The Ministry of Justice and Public Security

Report to the Storting (white paper) No. 38

(2016–2017)

Report to the Storting (white paper)

Cyber Security

A joint responsibility

The Ministry of Justice and Public Security

Report to the Storting (white paper) No. 38

(2016–2017)

Report to the Storting (white paper)

Cyber Security

A joint responsibility

Recommendation by the Ministry of Justice and Public Security of 9 June 2017, approved in the Council of State on the same date. (The Solberg Government)

Figure 1.1

Illustration: M. Sylstad, NSM.

Image obtained from Colourbox.

Part I
Introduction

1 Summary

This is the first white paper on cyber security. There are several reasons why so much attention has been devoted to cyber security. Digital development is an essential part of our value creation and growth. Digitization has contributed to a safer and more secure society. It is easier for people to communicate with each other and gain fast access to information. Digitization has also altered the nature of societal vulnerability. Today, no sectors and few nations can control their digital vulnerability on their own. The Digital Vulnerability Committee (the Lysne Committee)[1] points out that Norway is at the forefront of digitization, which means that we as a society face vulnerability challenges early on.

Threat assessments show that foreign states are willing to use various means of gaining access to sensitive and confidential information and influencing political, economic and administrative decisions. There are major financial losses due to cybercrime. In addition, computer systems have been known to fail due to human error, software and equipment failures, natural events or a combination of these.

To ensure improved efficiency through increased digitalisation of the Norwegian society, computer systems and digital services must be adequately secure and reliable. Businesses and individuals must be confident that systems and networks function as intended and protect the privacy of the individual. Good cyber security and the capability to detect and manage unwanted cyber threats are a prerequisite for gaining this trust.

Cyberspace is developing rapidly and the challenges are transboundary - across countries, sectors and businesses. Hybrid threats erase the traditional divide between peace and war and challenge the traditional division of responsibilities between the civil and military sector. Therefore, the Government wants to strengthen cooperation between private and public businesses, between the civil and military sectors and across national borders. At national level, the Ministry of Justice and Public Security, the Ministry of Defence and the Ministry of Foreign Affairs will strengthen their cooperation in this area.

The Lysne Committee presents a number of recommendations to reduce digital vulnerabilities in the society. This white paper provides an overview of the status of the follow-up of the committee’s recommendations. The status overview shows that there is a need to work in parallel with a wide range of areas within cyber security. Our society will never be able to be fully protected against failure of or attacks against the digital infrastructure and systems, but we must be able to implement the correct security measures to reduce the risk and to be able to restore normal function as soon as possible. The Ministry of Justice and Public Security will use the overview to follow-up the ministries in the future work on national cyber security.

[1] NOU 2015: 13 *Digital vulnerability – secure society.*

The status overview is a central knowledge base for the Government's future work. The Government will emphasise comprehensive and systematic work on preventive cyber security. A key measure will be to appoint a committee to consider cyber security regulation. The committee will assess the need for and possibly propose a national Cyber Security Act, among other things, with scope outside the Security Act. The committee will also consider organisational issues. In addition to this, the Government will establish and develop strategic forums to discuss issues related to national cyber security and international cooperation, forums which also support public-private cooperation.

The Government is committed to strengthening national capability to detect and manage cyber attacks. Furthermore, the Government wants to facilitate good information sharing and management through a national framework for cyber incident management. The Norwegian Ministry of Justice and Public Security has initiated work to improve the cooperation and flow of information related to cyber incident management in Norway. Furthermore, coordination between the Intelligence Service, the National Security Authority (NSM), the Norwegian Police Security Service (PST) and the police has been strengthened.

The Government will facilitate long-term development of cyber security competence through a national cyber security competence strategy. Cyber security applies to everyone. By ensuring that young people learn early on the importance of secure use and understand the need for cyber security, the coming generations carry cyber security competence with them into their future education and working life.

Our society consists of a number of critical societal functions that must be maintained at all times in the interest of society and the fundamental needs of the population. These functions require an ICT infrastructure that works almost everywhere and all the time. The Government is committed to ensuring that we as a society have a secure and reliable ICT infrastructure. One of the main recommendations of the Lysne Committee was to reduce dependence on Telenor's core infrastructure. The Government is implementing regulatory and financial measures to make the electronic communication networks more robust in line with the development in threats and the technical development, and have in Meld. St. 33 (2016–2017) *National Transport Plan 2018–2029* prioritized funds to establish a pilot for an alternative core infrastructure.

2 Background, frameworks and the contents of the report

Meld. St. 10 (2016–2017) *Risk in a safe and secure society* was presented to the Storting in December 2016. In the white paper, cyber security is highlighted as one of the Government's key areas within public security. The white paper places special emphasis on comprehensive and systematic work on preventive cyber security measures and our capability to detect and manage cyber attacks. Furthermore, emphasis is placed on society's need for good cyber security competence at all levels and a secure and reliable ICT infrastructure. In Meld. St. 27 (2015–2016) *Digital agenda for Norway*, cyber security and privacy are one of the main priorities of the Government's ICT policy.

Recently, several analyses on digital vulnerabilities have been prepared. They contribute to public education and awareness, but also to provide the authorities and business leaders with a decision-making basis to draw up policies and measures to reduce vulnerabilities.

A key knowledge base is Norwegian Official Report (NOU) 2015: 13 *Digital vulnerability - secure society* (the Lysne Committee). The Committee assessed digital vulnerabilities at several levels - both at overall social level and in technical infrastructures and systems. The Lysne Committee presented a number of recommendations to reduce digital vulnerabilities in the society and in critical societal functions. The report was presented to the Minister of Justice and Public Security on 30 November 2015.

Part III of this white paper provides an overview of the status of the authorities' assessment and follow-up of the Lysne Committee's recommendations and an overview of the priorities in the future follow-up work. The Ministry of Justice and Public Security will use the status overview to follow-up the ministries in the civil sector in the future work on national cyber security.

The status overview in Part III shows that there is a need for a broad approach to the work on cyber security in the future. Several sectors face similar types of challenges, such as developing expertise on cyber security or dealing with a serious cyber incident. Based on the assessments in Part III, together with the existing knowledge base, development features and challenges in the area, the Government will emphasise selected cross-sectoral areas. The Government believes that these areas are of particular importance for national cyber security.

- Preventive cyber security - businesses' own abilities
- Detecting and managing cyber attacks
- Cyber security competence
- Critical ICT infrastructure

The Government's emphasised areas and measures to improve cyber security are described in Part II. To succeed in these areas, the Government is committed to strengthening public-private, international and civil-military cooperation, which is discussed in more detail in Chapter 5.

In addition to the measures presented in this report, the Government is following-up NOU 2016: 19 *Cooperation for security*. Compared with the applicable Security Act, the proposals in this white paper will be able to enhance national cyber security in many ways. Several businesses outside the public sector are subject to the law. Businesses covered by the Act are obliged to provide an adequate level of security for all information systems critical to fundamental national functions. For further information, see section 6.1.

3 Trends and the importance of cyber security

There are high expectations that digital services are provided and available at all times, while also being robust and able to withstand threats and risks. Failure or a security breach may occur in a combination of different circumstances. These may be intentional acts and attempts at improper use, as well as human error, equipment failures or unclear responsibility. Competence is a key factor in handling demanding and complex incidents. The demand for cyber security competence has increased.

Many challenges related to cyber security develop faster than public and private businesses are able to respond. In the years to come, we will face ever-increasing and more complex security challenges. ICT infrastructure and systems are becoming more global, comprehensive and integrated. An increasing number of devices are connected to the internet. There is more widespread use of cloud solutions in private homes and in the workplace. The need to cut costs and have access to expertise means that more ICT functions are outsourced to third parties, particularly in low-cost countries. This trend creates dependency and vulnerabilities across sectors, areas of responsibility and national borders.

Threat assessments show that foreign states are willing to employ a variety of means to gain access to sensitive and confidential information and to influence political, economic and administrative processes and decisions. The same means are also used by national and international criminals. Cyberspace, in combination with the information access, also creates opportunities for influence operations, to an extent and impact we have never seen before.

Cyber security comprises the full range of digital vulnerabilities. Cyber security includes technical and administrative security measures and the protection of ICT systems and the information in these. Therefore, cyber security is about the protection of "everything" that is vulnerable because it is connected to or otherwise dependent on ICT. The term cyber security is used in this white paper synonymously with the term cyber security.

Integrity, confidentiality and availability are important security goals when it comes to maintaining cyber security:[2]

- Confidentiality means not disclosing information to unauthorised persons, and that only authorised persons have access to the information.
- Integrity means that the information and the information processing are complete, accurate and valid and a result of authorised and controlled activities.
- Availability means that a service meets certain requirements for stability, so that relevant information is available when needed.

Businesses will prioritise the various goals differently depending on the purpose the business has or will support, and the requirements and risk to which it must relate. A means of achieving the security goals is traceability, in order to know who has accessed the systems, and who has handled or changed information. Traceability is becoming increasingly important given the trends related to influence operations and other undesirable cyber incidents.

Good cyber security is necessary for everyday life to function well. Services such as bank, commerce and health have been transferred to digital platforms. Most businesses rely on digital services in their production of goods and services.

4 Cyber security and privacy

Protection of privacy is an important part of the right to respect for a private life – a fundamental human right protected in both the Constitution, the European Convention on Human Rights and the UN Convention on Civil and Political rights. NOU 2009: 1 *Individual and integrity – Privacy in the digital society* (the Norwegian Privacy Commission) defined privacy as follows:

> *Privacy concerns safeguarding personal integrity; safeguarding individuals' opportunity for a private life, autonomy and self-expression.*

[2] *Cyber Security Strategy for Norway*, 2012.

The Lysne Committee pointed out that in a digital context, the protection of personal data plays a particularly important role in privacy. The Privacy Commission defines the term as follows:

> *Protection of personal information concerns rules and standards for processing personal data that has safeguarding privacy as its main objective. The purpose of the rules is to ensure individuals an overview and control of processing of data about themselves. With certain exceptions, individuals should be able to decide what others should know about his or her personal circumstances.*

It is the authorities' responsibility to safeguard human rights and to provide security and safety for the population. Protecting privacy and maintaining a secure society are therefore prioritised tasks for the Government.

Good cyber security is a prerequisite for safeguarding privacy. In national and international regulations on protection of personal data there are therefore provisions on cyber security. In its consultation statement on the Lysne Committee's report, the Norwegian Data Protection Authority writes that privacy and cyber security concerns often go hand in hand, and that they find it difficult to see good privacy without good security mechanisms in today's digital age. Protection of privacy and cyber security are fundamentally linked. When it comes to the implementation of specific security measures, such as logging in ICT systems, there may still be need for balancing between the two considerations.

Protection of privacy is a prerequisite for successful digitalisation in the society. Efficient use of ICT strengthens business competitiveness and increases the society's overall productivity.[3] The Government wants to use these advantages to facilitate further digitalisation of society. We must then be aware of the challenges of digitalisation. Among the major challenges is safeguarding privacy, which through digitalisation is constantly put to the test. Protection of privacy is key to the users having trust in digital solutions.

While there is increasing emphasis on privacy, we are seeing different kinds of voluntary abandonment of such protection. For example, private individuals providing personal data in exchange for free services. Free e-mail, search engines, games and social media have been based on this model. Most mobile phones send information on the user's movements, residence, work address and personal tasks. The use and processing of these data are therefore important both in a privacy and an cyber security perspective. Those who collect and process personal data have a responsibility to ensure that the data are not misused or lost.

[3] Meld. St. 27 (2015–2016) *Digital agenda for Norway*.

