategic importance for Norway's foreign, security, and defence policy. In the work on the new Space Act, the government places emphasis on safeguarding national security interests. In addition, the government is seeking to further identify which areas within space activities that are particularly relevant to national security. In order to ensure the cross-sector considerations within space activities, specific matters are discussed in an interministerial space security committee.

4.4 Strategically important natural resources

Natural resources can be of importance to national security. In connection with the implementation of the Security Act, fundamental national functions have been identified within water supply, power supply, food supply and petroleum operations, among other things. Other natural resources are currently not defined as crucial for national security. However, natural resources such as mineral deposits, forest and agricultural resources should be assessed based on their importance for national security. Foreign ownership of strategically important natural resources may challenge our own control of these resources in the long run.

4.4.1 Ensuring control over strategically important natural resources

Regulatory instruments are the most important means for ensuring national control over strategically important natural resources, and can be used to prevent certain actors from purchasing some types of property or resources. State ownership is one of a number of means that have been used to ensure control over and, to some extent, to ensure income from the country's large natural resources. At the same time, natural resources

Figure 4.5 Natural resources can be of importance to national security.

Photo: Shutterstock

are location-bound. The state will therefore have a certain degree of control over these resources, regardless of ownership, and can regulate their management in different ways. National control of natural resources does not just refer to ownership, but also to our national ability to extract and utilise these resources.

An important element to consider when assessing the need for national control over natural resources is their geographical location, for example in areas of particular importance for national security or safeguarding Norway's sovereignty. Geographically, Svalbard and the High North are particularly relevant because of their strategic position, but locations near critical national objects will also be of great importance. Moreover, natural resources can be important for national security based on the needs they cover, for example security of supply, energy, water or food.

It is not necessarily a goal to have national ownership of natural resources that are crucial for national security. Rather, it may be important to have national control through other means, to prevent other actors from gaining ownership or control over such natural resources. This also applies where a natural resource is not currently considered to be of importance to national security, but which in the longer term may become important to our national security if another actor gains influence or control over it.

Norway must have relevant technological expertise on, for example, mineral deposits, extraction of water resources, oil and gas, and wind power. This can help to reduce our own dependence and vulnerabilities.

Box 4.9 The significance of energy, minerals, water and forest resources

Energy resources

Energy resources have been, and are, an important part of the basis for settlement, industry and business throughout Norway. The government wants our renewable energy resources to be used and refined in Norway. The government's climate policy must also contribute to a strong national ownership of natural resources.

A number of countries are seeking information about Norway's decision-making processes in energy production. Companies in the petroleum sector must be prepared for unauthorised persons trying to gain access to information. This is even more relevant given the energy dimension of Russia's warfare in Ukraine. In 2022, the government has put in place a number of measures to secure the petroleum sector.

There is currently a large degree of national ownership within the petroleum sector. The concession system ensures national control over those companies who are granted the right to extraction permits on the Norwegian continental shelf, and important decisions require the consent of the authorities. For reasons of national security, the Ministry of Petroleum and Energy may deny access to petroleum activities if the applicant or licensee is actually controlled by a state outside of the EEA, or by national from such a state.

Energy legislation sets requirements for both physical and cyber security, and has a wider scope than the Security Act. However, the aim of this legislation is not to safeguard national security, but power supply. This legislation will safeguard security of supply for power, and set requirements for preventive security and preparedness for both accidental and non-accidental incidents.

Mineral resources

Social development has shown that there is an increasing need for minerals, especially as a result of the shift towards a green economy. Minerals can be critical for important societal purposes and for technology development in strategically important areas. Internationally, it has been shown that control over raw material production can be used to monopolise the value chains. Mineral resources can be of importance to national security. It can therefore be desirable to prevent unwanted foreign actors from gaining access to mineral resources in Norway, on land or on the seabed. This can be due to those actors' national technological development, potential military use of civilian technology, and possibly through the property's location near critical national objects or infrastructure.

Water supply

Developments in the threat picture in recent years have shown a need for increased attention to the security of water supplies. Municipal water utilities have been exposed to cyber attacks on water and sewage infrastructure during 2021. Norwegian water supply must be equipped to withstand both intentional and unintentional incidents. Prevention and preparedness in the water supply are important for public security. A secure water supply is a basic national function as defined in accordance with the Security Act.

Forest and agricultural resources

Ownership of forest and agricultural properties can be of importance to national security when the property is in a strategic location, or is close to critical national objects or infrastructure. Furthermore, the totality of foreign ownership of forestry and agricultural properties can constitute a vulnerability for national security, if large areas of land are not owned nationally. National ownership and control of forest properties will be important. The government will continue working to ensure Norwegian ownership of forest properties through concession legislation. Furthermore, concession legislation for agricultural ownership contributes to national control and long-term, solid management of agricultural resources.