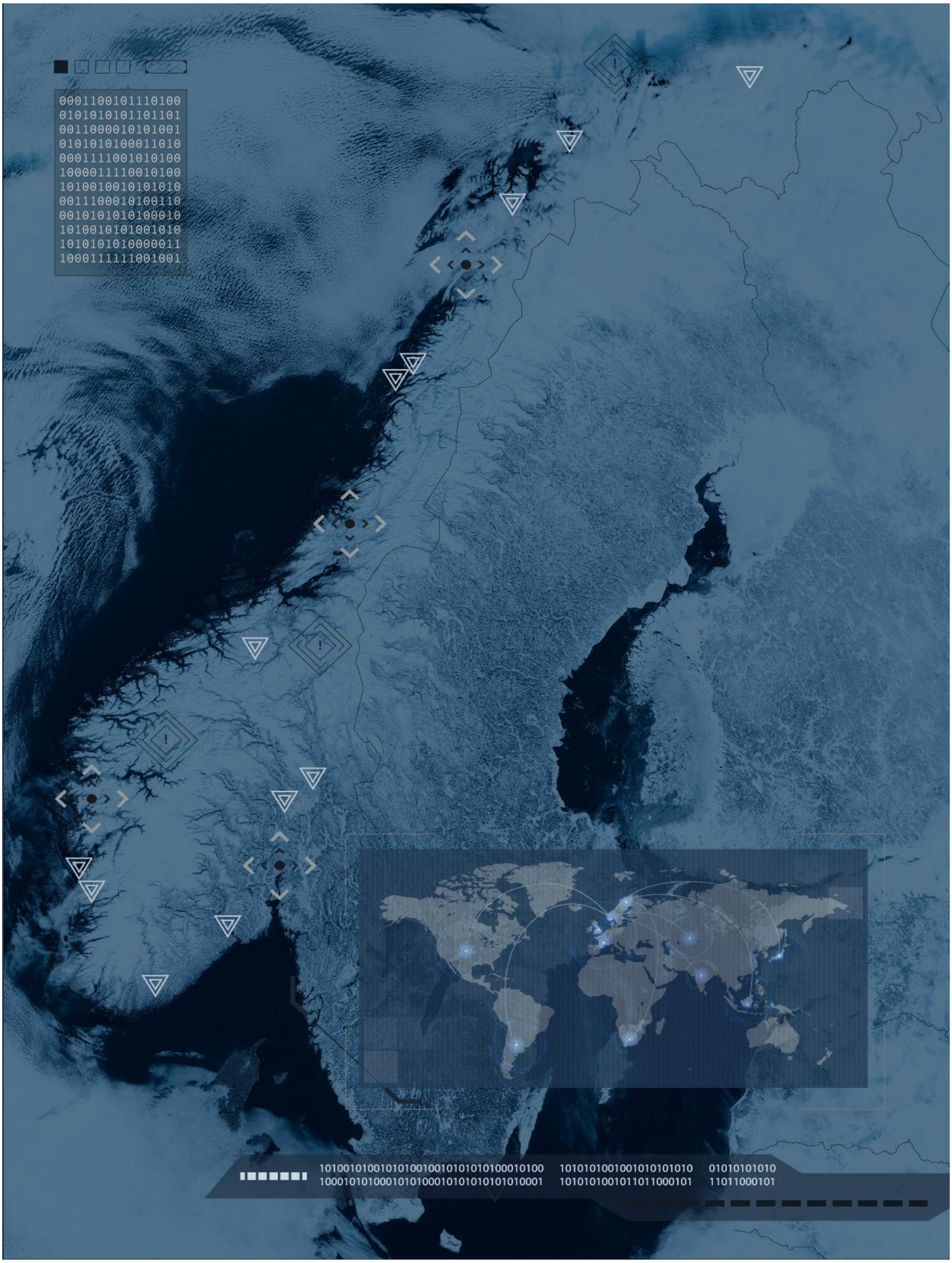

Figure 5.1

Illustration: M. Sylstad, NSM.

Image obtained from Visible Earth/NASA.

Part II

Key areas – Cyber security

5 A joint responsibility

ICT is primarily a responsibility at company level. Each cabinet minister has an overarching responsibility to maintain cyber security in his or her own sector. The Ministry of Justice and Public Security has a coordinating responsibility for cyber security in the civil sector. The Ministry will outline the Government's policy for cyber security, including national cyber security requirements and recommendations for public and private businesses. Affected ministries, authorities and industries will be involved in this work. Requirements will, if necessary, be sanctioned by laws and regulations. Responsibility for cyber security is described further in section 6.4 of Meld. St. 10 (2016–2017) *Risk in a safe and secure society,* and in the Royal Decree of 10 March 2017[4].

As pointed out in Meld. St. 10 (2016–2017), individuals and businesses have a responsibility for how their own actions may affect the security of others. This also applies within cyber security.

Society's dependence on ICT requires close cooperation between private and public companies, across national borders and between civil and military sectors. At national level the Ministry of Defence, the Ministry of Foreign Affairs and the Ministry of Justice and Public Security will strengthen their cooperation in this area.

Meld. St. 10 (2016–2017) states that the Government will prepare a new national cyber security strategy. In addition, an action plan with specific measures will be drawn up. The work will be led by the Ministry of Justice and Public Security and the Ministry of Defence. This white paper to the Storting will constitute an important platform for the forthcoming strategy. The new strategy will have a broader approach to the challenges than previous national strategies in this area. Strengthened cooperation between the Ministry of Justice and Public Security, the Ministry of Defence and the Ministry of Foreign Affairs and the need to strengthen civil-military, public-private and international cooperation will be emphasised.

The Government will develop the Information Security Network[5] to ensure that strategic issues related to cyber security in Norway and internationally are discussed and coordinated. This will be a key tool for the Ministry of Justice and Public Security's coordinating responsibility for cyber security in the civil sector, for the Ministry of Defence in civil-military issues related to national cyber security and for the Ministry of Foreign Affairs in their coordinating role in foreign policy issues related to cyberspace.

[4] *Responsibility for public security in the civil sector at national level and the Ministry of Justice and Public Security's coordination role within public and cyber security.*

[5] Information security network is a meeting place for the ministries to discuss key topics within information security. It is also a tool for the Ministry of Justice and Public Security's coordinating responsibility for cyber security in the civil sector.

Key measures:

- prepare a national strategy for cyber security, including an action plan
- establish a forum for public-private cooperation to support the national work on cyber security
- develop the Information Security Network to ensure that strategic issues related to cyber security in Norway and internationally are discussed and coordinated.
- further develop the Norwegian total defence concept and increase resilience of critical societal functions, for instance within robust communication systems.

5.1 Public-private cooperation

Neither the authorities, the industry and nor citizens can face the challenges in the cyberspace on their own. The public and private sector have different capacities, knowledge and expertise that can complement each other, despite different business goals. There is already significant public-private cooperation to prevent, detect and manage cyber incidents. Strengthened cooperation between the authorities and the private sector could contribute to better understanding of the situation, better decisions and improved access to more resources that can complement each other.

The Government wants to establish a forum for public-private cooperation to support the national work on cyber security. Participants in the forum will be relevant representatives from the authorities, industry and commerce, academia and interest groups. These will primarily be owners or managers of critical infrastructure or societal functions, or key cyber security stakeholders. The forum should be able to propose measures and provide advice to the authorities.

In the work on a new national cyber security strategy, the Government wants broad involvement of public and private stakeholders. The public-private cooperation forum will participate in the work on the forthcoming national ICT strategy.

5.2 International cooperation

International cooperation is crucial for the development of global guidelines and to reduce and combat threats in cyberspace. Norway has self-interest in having good and predictable guidelines in cyberspace. We also have a fundamental and long-term interest of having a secure, robust, open and free cyberspace. It is therefore important for Norway to be involved in drawing up the international guidelines that form this space. This includes the development of norms for government action, international cooperation to combat cybercrime and international cooperation on enhanced cyber security.

However, the evolution of the internet and digital services and product development are primarily being driven by private companies and research and development institutions. In addition, the backbone of the internet, the global digital infrastructure, is mainly privately owned. This contributes to competition, continued innovation and development. At the same time, it means that key decisions about cyberspace are largely being made by commercial and non-state actors outside traditional intergovernmental arenas. This trend indicates a greater need for public-private and international cooperation.

Meld. St. 37 (2014–2015) *Global security challenges in foreign policy* points out a sharp increase in cybercrime when connecting several developing countries to the internet. In many countries preventive cyber security is not a priority or good enough. Norway may play an important role by assisting with capacity building in developing countries, so that more countries have the capability to manage digital challenges and threats. The white paper to the Storting also proposes several other measures for the foreign policy work, including drawing up an international cyber strategy for Norway. The strategy will clarify the Government's overarching goals within the full range of international policy for cyberspace, where cyber security is one of several elements.

The development and implementation of EU's strategy for a digital inner market will have great importance for Norway through the EEA. The three pillars of the strategy are 1) better access for consumers and businesses to online goods and services across Europe, 2) creating the right conditions for digital network and services to flourish and 3) maximising the growth potential of our European Digital Economy.

Cyber security is part of pillar 2, where two of the measures are to work to strengthen the cyber security industry and integrate security at an early stage of technology development. The third and most comprehensive measure is to adopt and implement the EU Directive on network and information system security (the NIS Directive). The Directive imposes cyber security requirements on the member states, on businesses that provide services essential to the internal market's social and economic activities, and on providers of certain digital services. Norway has been invited to join several cooperation forums on the implementation of the Directive. The Ministry of Justice and Public Security represents Norway in these forums. For more about the NIS Directive see section 22.5.

The EU Agency for Network and Information Security (ENISA) develops general recommendations within cyber security, contributes to the development of regulations and guidelines and cooperates with operational units in Europe. Norway participates in ENISA without voting rights. Implementation of the NIS Directive will strengthen the Agency by assigning it the role of a hub for the network of national authorities established by the Directive. Norwegian participation in ENISA will therefore be even more important than it is today.

As part of the mid-term review of the digital internal market strategy, in May 2017 the EU Commission presented its plan to revise the cyber security strategy from 2013. At the same time, ENISA will be evaluated. The evaluation paves the way for a possible audit of the Agency.

International cooperation on cyber security also takes place in other international forums and in inter-governmental organisations such as NATO, OECD and the UN, but also in cooperation with industry and commerce, academia and society as a whole. See the discussion of NATO under section 5.3. The Government will participate and contribute actively to solve global challenges related to cyber security.

5.3 Civil-military cooperation

A changed security policy situation, combined with hybrid[6] threats, makes civil-military cooperation in cyberspace more relevant than ever before. The military and civilian sector use to an increasing extent a common ICT infrastructure and services are purchased by commercial stakeholders. This means that they also have common digital vulnerabilities. Good cooperation between civilian and military authorities is crucial.

The modernised Norwegian total defence concept includes mutual support and cooperation between the Armed Forces and the civilian society. The fundamental idea of total defence is that the whole of society's resources should, if necessary, be capable of being used in defence of the country, to deal with immediate or imminent threats to public safety in peacetime, security crises and war situations. It is no longer a prerequisite that the emergency legislation enters into force for it to be said that the support can be said to be within the scope of the Norwegian total defence concept.[7]

In November 2016, the Government decided that the Ministry of Justice and Public Security will establish a programme for further development of the Norwegian total defence concept and increase the resilience of essential functions. The reason for implementing this work is NATO's expectations for member states to strengthen the robustness of essential functions, adopted by NATO in February 2016.[8]

NATO places greater emphasis than previously on civil preparedness and civil-military cooperation. The reason is that civil preparedness, crisis management and robust critical social functions are a prerequisite for each country's and thus the alliance's, overall preparedness and defence. A robust and accessible ICT infrastructure is necessary to maintain all critical social functions and is an input factor in NATO's fundamental expectations for the member states.

In 2016, Norway signed a revised cooperation agreement with NATO on protection against cyber threats. The agreement ensures information sharing between the stakeholders which improves Norway and NATO's capability to protect ICT systems against cyber attacks.

NATO's Heads of State and prime ministers signed a joint cyber declaration under the NATO summit in the summer of 2016. It is important for NATO and the member states to work for increased cyber security across sectors in society and between countries. Norway must follow-up the obligations contained in the cyber declaration.

6 Preventive cyber security – businesses' own abilities

The Government is committed to facilitating that businesses can improve their own ability to prevent cyber incidents. The answer to the challenges does not only involve greater resources or

[6] Hybrid threats and instruments are understood to be actors' use of economic, political and military means to exploit vulnerab ilities to achieve something, such as to create unrest in a society. The actors may be state-sponsered or non-state-sponsored. In 2017, DSB will develop a scenario based on hybrid threats in its annual report "Crisis Scenarios".

[7] *Support and cooperation - A description of the total defence today* (the Government 2015).

[8] For more information, go to http://www.nato.int/cps/en/ natohq/topics_49158.htm?selectedLocale=en.

strengthening capacity. Appropriate regulations and organisation are also key in protecting our assets.

Businesses rely on complex digital value chains, and the vulnerability of others becomes their own vulnerability. It is necessary for businesses to have a sufficient overview of their own vulnerability. A good overview enables the enterprise to assess appropriate measures.

Key measures:

- set up a committee to assess legal regulation of the cyber security area and organisation of cross-sectoral responsibility
- facilitate so that businesses can assess and prioritise cyber security measures through systematization and development of recommendations and requirements
- develop and maintain a sound and accessible knowledge base that enables individuals, businesses and authorities to implement the correct measures to maintain adequate security in their ICT systems.

6.1 Legal regulation in the area of cyber security

Meld. St. 10 (2016–2017) *Risk in a safe and secure society* points out that Norwegian businesses must relate to different regulations relating to cyber security. Some regulations are sector specific, while others are cross-sectoral. The regulations have different purposes and considerations and often use different concepts and methods. The rapid digitalisation of society has meant that regulations and legislation are not always adapted to today's needs.

In recent years, digitalisation has contributed to far more cross-sectoral challenges. Several of these challenges are related to security issues. There may be a different understanding of the threat and risk situation in the sectors and an inadequate overview of how security in their own sector may also have consequences for other sectors. This may lead to fragmented regulation and lack of comprehensive thinking when formulating cyber security requirements, which also makes it challenging for the businesses to keep track of and comply with the various requirements.

The EU NIS Directive requires the member states to provide a minimum level of national cyber security. The Directive will ensure that each member state has a unified and cross-sectoral approach to cyber security. There is a possibility for various solutions in different countries for most sectors.

The current Personal Data Act has cross-sectoral provisions on cyber security. The EU's new Data Protection Directive sets out requirements for cyber security.

In NOU 2016: 19 *Cooperation on security* the Committee proposes improved systematics for the regulation of preventive national security (see box 6.1). The Committee proposes an extended scope and extent in relation to the current security legislation.

Box 6.1 The Security Committee's assessments

Through a sectoral identification of important social functions, businesses and infrastructures, a national and cross-sectoral security authority should be able to gain a comprehensive overview of our national security situation. The Committee also proposes that the businesses are required to protect their critical information systems. This will include everything from processing systems, office support systems and pure communication systems to control and management systems. The proposed bill obliges businesses covered by the law to implement security logging and authorises implementation of intrusion testing. Overall, the Act will help to improve national cyber security and thus reduce our total digital vulnerabilities. Furthermore, the systematics will improve the security authority's possibility to have a comprehensive and national overview of vulnerabilities, including the digital and other challenges. This will in turn form the basis for working purposefully to reduce our vulnerabilities.

There is a need to assess whether the current legal regulation of national cyber security is appropriately arranged. The Government will set up a committee to identify relevant sector-specific and cross-sectoral regulations within cyber security. It will be assessed whether existing regulations are consistent, and address the new digital societal challenges. It will be assessed whether there is a need for harmonisation of the existing legislation. Furthermore, the committee will investigate the need for and possibly propose a national cyber security Act. The report will be limited to provisions, organisation and authority that follow from the Security Act and proposed new Security Act.

6.2 Organisation of cross-sectoral responsibility

In connection with the report on legal regulation of the area of cyber security (see section 6.1), the Government will also investigate organisational circumstances, which as cross-sectoral coordination, advice, supervision, notification of incidents and the preparation of security requirements.

Digitalisation has a greater degree of dependence and connection between public and private, civilian and military and between different sectors of society. The threat and vulnerability situation changes quickly at the same time as the society becomes increasingly more complex. This creates several challenges for the authorities, including in terms of expertise and resources.

Utilisation of community resources must be optimised to achieve good cyber security. The committee will assess whether responsibility, roles and tasks are appropriately distributed and organised between agencies with cross-sectoral responsibility in the area of cyber security. The committee will also examine the possibilities for coordination, cooperation and synergies between the public and private sector so that national cyber security is maintained and strengthened.

6.3 Systematization and development of recommendations and requirements

The authorities come with a number of recommendations and requirements in the area of cyber security. There is significant systematic and good work in progress on implementing these (see box 6.2 on follow-up of national requirements and recommendations in cyber security at the Ministry of Climate and Environment). However, it may be demanding for businesses to relate to the scope of recommendations and requirements. Therefore, through the forthcoming action plan for national cyber security strategy, the Government will facilitate so that businesses can more easily assess and prioritise cyber security measures based on the size and maturity level of the business.[9]

[9] For further discussion of the new national cyber security strategy, see Meld. St. 10 (2016–2017) *Risk in a safe and secure society*.

Box 6.2 An example of follow-up of national requirements and recommendtions within cyber security

The Ministry of Climate and Environment has drawn up a long-term plan to reduce ICT vulnerability in the sector. In the ministry's ICT strategy for 2016-2020, emphasis was placed on increasing cyber security in the sector. Specific measures have been put in place to meet the objectives of the strategy. These measures include establishing a common environment for ICT operations. National Security Authority (NSM) has called for fewer ICT environments in the public sector, i.a. in the National Security Advice 2015.

The Ministry of Local Government and Modernisation, in cooperation with the Ministry of Justice and Public Security, assess how the cyber security work in the public sector should be further developed. Key recommendations from *Action plan for information security in the public sector (2015–2017)* will be incorporated into the forthcoming action plan for the national cyber security strategy.

In 2017, NSM has begun the work on establishing a guideline for cyber security, based on recognised standards and defined basic principles. The framework will be further developed to reflect changes in technology and risks. The purpose is to establish a set of key measures for securing ICT solutions of social importance. This work will be an important basis for the Government's forthcoming action plan, and together with the framework for cyber incident management (see section 7.2) will provide uniformity in the work on cyber security in Norway.

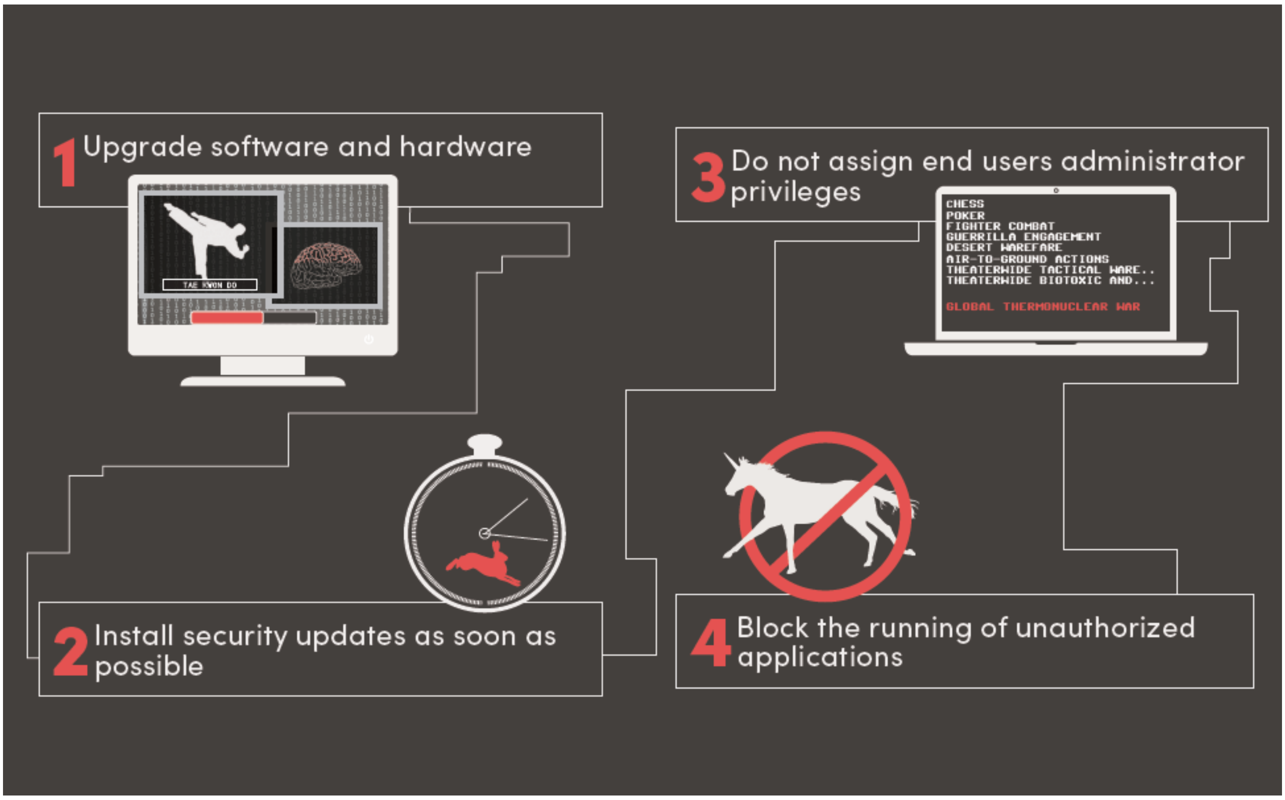
1 Upgrade software and hardware
TAE KWON DO
3 Do not assign end users administrator privileges
CHESS
POKER
FIGHTER COMBAT
GUERRILLA ENGAGEMENT
DESERT WAREFARE
AIR-TO-GROUND ACTIONS
THEATERWIDE TACTICAL WARE..
THEATERWIDE BIOTOXIC AND...
GLOBAL THERMONUCLEAR WAR
2 Install security updates as soon as possible
4 Block the running of unauthorized applications

Figure 6.1 Measures against cyber attacks.

Illustration: M. Sylstad, NSM.

In 2017, NSM will also establish an arena for transfer of experience so that public and private businesses will to a greater extent receive coordinated, adapted and appropriate advice and guidance in the area of cyber security. The Government will continue to support the Norwegian Centre for Information Security (NorSIS) (see box 6.3) in its work. NorSIS is an important contributor that provides advice and guidance to small and medium-sized businesses and creates greater awareness in the population about cyber security challenges.

Box 6.3 NorSIS

NorSIS is an independent organisation that works to increase knowledge about and understanding of cyber security. NorSIS receives funding from the Ministry of Justice and Public Security and is a part of the authorities' national commitment to cyber security.