Box 4.10 Meraker Brug

Meraker Brug was one of the largest private forest and wilderness properties in Norway, and has a history stretching back to the early 18th century. The property has a total area of 300,000 acres, of which more than 50,000 acres are productive forests. The property lies in the municipalities of Meråker, Stjørdal, Malvik and Steinkjer. Statskog SF has entered into an agreement to buy 94% of AS Meraker Brug's shares and is in the process of purchasing the remaining. The purchase was approved by the Storting in November 2022. Through state ownership, the government has ensured the property remains in Norwegian hands. With this purchase, Norway's largest privately-owned property passes into public ownership and common natural resources benefit the community.

Figure 4.6 Large areas south of Meråker with Fonnfjellet and Skarvene in the background.

Photo: AS Meraker Brug

4.5 Strategically important technology

Technological development is progressing ever faster. The distinction between civilian and military technology is getting blurred, while more and more actors are gaining access to the same technology. Technological development affects international relations and the instruments used by states and non-state actors in peace, crisis, and armed conflict. If Norway is to be able to utilise technological development to strengthen national security, it is crucial to have national expertise, research and development, in addition to creating business development. As a small nation, Norway does not have the resources to have expertise within all emerging and disruptive technologies. It is therefore important to assess which technologies are of importance to national security and the areas in which there is a particular need for national expertise. Examples of this can be quantum technology, artificial intelligence, computer science or space technology.

Within defined strategically important technology areas, national ownership and control can

include having sufficient national specialist expertise, preventing foreign investments that threaten national security or having clear export control regulations for the transfer of knowledge into and from Norway. Reference is also made here to Meld. St. 17 (2020–2021) *Cooperation for Security – National Defence Industrial Strategy [for a] Technologically Advanced Defence for the Future* and the Ministry of Defence's strategy to protect Norwegian-developed defence technology. The strategy is geared towards national areas of technological expertise and also includes other areas of technology that are defined as critical, especially emerging and disruptive technologies, such as space technology.

4.5.1 National Centre for Applied Cryptology

Cryptology is an important part of the national preventive security work and is essential for protecting classified information. Technological development, with rapidly increasing computing power, reduces the level of security in today's crypto algorithms. In some cases, we must take into account that encrypted information that we consider secure today could be stored by unauthorised persons and decrypted at some point in the future. The problem is further made relevant by developments in quantum computers. It is thus crucial to ensure that we have the required expertise to meet these cryptology challenges. There is a need for cryptology expertise within academia, the crypto industry and the authorities.

Norway is a significant supplier of high classified cryptography to other NATO countries. These deliveries form an important basis for cooperation which is of importance to national security. It is key to ensure the national capability and competence required to meet crypto developments and to maintain the position as a credible supplier of crypto solutions to NATO.

The NSM was granted NOK 6.2 million in 2022 to establish a national centre for applied cryptology. The Centre will contribute to Norway maintaining and further developing national crypto competence and ensure Norway is equipped to meet future challenges in cryptology. The NSM's upgraded high-technology crypto laboratory is a central part of the Centre.