An important task for NorSIS is to provide advice and guidance to the public, companies and public businesses. The largest single initiative is "National Security Month", which is held in October each year. The Security Month is a national exercise to create awareness about information security that is relevant to businesses and individuals. In 2016, 420,000 employees had access to e-learning during the Security Month. This is an increase of almost 60,000 from 2015. In addition, a number of security-related lectures were held throughout Norway.

NorSIS has prepared several guidelines intended for private businesses. NorSIS cooperates with NSM and Nkom on nettvett.no. This is a service where you can find information, advice and guidance on safer use of the internet. The information is aimed at consumers and small and medium-sized businesses. The purpose of the services is to provide a more uniform and coordinated flow of information on security and security culture related to ICT. NorSIS operates and has editorial responsibility for the service, while NSM and Nkom contribute to further development and funding.

6.4 Outsourcing

Many businesses choose to acquire ICT services from one or more external providers instead of producing them themselves. The services may be provided internally in the enterprise or externally by national or international providers. There may also be combinations of these.

Outsourcing of ICT services to professional providers could provide improved security and more stable and available services. It can also provide lower and more predictable costs and contribute to better prioritisation of core business areas. This requires the enterprise to have the expertise to follow-up the providers. At the same time, the enterprise must be aware of the assets that are exposed through outsourcing and implement the necessary measures. The need for confidentiality, integrity and accessibility should be particularly emphasised in the assessments, and which laws, requirements and regulations apply to the sector nationally and internationally.

There are currently few cloud providers with facilities in Norway. Therefore, outsourcing using cloud services involves storage and processing primarily being carried out at the cloud providers' facilities outside Norway and thus outside national control. A more detailed discussion of outsourcing and cloud services is found in section 22.10. See box 6.4 for ICT outsourcing in the health service.

Box 6.4 Outsourcing ICT in the health service

The health service relies on private service providers to develop and introduce solutions and provide service, maintenance and operation.

Inadequate procedures and risk assessments were discovered while South-Eastern Norway Regional Health Authority was in the process of outsourcing operation of its ICT infrastructure to an international provider. Outsourcing to external system operators requires control measures and risk and vulnerability analyses to ensure that personal data processing requirements are met.

The Ministry of Health and Care Services will therefore initiate work to examine information security management when using private sub-contractors in the health sector.

The Government wants businesses to be aware when outsourcing ICT services and to follow national advice and recommendations. Several guidelines have been prepared by the Norwegian Data Protection Authority, the Directorate for Administration and ICT (Difi), the Directorate for eHealth, NorSIS and Uninett, among others, to help businesses that are considering outsourcing. NSM will also prepare a report on outsourcing in 2017.

6.5 Intrusion tests

Identification and attempts at intrusion take place continuously towards devices connected to the internet. Intrusion testing is an efficient tool to identify vulnerabilities and test the resilience of ICT systems. This is done through targeted search, analysis and attempted exploitation of vulnerabilities, faults and defects. Vulnerabilities in infrastructure connected to the internet may also be detected by using mapping tools, such as Allvis NOR (see box 6.5).

Box 6.5 Allvis NOR

National states, organisations and private individuals identify vulnerabilities from the internet. In Norway, the general public were made aware of this phenomenon through daily newspaper Dagbladet’s series of articles on “Zero CTRL” in 2013/2014.

Since then NSM has established a similar mapping service, Allvis NOR. Allvis NOR searches through affiliated businesses’ internet-exposed ICT interfaces to detect vulnerable or incorrectly configured services and equipment, so that the enterprise itself can reduce its vulnerabilities. The service is consent-based. Allvis NOR was further developed to be able to detect the specific vulnerability that was used by the ransom virus referred to as “WannaCry” in May 2017. NSM experienced an increased demand for the service during this incident.

Allvis NOR provides the authorities with insight into the state of the public sector in Norway’s internet security and ensures that the development can be monitored over time. Allvis NOR will be a useful supplement to ordinary intrusion testing and will help improve basis security in society.

The Ministry of Justice and Public Security recommends use of intrusion tests. A number of businesses have followed the recommendation, and in most cases have revealed serious vulnerabilities and helped them to be dealt with.

Enterprises subject to the Security Act may request NSM for assistance. NSM has implemented such tests in the Ministry of Justice and Public Security, the Ministry of Defence and the Ministry of Foreign Affairs, among others. Other businesses may use private companies to carry out the testing. Different sectors may also build up their own expertise to carry out tests, such as Norsk Helsenett SF has done. Systematic implementation and follow-up of such tests could reduce the vulnerability of the businesses' systems and make them more resilient to cyber attacks.

The Government encourages businesses critical to society to use intrusion tests to identify vulnerabilities and test the resilience of own ICT systems.

6.6 Knowledge base

Recently, several analyses on digital vulnerabilities have been produced. These serve several purposes. They contribute to public education and awareness, and provide the authorities and business leaders with a basis for decision-making to draw up policies and measures to reduce vulnerabilities.

In 2015, NSM prepared its first *Comprehensive ICT risks* report. The report is published annually. The purpose of the reports is to provide a common status of the situation which enables businesses and authorities to make the right decisions. In addition, it provides a tool for businesses in their work on preparing risk assessments. NSM has been commissioned to develop the report in cooperation with other relevant businesses.

Examples of other analyses are NorSIS' annual report on threats and trends. The report shows security challenges to which individuals and society as a whole must relate. In addition, annual analyses are prepared by the Police Security Service, the Intelligence Service, Kripos, the Directorate for Civil Protection and Emergency Planning (DSB), the Financial Supervisory Authority and the National Communications Authority (Nkom). Different sectors and businesses' risk analyses, evaluations following exercises and incidents, research in the field and private industry assessments contribute to the overall overview. The analyses have a somewhat different approach and target groups, but a common theme is that the challenges in the field of cyber security are usually cross-sectoral.

The Government will develop, maintain and support a sound and accessible knowledge base that enables individuals, businesses and authorities to take appropriate measures.

6.7 Culture and leadership

In Meld. St. 10 (2016–2017) *Risk in a safe and secure society* the Government points out the importance of culture, management and attitude to public security in Norway. How we relate to risk, and how well prepared we are for a serious incident, is affected by our attitudes and the culture of which we are a part. This applies in particular to cyber security. Security was easier to assess when what was being secured was something physical, tangible and stable. Lockable cabinets and physical obstacles are easy to understand. In the digital world you can soon become alienated in terms of security. We no longer have the same overview of the vulnerability situation. A cyber attack will often not be visible to anyone affected. The need for increased awareness about vulnerability and security threats, as well as increasing the expertise of the individual, is becoming increasingly more relevant.

Good security management in the businesses lays the foundation for satisfactory protection of assets. Management commitment to information security as well as commitment through the allocation of resources to secure information and information systems is important. All protection starts with a valuation - what input factors and assets are important for our enterprise, business partners, society as a whole, etc. Structured value and risk assessments provide an overview of assets and to what extent these are exposed to risk. The assessments are both a management tool - what must be done to achieve a satisfactory security level - and they contribute to risk recognition in the businesses.

The Government will work to make a general improvement in the security culture in businesses and society as a whole through competence-enhancing measures and improved risk recognition.

6.8 Privacy and preventive cyber security

When implementing security measures, the potential impact of the measure on privacy must be considered. If the measure has an impact on privacy, national and international regulations set forth requirements for implementation of the measures. NOU 2016: 19 *Cooperation for security* describes the relationship between preventive security and privacy. The Committee listed five items with the principles and guidelines that were used as a basis for the work on considering a new legislation for preventive national security. The list may also serve as a basis for the cyber security work:

- precision in the formulation of the legal authority for the security measure (the statutory requirement)
- assess the impact of the security measure on existing measures (the purposefulness)
- assess the proportionality between the security effect and how much the measures intervene in privacy and legal protection (proportionality)
- consider alternative and lower level of intervention that may give the same effect (the principle subsidiarity)
- establish adequate privacy or guarantee of due process where there is intervention in the individual’s legal sphere (procedural mechanisms)

As stated under section 6.5, intrusion testing is considered a sound cyber security measure. Many ICT systems process personal data. This is an example of a security measure where the principles must be used before implementation, and where security considerations must be weighed against privacy considerations.

7 Detecting and managing cyber attacks

The Government is committed to strengthening our national capability to detect and manage cyber attacks. Cyber attacks may be difficult to detect and in extreme circumstances may pose a threat to national interests and violation of Norwegian sovereignty. The victims may be other states, organised non-governmental groups and private legal persons. The goal of the attackers may be crime for profit, blackmailing or destroying or changing information or functionality. It may also be to acquire information on state and trade secrets, research findings or technological innovations from commercial companies. The problems are often global, and the risk of punishment and consequences is low.

Viewed from a state and public security perspective, the greatest threat is the perpetrators who have the resources to carry out actions that we do not detect, which are detected too late, which can cause damage to critical infrastructure, or which may affect democratic processes. In this category we often find government parties, particularly other countries' security and intelligence services.

One challenge may be that there is uncertainty and inadequate coordination between government agencies responsible for combating serious cyber attacks. Therefore, the Government is committed to facilitating cooperation and sharing information.

Key measures:

- further develop the national warning system for digital infrastructure (VDI) to increase the ability to detect cyber attacks.
- establish and further develop a national framework for cyber incident management that leads to more efficient management and improved cooperation between parties.
- establish information sharing work to improve cooperation between public and private businesses during cyber incidents and establish a technical platform for sharing information.
- report on and clarify how a type of digital border defence can be established and regulated by law.
- increase police capability to combat crime in the digital landscape.
- increase the national capability to withstand serious cyber attacks through further development of cooperation been the Intelligence Service, NSM, PST and the police in general.
- improve NSM's ability to analyse serious cyber attacks against infrastructure and information critical for society.

7.1 The warning system for digital infrastructure

The ability to detect and manage cyber attacks depends on cooperation between authorities, sector CERTs and public and private businesses. NSM operates the national response function for serious cyber attacks against critical infrastructure and is responsible for organising and operating the national warning system for digital infrastructure (VDI). VDI is a network of sensors located in public and private businesses that own critical infrastructure. Information from the sensors contributes to a national capability for early detection and verification of coordinated and targeted attacks. The Government wants to upgrade the sensor technology in VDI.[10]

In Prop. 97 L (2015–2016) *Amendments to the Security Act*, the Government presented a proposal to legislate the activities currently carried out by NSM through NorCERT and VDI. When discussing Innst. 352 L (2015–2016) the Storting decided that NSM should be responsible for a national response function and a warning system for digital infrastructure. In connection with this, the Government also considered whether a legal basis should be established to be able to order certain businesses with critical infrastructure to connect to VDI. Based on the feedback from the consultation bodies, the Government concluded that such an order had to be investigated further and seen in context with an assessment of the future funding model for NorCERT and VDI.

[10] Prop. 151 S (2015–2016) *Long-term plan for the defence sector*.

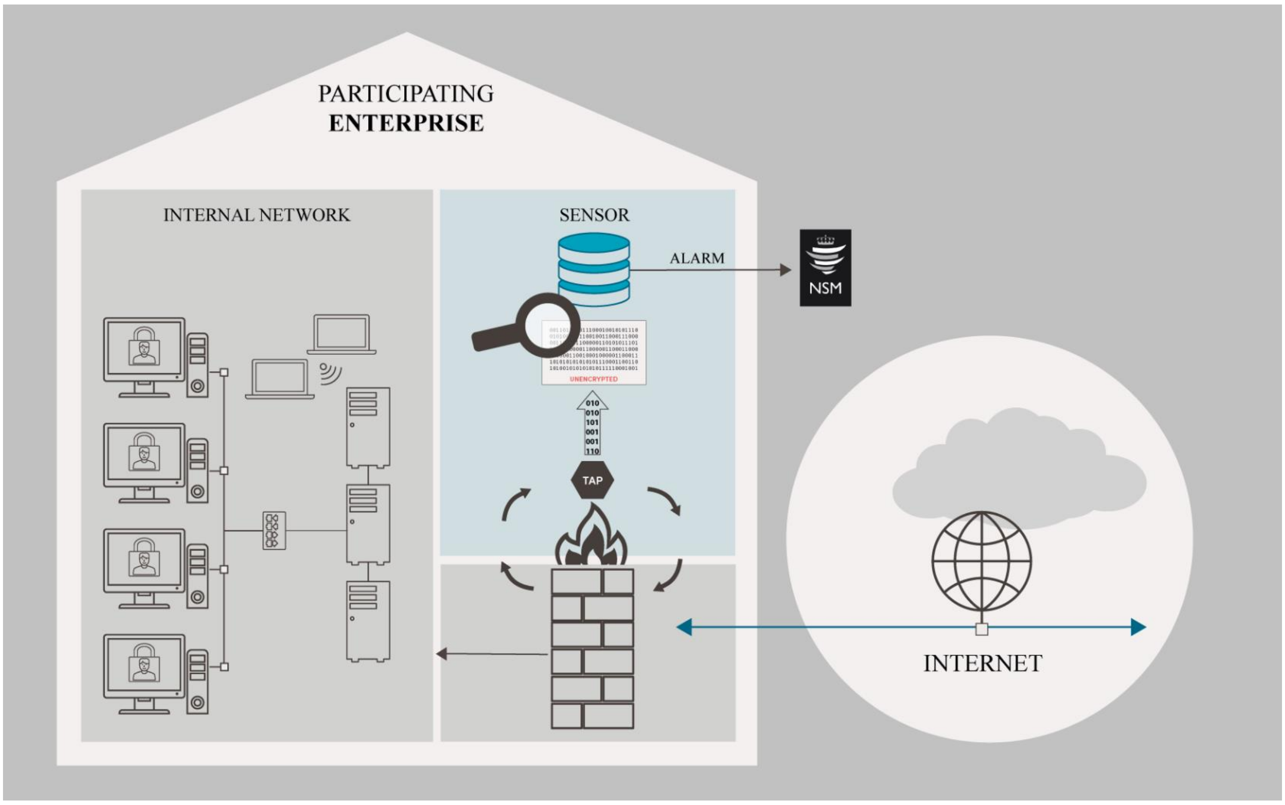

Figure 7.1 The warning system for digital infrastructure (VDI).

Illustration: M. Sylstad, NSM.

7.2 Framework for cyber incident management

The Government is committed to strengthening cooperation between different parties to manage serious cyber attacks. The Government has decided to establish a national framework for dealing with cyber incidents. An initial version of the framework will be completed in 2017 (see box 7.1). The framework describes the national structure of how Norway organises itself to manage cyber incidents. This will help relevant parties to effectively exercise their responsibility in a coordinate national response in the event of cyber attack. The framework will also describe early warning and information sharing procedures and establish a homogeneous system of concepts. The correct information to the right time is crucial for companies to prevent, detect and manage cyber incidents, and to make sure they have a proper picture of the situation. Information sharing between businesses, CERTs, ministries and NSM is crucial to this.

Box 7.1 National framework for cyber incident management

The framework will contribute to

- clarify responsibilities and roles for the government and other key parties in cyber incident management
- communicate what public and private businesses must be prepared to deal with themselves, and what kind of support and coordination they can expect from the National Security Authority (NSM)

- clarify and strengthen the frameworks for cooperation between businesses, sector CERTs, NSM, the Intelligence Service, PST and the police in general.
- further develop the ability to share relevant information and report cyber attacks
- clarify points of contact with other countries and organisations

To ensure that all relevant parties receive the correct warning information and are enabled to take the necessary action, the government has decided to establish sectoral CERTs. The CERTs will have an overview of their own sector, be the information hub for all relevant businesses and be the sector's link with NSM. Sectoral CERTs are a key prerequisite in the framework for national incident management. Sectoral CERTs are discussed several places in part III.

A draft framework was used during the national "IKT16" exercise in November 2016. Experience from the exercise is now being used in the work of completing the framework (see the overview of preliminary findings in box 7.2).

In the event of failure of critical social functions due to a cyber attack, there will be a need for crisis management at community level by a number of players, such as emergency preparedness agencies, local authorities or voluntary organisations, similar to other incidents affecting critical societal functions.

Box 7.2 Preliminary findings from the "IKT16" exercise

The purpose of the "IKT16" exercise was to put Norway in a better position to manage a major cross-sectoral cyber attack. Learning was prioritised in the planning, implementation and follow-up of the exercise. DSB led the work on the exercise.

Some of the preliminary findings from the exercise:

- The National Framework for Digital Event Management provides a good basis for dealing with a coordinated response to a cyber attack.
- There is a clarification need for what to expect between businesses related to information sharing and situation report.
- NSM’s unclassified national situation report was an important source of information.
- There is different organisation and maturity level in the sector CERTs. It is important to include different environments in a coordinated national response in the further development of the framework.
- There is a need for clarification of roles and responsibilities between the businesses’ ICT environments and emergency preparedness environments. Both types of environment must be involved in the crisis management and it is crucial that they cooperate well.

The final evaluation report will be available in 2017.

7.3 Information sharing

Information sharing is essential for detecting and dealing with cyber attacks. This has potential for improvement and was a key topic in the Lysne Committee's report. The Committee meant there was untapped potential for information sharing. Therefore, NSM has initiated work to improve the cooperation and flow of information related to cyber incident management in Norway. The purpose of the work is to ensure that assessment of cyber attacks can be made across sectors, and to ensure two-way exchange of information and coordination between NSM and various CERTs. The Government is particularly keen to achieve good public-private cooperation in the field, and relevant parties from the public and private sector will therefore be involved in the work. The work will also examine how information and cooperation may be improved beyond the businesses currently included in the national framework for cyber incident management.

NSM has also implemented several measures related to information sharing. NSM gathers CERTs sector-by-sector each month for a review of cyber incidents, as well as discussion of development needs and policy clarifications for the cooperation. A weekly video conference is also held with the CERTs in the various sectors. One of the goals is to unite all these CERTs in a joint reporting format.

NSM has produced an unclassified national situation report, available via a portal with a login option for CERTs in the various sectors and national decision-makers. The purpose is to be able to share information quickly and securely. The portal was tested during the "IKT16" exercise, and the experience showed that the portal was an important source of information. In the spring of 2017, the portal was operational on an unclassified platform, and NSM is considering the possibilities to develop a similar portal on classified communication platforms. In 2017, NSM will also develop solutions for automatic sharing of warnings and technical information with CERTs in the different sectors. NSM exchanges weekly reports with the Nordic countries’ CERT functions.

7.4 Digital border defence

The challenges of detecting cyber attacks also affect the issue of digital border defence in Norway. In 2016, the Ministry of Defence set up a committee (Lysne II) to investigate the principal aspects of granting the Intelligence Service access to digital communication in and out of Norway. The report points out the trends in society that highlight the need for new intelligence methods that monitor cross-border data transfer. Almost all the traffic has moved from radio and satellite to digital signals in cables. The Intelligence Service currently has no systems to control cross-border digital communication, and it has little or no access to the information in the communication cables.

The Committee presented its report on 26th August 2016 and recommended introduction of a digital border defence with a clear framework and very strict control mechanisms to protection of privacy. A number of parties have been involved in the public debate, and conflicting views have been aired in a comprehensive consultation round.

The Government believes that there is a need to strengthen Norway's capability to protect itself against external threats in and through use of cyberspace, and that there is a need to establish some kind of digital border defence. Therefore, the Government will consider and clarify how a digital border defence can be established and regulated. In such an investigation, it will be crucial to find a balance between the security and intelligence impact a digital border defence may have, and the privacy related issues such access raises. The Government is aiming for a consultation paper with draft legislation to be sent for comments in 2018.

7.5 Cybercrime

Cybercrime is on the increase. Cybercrime is divided into crime targeting the ICT systems themselves, and criminal acts committed by using ICT.

Several reports show the need to strengthen police expertise and capacity in this field. In the police's own situation analysis from 2015, it is pointed out that technology is developing at such a fast pace that the police are constantly challenged. The development places new demands on the police's own task solving in terms of more expertise and new technology.

In 2015, the Ministry of Justice and Public Security drew up a strategy to combat cybercrime. This is the Ministry's first strategy document in the field, and it focuses on strengthening expertise and capacity, building knowledge, strengthening research and identifying technological needs and solutions.

One of the measures in the strategy is to establish a national centre to prevent and combat cybercrime. The Lysne Committee supported the proposal for a national centre with a special assistance function to support the police districts from a point of police tactics and prosecution. The National Police Directorate (POD) has drawn up a specific proposal for how to establish such a centre in the police to prevent and combat cybercrime, including the tasks that should be assigned to the centre, organisational anchorage and resource requirements. The proposal states that the police must allocate significant resources. For some functions, the need must be met through external recruitment of expertise that the police does not have today. Therefore, the proposal must be dealt with in the ordinary budget process, and assessed against other important initiatives.

The Government wants digital expertise to be established in all the police districts so that the police have sufficient prerequisites for combating cybercrime. In cyberspace, the police and the prosecuting authority also have fewer opportunities to arrest, prosecute and bring to trial. This means that the efforts of the police must to an increasing extent be aimed at preventive work, intelligence, detection, stopping and restoring a lawful situation by having presence in cyberspace.

The tools for handling digital tracks must be updated in line with the technological development, and the police investigation methods must keep pace with the criminals' use of modern technology. Police training must be strengthened so that the police have the necessary expertise. This applies to the basic training and the post-qualifying training and further education. Employees without police training, including specialists with a high level of technological expertise should receive supplementary police training. As of the Ministry of Justice and Public Security's strategy of 2015 to combat cybercrime, POD has drawn up its own strategy for digital skills enhancement.

The Government has also provided the police with important tools in the battle against serious crime through legislative amendments. In June 2016, based on Prop. 68 L (2015–2016) *Amendments to the Criminal Procedure Act, etc. (covert coercive measures)*, the Government granted the police extended access to use concealed coercive measures in investigation, avoidance and prevention of serious offences. This access included methods such as communication control, secret searching, electronic room surveillance, technical tracking and camera surveillance. The amendments entered into force on 17 June 2016. In addition, the use of a new concealed coercive measure in the form of data reading is allowed. These provisions entered into force on 9 September 2016. On 5 April

2017, the Government presented a proposal to the Storting on legislative amendments that will ensure the police access to mobile phones, tablets and other computer systems that are opened using a fingerprint scanner and other biometric authentication.

The reason for these legislative amendments and the proposals is a changed crime and threat situation and the technological development. The risk of terror has increased considerably, serious and organised crime is spreading, and encrypted communication is becoming increasingly more common. The police must have the necessary means to be able to protect the citizens and society efficiently in line with the requirements in section 2 of the Police Act, while taking due account of the citizens' protection against threats to general security.

On 18 May 2017, a government appointed committee presented its report on organisation and in police specialist units.[11] The Committee has considered future models, and in its assessment has placed great emphasis on the ability of the police to combat cybercrime. The report was submitted for wide consultation.