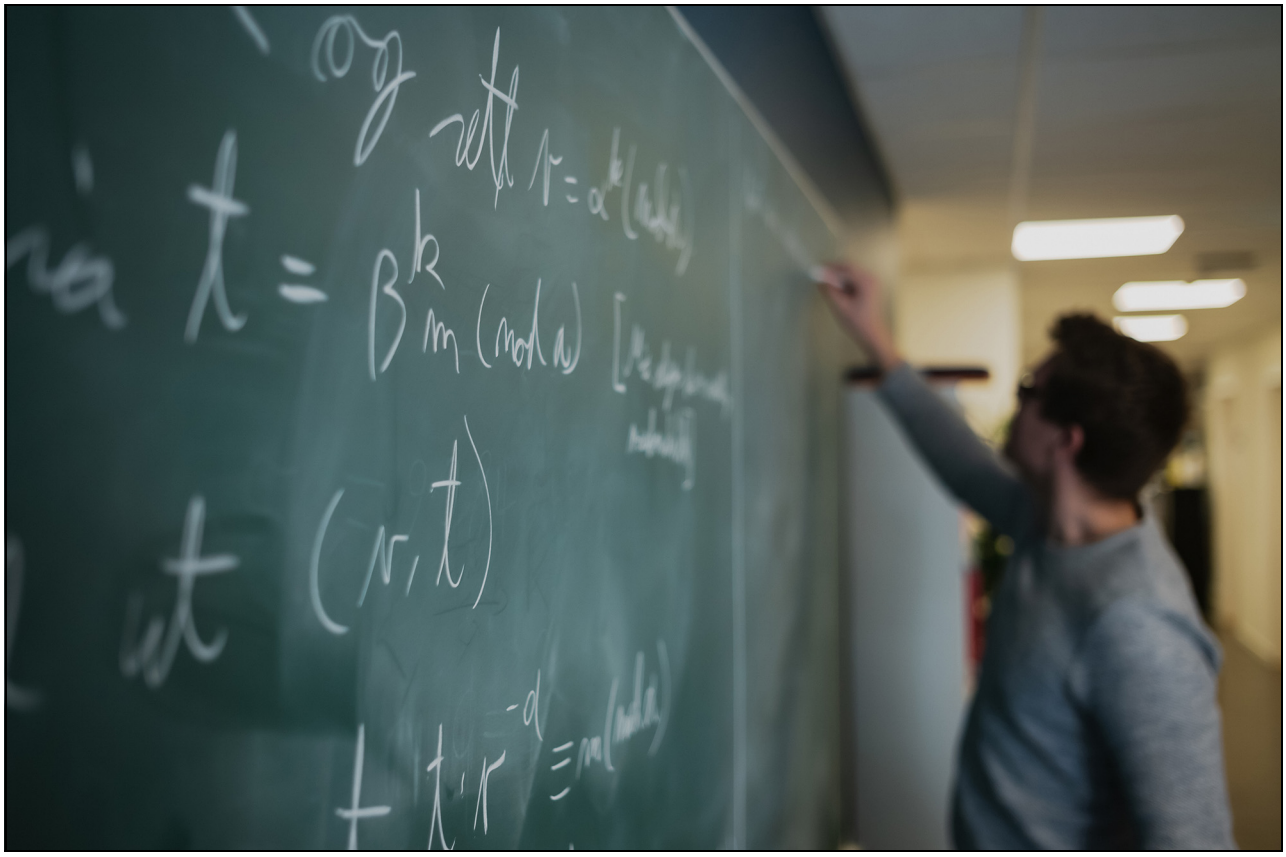

Figure 4.7 The NSM has researched crypto-analysis and secure cryptography for national security since the 1940s.

Photo: Norwegian National Security Authority

4.5.2 Bringing together expertise and capability building in various technology areas

Different technologies reinforce and interact with each other. Artificial intelligence, with the use of machine learning and big data, the Internet of Things, 5G/6G, the development of quantum technology and other ground-breaking technologies are examples of this. The use of new technologies in security areas will increase, and the balance between offensive and defensive capabilities will be challenged and constantly find new forms.

An example of this is that complex telecommunication infrastructure will increasingly be controlled by automatic analysis based on artificial intelligence. This technology enables self-repairing networks with a very short time for reconfiguration after an incident, but at the same time, it opens an arena for new and advanced attacks. Telecommunications companies have control over how and to what extent this is to be introduced, and the Electronic Communications Act requires an appropriate level of security.

Another example is quantum technology. Quantum computers will be able to solve certain types of complicated tasks that are unsolvable with today's classic computers. It is likely just a question of time before quantum computers will be able to crack some of the most common encryption mechanisms currently in use.

In addition, technological developments, such as the Internet of Things, show that it will be possible to include sensors and network connectivity to many, if not most, of the objects which surround us. Close international cooperation is an important arena for standardisation and necessary regulation.

Even if it is difficult to know the results of this technological development, the consequences will likely be significant. The government will monitor developments and contribute to ensuring that there is good and robust Norwegian expertise within the various technology areas.

4.6 The High North

The High North is Norway's most strategically important area, and the government will give new impetus to the High North policy. The government wishes to emphasise cooperation with other countries, and the increased activity on land in Norway. It is important for the government to ensure Norwegian ownership of important infrastructure and properties, and national control of natural resources in the High North.

At the same time, foreign intelligence activities in the High North can weaken Norwegian authorities' scope of action. The greatest threat is still from Russian and Chinese intelligence agencies. It is expected that Russian intelligence services will continue their mapping of civilian and military infrastructure in the region, while China and Chinese actors will continue to prioritise their long-term positioning in the High North, including for future resource extraction. State means for contributing to national security in the High North should be assessed in light of the region's strategical significance. Properties, infrastructure, natural resources and companies of importance to national security should therefore be individually assessed with regard to their geographical location along the coast, in border regions and near important infrastructure.

Larger towns and many coastal areas in Northern Norway have good demographic development. However, there are also sparsely-populated areas and large distances where the population is decreasing and where big changes in the population's demographic constitution are occurring.[7] The less central municipalities and the smallest municipalities in terms of population are facing the largest challenges. This includes in particular recruiting labour and providing services. These challenges are greatest in Nord-Troms and Finnmark.