7.6 Coordination between NSM, the Intelligence Service, PST and the police

The Government emphasises the importance of close and good cooperation between NSM, the Intelligence Service, PST and the police. Rapid exchange of information and efficient mechanisms are needed to establish a common operational picture in the event of a cyber attack. This could help the necessary countermeasures to be identified and implemented as quickly as possible.

NSM, the Intelligence Service and PST have previously cooperated within the framework of the Cyber Coordination Group. The group had regular meetings and provided information and a decision-making basis for the operational and strategic management on threats and vulnerabilities in cyberspace. Kripos and the Cyber Defence participated in an extended part of this cooperation and the Cyber Coordination Group could be expanded with representatives from other relevant parties when required.

As described in Meld. St. 10 (2016–2017) *Risk in a safe and secure society* in the autumn of 2016, NSM, the Intelligence Service and PST were commissioned to establish a Common Cyber Coordination Centre as a further development of the Cyber Coordination Group.

The Joint Cyber Coordination Centre was established on 31 March 2017 as a permanent, co-located specialist unit with representatives from NSM, the Intelligence Service and PST. The centre will help increase the national capability to withstand serious cyber attacks and support strategic analysis products and maintain a "bigger picture" of threats and the risk in cyberspace. The centre is not an independent body with its own decision-making authority, and the establishment involves no changes in the legal basis, authority, roles or tasks. The information sharing that took place between the Cyber Coordination Group and the Norwegian Armed Forces is continued between the Common Coordination Centre and the Norwegian Armed Forces.

[11] NOU 2017: 11 *Better assistance Better preparedness. The future organisation of police specialist units.*

NSM, the Intelligence Service and PST have previously been commissioned to further improve cooperation and increased information sharing between the agencies and Kripos in dealing with cyber attacks and crime in cyberspace. The services and Kripos have proposed to the Ministry of Justice and Public Security and the Ministry of Defence that Kripos should also be involved as a permanent participant in the Common Cyber Coordination Centre. The proposal is being considered by the ministries.

7.7 Openness about cyber attacks

The Government seeks openness about cyber attacks. On behalf of the Ministry of Justice and Public Security, NSM has previously drawn up recommendations on how openness about cyber attacks should be considered. The guidelines were drawn up in cooperation with Difi, POD, NorSIS and the Norwegian Business and Industry Security Council.

Openness forms the basis for learning and helps enable the businesses to prevent, detect and manage incidents. This also provides businesses and the authorities with better prerequisites for understanding the challenges in cyberspace. At the same time, publication and information sharing is practised in such a way that the provisions relating to confidentiality are complied with and the advantages must be weighed against the possible negative consequences. The Government encourages public and private businesses to follow the recommendations on openness.

7.8 Analysis capacity

Serious cyber attacks have become more advanced and more difficult to detect. It is time-consuming and skills-intensive to conduct analyses of such attacks. Despite the businesses being better able to manage incidents, greater complexity of each incident has resulted in a significant demand for NSM's analytical competence. At the same time, NSM has limited analytical capacity to meet this demand. Therefore, the Government will strengthen the national capacity by improving NSM's capability to detect and analyse serious cyber attacks against critical infrastructure and information, cf. Prop. 151 S (2015–2016) *Fighting strength and sustainability*.

8 Cyber security competence

The Government wants to strengthen cyber security competence in Norway and ensure that expertise requirements for cyber security are addressed in society as a whole and in business and industry.

Cyber security competence is a scarce resource nationally and internationally. The need for more and better educated cyber security personnel has been emphasised both in the Lysne Committee's report, in Meld. St. 10 (2016–2017) *Risk in a safe and secure society* and in Meld. St. 27 (2015–2016) *Digital agenda for Norway*. In recent years, the Government has facilitated better education capacity and increased research on cyber security.

Key measures:

- establish a national cyber security competence strategy, where the need for student capacity and research efforts are considered
- through the commenced school reform in primary and secondary schools, consider whether cyber security has been adequately included in the basic digital expertise the pupils will acquire
- strengthen cyber security competence in supervisory institutions
- emphasise systematic follow-up and learning after exercises and incidents, including cyber incidents.

8.1 National strategy for cyber security competence

As stated in Meld. St. 10 (2016–2017), the Government will prepare a new national cyber security strategy. One of the aims of the strategy is to facilitate long-term building up of expertise. The strategy will deal with measures to strengthen the national capacity within research and education. It will also deal with awareness measures directed at the population and businesses.

Cyber security competence has previously been included in several different strategies, reports to the Storting and other documents, but this is the first time a strategy is developed that addresses the challenge of competence as a whole.

In order to provide sound knowledge as a basis for the forthcoming cyber security competence strategy, the Norwegian Institute for Studies in Innovation, Research and Education (NIFU) has been assigned the task of mapping the future needs for cyber security competence in working life (see box 8.1). The report prepared will help identify the gap between available competence and the demand for this competence.

Box 8.1 NIFU's competence study

NIFU has been mapping the number of students in cyber security programmes and ICT programmes with courses in cyber security in Norway in the period 2012-2016 and how many have graduated in the same period. The survey shows an increase in the number of students from 166 in 2012 to 358 in 2016 taking a study programme in cyber security and an increase from 1582 in 2012 to 2695 students in 2016 taking the study programme with courses in cyber security.

NIFU's project is still in an early phase, but a preliminary calculation shows that despite an expected steady increase in the number of people with advanced cyber security competence, the gap between supply and demand is increasing.

The Ministry of Justice and Public Security will be responsible for developing the strategy in cooperation with the Ministry of Education and Research, among others. To ensure good support, the Government will assume that relevant parties are involved in the work. The work on the competence strategy will also be seen in context with the need to increase ICT competence in general and advanced ICT competence in particular.[12]

[12] Meld. St. 27 (2015–2016) *Digital agenda for Norway*.

8.2 Primary, lower and upper secondary school education

Digital competence has become an important part of primary, lower and upper secondary education. In the development of the pupils' digital skills, in addition to the possibilities in the technology, it is also important to focus on safe and secure use. The pupils must understand the need to update software, making regular backups and the risks of uncritical use of downloaded software and online services.

The Government follows this up through Meld. St. 28 (2015–2016) *Subjects – Specialisation – Understanding – A renewal of Knowledge Promotion*. In the follow-up work, it will be considered whether cyber security has been adequately included in the basic digital expertise the pupils will acquire. Relevant curricula for upper secondary school education will also be considered in the follow-up of the report.

8.3 Higher education

To reduce the gap between supply and demand in the field of cyber security, it is crucial to educate sufficient people with relevant expertise.

In recent years, the Government has had a following-up on both Meld. St. 27 (2015–2016) and the Lysne Committee by earmarking more student capacity to ICT and cyber security. In the revised National Budget for 2015, 45 student places were earmarked for ICT and 200 student places for other technology and science subjects. In the budget for 2016, 100 student places were allocated to ICT. In the revised National Budget for 2016, 65 student places were earmarked cyber security and 135 student places were earmarked health and ICT education. For 2017, 500 student places for one year were earmarked ICT and when allocating the student places, the institutions were requested to take into account the need for cyber security.

An increasing number of educational institutions include topics on cyber security as part of general ICT programmes. It is also important that cyber security and privacy related issues are part of other education programmes, such as law, economics and management.

In recent years, there has been a significant increase in applications to ICT programmes. This contributes to increased competition for student places, which may result in improved quality and faster throughput. Seen over a longer perspective, the earmarked student places will result in a significant increase in the number of candidates with ICT and cyber security competence.

The Government will prepare a new national strategy for cyber security competence. The strategy will assess the need for university places, among other things.

Figure 8.1 Education.

Illustration: M. Sylstad, NSM.

Image taken from Colourbox.

8.4 Research

Norway is dependent on building outstanding and permanent research within cyber security. There are several good research environments for cyber security in Norway, such as the Norwegian Defence Research Establishment, NTNU Center for Cyber and Information Security (CCIS) in Gjøvik, Simula Research Laboratory and the universities of Oslo and Bergen.

The Research Council's programme IKTPLUSS and EU's programme Horizon 2020 fund most of the cyber security research in Norway today. The Government encourages industry and commerce and the public sector to be more involved in research, both as clients and as partners. Schemes such as Industrial PhD and Public Sector PhD have been established, but have the potential to be used more.

In the Ministry of Justice and Public Security's Research strategy for public security (2015-2019), secure digitization of society is a priority research topic. The strategy describes the partnership with research institutions as an important instrument. Increased contact between research, education, authorities and end users increases the possibility for mutual dialogue that can provide more relevant and useful research projects.

Through IKTPLUSS, the Government granted NOK 150 million to cyber security projects in 2015. These projects are now ongoing. The Government has also increased the number of posts for recruitment (post-doctoral and fellowship positions) to science and technology. In the National Budget 2017, 16 new posts for recruitment at universities, colleges and the institute sectors have been earmarked cyber security. In the Revised National Budget 2017, the Government proposed granting funds to a further 4 new posts for recruitment at NTNU. The recruitment posts go to CCIS in Gjøvik. New posts for recruitment will help strengthen research and knowledge about cyber security.

The Ministry of Justice and Public Security also funds research in the field of public safety in general. The greatest effort is in the research programme SAMRISK at the Research Council of Norway. One of the aims of the programme is to contribute to better resistance, prevention, preparedness, rescue work, crisis management and learning. SAMRISK is a cross-sectoral and interdisciplinary programme. The programme's activities are also seen in context with NordForsk's commitment to public security and EU's security research.

The Government will prepare a new national strategy for cyber security competence. The strategy will assess the need for research in the field.

8.5 Post-qualifying and further education

It is important to provide post-qualifying and further education to people who need cyber security competence in the workplace. Post-qualifying and further education may be organised flexibly, thus reaching many, such as through ICT supported, decentralised and session-based programmes. It is important that there is good contact between the providers and the clients when developing such courses, so that the programmes offered are in accordance with the labour market's needs.

The Government believes that in post-qualifying and further education that earn credits, there is a need for certification courses and other purposeful cyber security courses. If in the short term we want to have the possibility to raise ICT competence in society, there must be a wide range of courses adapted to the various users. This requires that educational institutions and course providers have sufficient capacity and courses, and that employers allocate resources so that employees can get post-qualifying and further education.

The Government encourages employers in the public and private sector to prioritise post-qualifying and further education of employees to build sufficient cyber security competence in the businesses.

8.6 Competence in supervisory institutions

Supervisory activities are instruments for the authorities to ensure compliance with regulations and requirements by the businesses. The technical development and continuous changes in the way ICT systems are used, supplied and operated requires greater cyber security competence among the supervisory authorities. The Lysne Committee points out this in its report. Today, there is potential for greater cooperation between the supervisory authorities on cyber security to improve expertise.

To improve cyber security and the quality of cyber security supervision conducted in the various sectors, the Ministry of Justice and Public Security and the Ministry of Defence will establish a common arena for the various sectors' key supervisory authorities. The purpose is to contribute to information sharing and transfer of competence and in this way increase the quality of the sectors' supervision of cyber security. NSM will lead the arena. See also section 22.7.

It is a goal that the supervisory authorities themselves will have greater expertise to conduct supervisory activities in the field of cyber security. NSM, together with the sectoral supervisory authorities, will considering providing a central capacity with cyber security competence that will be used as a resource for the supervisory authorities. This central capacity can assist people from the supervisory authorities. It may also be considered whether there are commercial services that can provide help in case of any lack of competence.

8.7 Exercises

Exercises are a useful tool for better prevention, detection and management of undesirable cyber incidents. All parties and businesses in charge of critical societal functions and that rely on having a functioning ICT infrastructure and services, have an individual responsibility for conducting exercises. Many large, national cross-sectoral exercises carried out on behalf of DSB have included digital vulnerabilities. Digital vulnerabilities were the main topic of the national "IKT16" exercise and in Nkom's national cyber exercise for the electronic communication and energy sector (NCEK 2015).