Given the High North's strategic location and significance, these development trends may have consequences for the municipalities, and for the state's handling of unwanted incidents that can threaten national security. This in itself represents a vulnerability, in that the municipalities are more dependent on private investment to carry out legally required tasks and ensure citizens' welfare. Municipalities can lack sufficient expertise and experience to be able to handle and assess cases of importance to national security, such as setting up Russian war memorials, foreign property acquisitions or certain forms of tourism.

Vibrant and viable civilian society in Northern Norway, especially in the east of Finnmark, is an important part of Norwegian security. Securing Norwegian settlement in the areas close to Russia's border helps to underpin Norwegian sovereignty and Norwegian interests in the region.

---

[7] 'Regional development trends 2021', Report, Ministry of Local Government and Regional Development.

Figure 4.8 Svalbard has high strategic significance for Norway's scope of action in the High North and the Arctic.

Photo: Shutterstock

Through Prop. 78 S (2021–2022), the government has strengthened the ability of the intelligence and security services and the police to prevent security-threatening activities, especially in our three northernmost counties.

Svalbard

Svalbard is of great strategic importance for Norway's scope of action in the High North and the Arctic, and Svalbard policy is therefore an important part of the High North Policy of the government. National control contributes to achieving the objectives set by the Storting in regard to Svalbard policy. There is a substantial tradition of overarching political consensus regarding the core patterns of Svalbard policy, the objectives of which having been fixed for a long period of time:

- Consistent and firm enforcement of sovereignty
- Proper observance to the Svalbard Treaty and control to ensure compliance with the treaty
- Maintenance of peace and stability in the area
- Preservation of the area's distinctive natural wilderness
- Maintenance of Norwegian communities in the archipelago

The government's central policy instruments for societal development in Svalbard are the comprehensive white papers to the Storting regarding Svalbard, legislation, economic policy instruments, various forms of ownership, including property, land and infrastructure, as well as strategies. The objectives of Svalbard policy necessitate that regulations and other relevant frameworks for Svalbard are assessed and adapted in accordance with observed patterns of societal development.

Voting rights and state ownership

Certain policy instruments are utilised in Svalbard that are not utilised on the mainland. This is in part a consequence of the fact that certain sections of Norwegian legislation are not applicable to Svalbard, including the Immigration Act. In recent years there has been an increased influx of people to Longyearbyen directly from foreign countries. Longyearbyen Community Council is the locally elected municipal body for Longyearbyen, administering assets as well as functions of national significance. Persons elected to the Council must have a good knowledge of the objectives of Svalbard policy and the special framework conditions for Svalbard. Consequently, a require-

ment that foreign nationals have at least three years of residence in a municipality on the mainland to be able to vote and stand for election in Longyearbyen has been introduced.

State ownership is another policy instrument utilised on Svalbard. The government owns several companies in Svalbard, either directly or indirectly. Store Norske Spitsbergen Kulkompani AS (SNSK), Kings Bay AS, Bjørnøen AS and The University Centre in Svalbard AS are all companies directly owned by the state. The rationale for state ownership of these companies is in part contributing to the objectives of Svalbard policy outlined above.

The government is also a large landowner in Svalbard. Government owned property includes all the land in and around Longyearbyen. In 2016, the government purchased the property Austre Adventfjord near Longyearbyen. In total, the government direct ownership amounts to 98.75% of the land on Svalbard.

Direct state ownership of companies, state ownership of land and Norwegian legislation provide a solid basis for managing Svalbard for the good of the public.

5 Economic and administrative consequences

Preventive national security work aims to increase security in society. Security and security measures can be costly, and the proposed measures in this report could entail political and financial costs for the Norwegian society. However, the lack of appropriate level of security can have huge societal and economic consequences. Measures must therefore be understandable and proportionate, and must be used in such a way that they contribute to predictability and trust, balance various considerations and also contribute to safeguarding national security.

Significant parts of national security work, and work with cyber security, take place in each individual sector, based on the Security Act and relevant sector legislation, as well as specific requirements and recommendations for cyber security work. The security work must be an integrated part of ordinary management. If the risk and threat picture changes, it is important that the measures and policy apparatus are adjusted accordingly. It follows from the Security Act that cost-benefit assessments must be made before security measures are decided. The government aims to strengthen national security in several central areas. This report refers to a number of measures. Any expenditure that exceeds the current budget framework will be returned to by the government in connection with annual budget proposals.

Ministry of Justice and Public Security

r e c o m m e n d e d :

Recommendation from the Ministry of Justice and Public Security, National control and cyber resilience to safeguard national security, sent to the Storting on 9th December 2022.

Published by:
Norwegian Ministry of Justice and Public Security

Additional copies may be ordered from:
Norwegian Government Security and Service Organisation
www.publikasjoner.dep.no
Telephone: + 47 22 24 00 00
Publications are also available on:
www.government.no

Illustration: Konsis

Print: Norwegian Government Security
and Service Organisation 12/2023 – Impression 200