Several of the recommendations from the Lysne Committee highlight exercises as a means of reducing the digital vulnerability. In Part III of this report, exercises are described as important measures for several sectors when the status of the recommendations from the Lysne Committee is reviewed.

Learning from exercises is demanding. Meld. St. 10 (2016–2017) *Risk in a safe and secure society* emphasises the systematic follow-up and learning from exercises and incidents. The Government wants to learn as much as possible from exercises and incidents. Therefore, the Government will introduce new requirements for follow-up of findings from incidents and exercises in government administration in the civil sector.

All incidents and exercises will be evaluated. Findings and points of learning will be followed-up through a management-based action plan. Follow-up of exercises and incidents will not be considered completed until all the points of the action plan have been followed-up satisfactorily or signed off through a management-based assessment. The results of the follow-up of exercises and incidents over a certain size or severity will be reported to a superior authority.

The Ministry of Justice and Public Security, together with other relevant ministries, will place greater emphasis on also using international exercises to work on prevention and management of cyber incidents, particularly NATO-based exercises (see box 8.2 about NATO and exercises).

Box 8.2 NATO and exercises

NATO's Crisis Management Exercise improves the Alliance's strategic military-political level, in Allied capitals, and in NATO's organisation. The scenarios for the exercise vary from year to year between crisis management operations in peacetime and collective defence. Protection against cyber threats is usually among the elements of the exercise. Participants in the exercises, besides the NATO institutions and the member states, may be NATO partner countries and observers from humanitarian organisations and the EU. The exercise has been conducted annually since 1992

The target group of NATO's annual Cyber Coalition is the environments in NATO and the member states who will manage cyber incidents at operational and partly technical level. Cyber Coalition 2016 was the Alliance's largest exercise so far in this field, with participation from 27 NATO countries and partner countries besides participation from the EU, industrial players and academia. This exercise has been conducted since 2008.

9 Critical ICT infrastructure

Our society consists of a number of functions critical to society, such as energy supply, financial and satellite-based services. These are functions that must be maintained at all times in the interest of society and the population's fundamental needs. A number of these societal functions require that there is an ICT infrastructure that works almost everywhere and all the time.

ICT infrastructures consist of information and communication infrastructures (internet services, electronic communication networks, etc.) and information and communication systems that are part of the essential function.[13] These may include central management and control systems, as well as administrative and logistic systems.

Protection of critical ICT infrastructure is one of the main areas of the EU's ENISA agency. All EU member states are encouraged to prioritise this in their national cyber security strategies. NATO has civil preparedness and civil-military cooperation on the agenda to a greater extent than before. Civil preparedness, crisis management and robust essential functions are a prerequisite for each country's and thus the Alliance's, overall preparedness and defence.

The Government wants critical ICT infrastructure to be robust and reliable, so that undesired incidents are avoided as much as possible, while being able to quickly restore a normal situation following an undesired incident. We must also be able to ensure that no unauthorised person have access to the information communicated through such infrastructure. Protection of critical ICT infrastructure is vital in the work the Government is doing within cyber security. Part of this work is to participate in international arenas (see box 9.1 about Meridian).

Box 9.1 Meridian

Meridian is an annual international meeting place for government representatives who work on national policy-making related to protection of critical ICT infrastructure. The object of the conference is to exchange experiences from how to deal with national and global challenges.

Meridian has contributed to the preparation of the "Good Practice Guide on CIIP for governmental policy-makers". The guide provides a good overview of the steps to protect critical ICT infrastructure. It is intended to be particularly useful for countries initiating a process to identify and protect critical ICT infrastructure, but is also useful for countries that have advanced further in the field.

[13] The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers.

Norway will host the 13th conference in the series, which will be held in Oslo in October 2017.

The Lysne Committee highlights the national infrastructure for electronic communication as a key component of almost all digital value chains.[14] In line with the recommendations of the Lysne Committee and the Ministry of Transport and Communication's follow-up of the national electronic communication plan,[15] Nkom was commissioned to consider vulnerability-reducing measures related to the dependence of society and essential functions on Telenor's core infrastructure, and how different transport networks and international connections may be combined to improve the overall national capacity and security in the electronic communication networks. In the report *Robust and Secure National Transport Networks - Visions and Vulnerability Measures* from April 2017, Nkom follows-up the assignment and explains the current situation, anticipated development in the market and what policy and budget measures are required to improve the security of the Norwegian electronic communication networks. The report is an important knowledge base for the Government's future work in the area.

In addition, businesses responsible for essential functions that rely heavily on electronic communication must consider their own measures that may reduce the risk for loss of communication.

Key measures:

- priority funding for establishment of a pilot for an alternative core infrastructure, cf. Meld. St. 33 (2016–2017) National Transport Plan 2018–2029
- continued work on developing possible government measures that may help to facilitate more fibre cables abroad
- work for strong communication protection in Norway

9.1 Alternative core infrastructure and robustness in the regional transport networks

Development of a Norwegian electronic communication network is mainly funded and operated by commercial developers who choose their own development strategy and develop their own services and business models. The Government and the electronic communication providers are currently implementing measures to strengthen the security and robustness of the Norwegian electronic communication networks. In Norway today only Telenor provides a national core interface solely based on its own infrastructure. Other key transmission providers depend on Telenor or partners to provide an infrastructure with similar capacity, coverage, robustness and independence. Even though Telenor's core infrastructure is developed and operated with a very high degree of security, and over time has shown high reliability, the dependence on one single party's network represents a vulnerability that should be dealt with. The Government wants Norway to have a strong and robust electronic communication network, and is committed to reducing this vulnerability.

[14] See also the scenario about "Cyber attacks on electronic communication infrastructure", National risk situation (DSB 2014). The scenario shows the dependence of essential functions on the electronic communication infrastructure.

[15] Meld. St. 27 (2015–2016) *Digital agenda for Norway*.

In Meld. St. 33 (2016–2017) *National Transport Plan 2018–2029* allocated funds to establishment of a pilot programme for an alternative core infrastructure in 2018-2021. The pilot programme will demonstrate the security needs and the commercial basis for investment in a core infrastructure that competes with Telenor's network. The objective of the pilot programme is to establish a functioning market for alternative core infrastructures aimed at critical businesses and other users.

To achieve the pilot programme's objective, and in the long run to facilitate a fully-fledged alternative to Telenor’s transport infrastructure, Nkom believes that it is relevant to look closer at the following categories of measures:[16]

- Altibox, Broadnet and Telenor reserve dark fibre/wave length by each other in particularly exposed stretches to strengthen own robustness
- Government support to new fibre cables in strategically important areas in cooperation with Telenor, Broadnet, Altibox, the Norwegian Armed Forces (North–South, Western Norway, Finnmark)
- Government support facilitating additional redundancy and provider diversity in the transport network part of the mobile networks.

Nkom’s assessment is that there is a need to establish more coherent fibre connections in key areas between the different regions of the country that are important for national preparedness and security. The measures are delineated against investments that the providers must do themselves in order to provide a proper electronic communication infrastructure to their users. The Government will work together with the electronic communication providers to link together particularly important stretches of the existing fibre network.

9.2 International connections

In 2016, Nkom delivered a report[17] on access to fibre infrastructure in Norway and delivery roads abroad. The report shows that there is good access to alternative fibre feeds in most parts of the country, but not everywhere. The report also shows that most of the international traffic is routed via the Oslo area and abroad through Sweden.

Established transmission providers have so far not wanted to change the current traffic management out of the country. The providers show limited interest or willingness to use new delivery roads abroad. The Government will continue to work on development of possible state measures that may help facilitate more fibre cables out of the country.

9.3 Emergency and preparedness communication

Emergency and preparedness prosecutors rely on good and secure communication solutions in their daily work and in crisis situations. The Norwegian Emergency Public Safety Network serves a good solution for secured voice communication.

[16] Nkom, 2017, *Robust and secure national transport infrastructure – Visions and vulnerability-reducing measures*.

[17] Nkom, 2016, *Mapping and assessment of infrastructure that may be used by data centres*.

The needs of the emergency and preparedness services, including data, may require new solutions. Both the technological development and the development of the threat situation point to the fact that the emergency and preparedness services will need mobile broadband solutions with a high degree of security and robustness. This will require significant involvement and resources from the Government to realise a future solution of secure and robust mobile broadband services for the emergency services. The State must take responsibility for facilitating satisfactory frameworks and services for this purpose, regardless of whether the needs are to be realised through the commercial electronic communication networks, through a separate network for emergency and preparedness services or through a combination of these solutions.

Through the National Electronic Communication Plan, the Government has expressed an objective that the public electronic communication networks should as far as possible be able to carry future services for the emergency and preparedness services. The Government has also decided that frequency resources in the 700 MHz band will be used for mobile services when they are available in the future. Nkom is in dialogue with DSB and the Norwegian Defence Material Agency on relevant problems and needs, and different options are considered against socio-economic cost/benefit. cyber security considerations such as integrity, confidentiality and availability and special functionality for this user group are important assessment topics.

9.4 Cyber security in management and control systems

Many of the important societal functions require round-the-clock operation of automatic management and control systems. The technology used is a mixture of the usual ICT equipment and specialised computers (automation equipment). Part III describes such social functions in the chapters on energy supply, oil and gas, water supply and transport. This equipment has many of the same vulnerabilities as the usual ICT equipment, but it is more vulnerable because of the need for round-the-clock operation and that it is used in businesses that do not necessarily have a robust ICT department.

The management systems themselves rarely need to be connected to the individual company’s data network, but such connection is usually established because there is a desire to be able to carry out maintenance or troubleshooting, or to use operating data for reporting and maintenance management. This link means that the vulnerabilities in the management systems are exposed. Enterprises must be aware of how management and control systems are secured and followed-up, and they should cooperate to increase knowledge within the field.

Figure 9.1 Management systems.

Illustration: M. Sylstad, NSM.

Image obtained from Colourbox.

9.5 Privacy and critical ICT infrastructure – communications protection

Communications protection as a concept includes legal and actual protection of information in transit, en route from one place to another. The concept also includes information about such information or communication, so-called meta data. Communications protection is usually regarded as part of the wider concept of privacy, as it is difficult to image efficient privacy without the communication between two or more parties being confidential.

Use of electronic communication provides information about a variety of circumstances that affect the individual's private sphere and personal integrity, such as geographical movement, contact network, etc. The pressure to obtain access to this type of data also increases as the commercial use of so-called big data increases. Today's communications protection in Norway is good, but new technology, new services and business models challenge these regulations.

The electronic communication services are produced to an increasing extent in data centres outside Norwegian territory. Norwegian legislation is therefore not always sufficient to safeguard the privacy and communications protection of each user in Norway. The Government wants Norway to continue to work internationally to promote good solutions that protect Norwegian users.

Figure 10.1

Illustration: M. Sylstad, NSM.

Image obtained from Colourbox.

Part III
Follow-up of the Lysne Committee's recommendations

10 Electronic communication

10.1 Reduce the criticality of Telenor's core infrastructure

Problem description (NOU 2015: 13, section 11.7.1)

Telenor's core infrastructure is a component of virtually all digital value chains. Therefore, an outage in this infrastructure has serious and simultaneous consequences in most areas of society, and for the essential functions discussed in this report. Telenor's core infrastructure is well-developed, professionally operated and historically has very high stability. Nevertheless, it could be paralysed by human error, failure to follow procedures, sabotage, terror or disloyal personnel. In the view of the committee, the sum of the social values this network carries is unacceptably high. Therefore, the committee will recommend working towards goals where at least one additional player has a nationwide core infrastructure at thee same level as Telenor's with respect to coverage, route diversity, redundancy and independence. The Lysne Committee's report estimates the costs of establishing an alternative core infrastructure to be NOK 575 million.

Status of measures

The Committee's assessments of the criticality of Telenor's core infrastructure are receiving a lot of support in the consultation round. In Meld. St. 33 (2016–2017) *National Transport Plan 2018–2029*, the government has given priority of funds to the establishment of a pilot project for an alternative core infrastructure from 2018-2021. The pilot programme will demonstrate the security needs and the commercial basis for investment in a core infrastructure that competes with Telenor's infrastructure. Reference is made to the discussion of the status of the measure under section 9.1.

10.2 Ensure diversity among the suppliers of the infrastructure

Problem description (NOU 2015: 13, section 11.7.2)

Efforts should be made to have controlled heterogeneity among equipment suppliers in the Norwegian electronic communication infrastructure. The National Communications Authority (Nkom) should, in consultation with the Norwegian Competition Authority, take the initiative to investigate whether we currently have sufficient policy instruments to address this or whether there is a need to establish policy instruments to ensure the diversity of the equipment. This problem should also be included in the formulation of a new Security Act (part II),

Status of measures

The provider situation in the electronic communication sector changes over time. The main producers of advanced telecommunications equipment has previously been the US and Europe, but in recent years we have seen that more and more of the most advanced equipment is produced and supplied by Asian companies. The electronic communication providers choose themselves which suppliers they will use, and they are responsible for the security of their network and for their customers. This applies regardless of whether the suppliers come from a country with which Norway has security policy cooperation, or not.

For the electronic communication providers it may have advantages and disadvantages to associate with one single supplier of equipment and services. The electronic communication providers may achieve lower operating costs and fast technological development, but may also be dependent on the supplier for price and technological development. Not least, they may be vulnerable to faults linked to one supplier. The providers should therefore see the benefit of using several suppliers in their networks. The electronic communication authorities (the Ministry of Transport and Communication and Nkom) follow the development in the supplier situation and give advice and guidance in the Electronic Communication Security Forum.[18] Vulnerabilities that cannot be dealt with in the Electronic Communication Security Forum may be discussed with Nkom and the Ministry of Transport and Communication.

According to the Ministry of Transport and Communication's assessment, the competition legislation is not suitable for solving the challenges the Committee highlighted. The objective of the competition legislation is to ensure competition in the market and efficient use of resources. To avoid being restricted, electronic communication providers usually have more than one supplier of critical components.

In NOU 2016: 19 *Cooperation for security*, the problem is dealt with in connection with a broader discussion of supplier security,see the explanation in Chapters 11 and 12 on classified acquisitions and ownership control. The Committee recognises the problem and sees it in context with challenges related to foreign ownership with strategically important companies, including supply security. Reference is made in the report to Meld. St. 9 (2015–2016) *National Defence Industry Strategy*. Provisions already apply today to businesses subject to the Security Act, which allow control of suppliers who receive access to sensitive information or object, cf. chapter 7 of the Security Act. In addition, the Committee proposes new provisions that allow the authorities to control ownership of strategically important companies, cf. Chapter 10 of the bill.

10.3 Create a CSIRT in the electronic communication sector directed by Nkom

Problem description (NOU 2015: 13, section 11.7.3)

Most providers of electronic communication services in Norway are very small, and few of these own their own network. There is a need for good overall management of incidents in the digital

[18] A forum where private electronic communication providers and the security authorities share relevant information.

space that embraces all these small providers of electronic communication services. The Committee recommends a “Computer Security Incident Response Team” (CSIRT) organised in connection with Nkom.

Status of measures

Nkom CSIRT was put into trial operation from 1 April 2016 at Nkom in Lillesand. Nkom CSIRT will be in operation from 1 July 2017.[19] Nkom CSIRT was established following an assessment of the strengths and weaknesses of alternative organisational structures in light of possible ambition levels for the electronic communication sector’s future response environment. CSIRT’s independence from the supervisory authority was assessed against the advantages of the mutual benefit of co-location and the possibility for exchange of information and access to expertise. Function and the need for a response environment were discussed with the main electronic communication providers.

Nkom CSIRT is staffed from the start-up with five full -time equivalents and will assist in managing serious incidents within the sector as well as being the link between the electronic communication sector and NSM during cross-sectoral incidents. Regardless of incidents, Nkom CSIRT will assist with advice, competence building and information sharing and contribute to a high level of trust and stakeholder cooperation within the sector. See further information on measures for detecting and dealing with cyber attacks, including information sharing with NSM, in Chapter 7.

10.4 Active authority by the Ministry of Transport and Communication and the National Communications Authority

Problem description (NOU 2015: 13, section 11.7.4)

The electronic communication authority must strengthen efforts by guiding the providers on the content of legal standards related to security and robustness. A proper link between key electronic communication companies and the national security services is essential to safeguard national security needs, and it is recommended that this work is developed further through the Electronic Communication Security Forum.

A broader future electronic communication plan may be required that also includes the electronic communication perspective across sectors in Norway, including the Norwegian Emergency Public Safety Network, among others and the future need for emergency communication. This should take into account how electronic communication network and service requirements reflect society’s increasing need for digital services. The plan should include a systematic overview that regularly shows how different preventive measures should be prioritised. This overview of the electronic communication area should also be used as a contribution in the Ministry of Justice and Public Security’s overview of ICT vulnerability in Norway.

[19] The new name from 1 July 2017 will be EkomCERT.

Status of measures

The Electronic Communication Act sets out functional security requirements for electronic communication networks and services. The providers shall offer an electronic communication network and service with proper security for its users in peace, crisis and war. The regulation requires that the supervisory authorities must also provide guidance and requirements, in addition to monitoring whether the requirements are followed-up. This is continuous work that must constantly be developed.

The electronic communication authority uses to an increasing extent resources on active guidance of the businesses in the sector. It is important that the authorities are involved at an early stage in assessments the providers make about service architecture, sourcing strategies, etc. In some cases, the guidance process may be followed-up with supervision.

In 2016, the Ministry of Transport and Communication presented an electronic communication plan as part of the Government's overall ICT policy.[20] The Ministry of Transport and Communication will assess whether the electronic communication plan should be followed-up with a broader electronic communication plan and strategy for society's use and dependence on electronic communication in line with the Lysne Committee's proposal.

With input from DSB and the Norwegian Armed Forces, Nkom has already made assessments about using the 700 MHz band for mobile data services to the emergency and preparedness services. Various options are now being considered, which are being assessed against socio-economic cost/benefit. DSB emphasises that the assessment must take account cyber security requirements such as integrity, confidentiality and availability and special functionality for this user group.

10.5 Establish measures to regulate the handing over of traffic data to the police

Problem description (NOU 2015: 13, section 11.7.5)

The scope of police retrieval of traffic data is reasonably stable, while the number of requests to lift a duty of professional secrecy in order to be handed over signalling data is rising sharply. There are many questions associated with the relationship between decisions on the lifting of a duty of professional secrecy pursuant to section 118 of the Criminal Procedure Act, cf. Section 230 and section 2 of the Human Rights Act, cf. the European Convention on Human Rights, Article 8.

The Committee believes that the use of data for other purposes (particularly signalling data), should be investigated. In this context, the judges' technical competence as a basis for deciding on requests for access to information should also be assessed. The Committee believes there is a need to clarify the legal basis for regulation of access to signalling data. The Committee is also of the opinion that use of signalling data has become so widespread as an investigative tool that regulation of this should be considered as a separate coercive measure.

[20] Meld. St. 27 (2015–2016) *Digital agenda for Norway*.

Status of measures

The questions about the legal basis for signalling data and use of signalling data as a separate coercive measure has been assessed in Proposition no. 68 L (2015–2016) *Amendments to the Criminal Procedure Act, etc. (covert coercive measures)*. In connection with the legislative amendments, the legal basis for police access to location and signalling data was to some extent clarified. An addition was adopted in section 216 b, subsection 2, letter d on communication control that authorises the police to retrieve historical information from network and service providers regarding the geographical location of a particular communication system (location data), regardless of whether the system is in use for communication. The fact that police access to location data is now governed by the Criminal Procedure Act's chapter on communication control means that police use of the coercive measure is subject to constitutional review and subsequent control by the Communications Control Inspectorate. The Lysne Committee point out that it may be a challenge for judges to have sufficient technical insight when considering requests for access to data. Prop. 68 L (2015–2016) does not address this problem. However, the legislative amendments mean that there is no longer the same reason to distinguish between the different "types" of data.

In addition to using the provisions on communication control, the police may use the extra-judicial system to lift the telecommunication providers' duty of professional secrecy from Nkom in order to receive traffic data, including signalling data. In 2015, the court heard 189 communication control cases, while Nkom processed 1,459 cases regarding exemption from the duty of professional secrecy. Nkom deals with requests for signalling data according to the same set of rules as requests for exemption from the duty of professional secrecy for traffic data, i.e., section 118 of the Criminal Procedure Act, cf. section 230 The provisions on Nkom's lifting of the duty of professional secrecy also apply to confiscation or orders for compulsory disclosure, cf. section 203 et seq and section 210 of the Criminal Procedure Act. Pursuant to section 118, subsection 1, second sentence, Nkom shall give consent in these cases, unless this will expose the state or general interests to harm or appear unreasonable to the party who has the right to secrecy. In this context, Nkom uses the statement provided by the prosecuting authority or together with other information obtained when processing the case. It cannot be ruled out that today's arrangement, where waiver of confidentiality is done by Nkom according to the Criminal Procedure Act and the Electronic Communication Act, may challenge the communication protection. Based on this, the Government will consider whether further investigation of communication protection in Norwegian law is necessary in connection the implementation of the EU's new Regulation on Privacy and Electronic Communication, which is being considered by the Council of the European Union and the European Parliament, with scheduled entry into force in the spring of 2018.

11 Satellite-based services

11.1 Clarify a regulatory responsibility for Norwegian space activities

Problem description (NOU 2015: 13, section 12.5.1)

Satellite-based services are a critical societal function. Most areas of society depend on digital satellite-based services. These services may be position, navigation, precise indication of time, communication, earth observation, etc. Regulation of the space activities is sanctioned by many different laws and regulations and the responsibility for monitoring the space sector has been decentralised. Governance related to this area is complex and it is recommended that the regulatory responsibility for space activities is clarified. The purpose of such clarification is to raise awareness of vulnerabilities, identify dependencies and set requirements for security work that has the capability to look along entire value chains and covers the whole and the width of the space activities.

The Lysne Committee recommends that a small unit is established to assess what currently exists of laws, regulations and supervision of satellite based services, and then derives what new regulations, guidelines or needs for supervision must be established. Based on own assessments and a report from Oslo Economics, the Committee recommends that the responsibility lies with either Nkom or DSB. The Committee believes a separate assessment is required in order to be able to decide which of these entities will be in charge.

Status of measures

There is broad consensus among the consultation bodies that it is necessary to clarify regulatory responsibility within the space activity. However, the majority of the consultation statements do not support the recommendation by the Lysne Committee to consider establishing a new agency, or selecting a single agency, with special responsibility to follow-up the space activity at national, cross-sectoral level.

Follow-up of the Lysne Committee’s recommendation to clarify the regulatory responsibility for Norwegian space activity has been discussed by the Inter-departmental Coordination Committee for Space Activity (IKU), led by the Ministry of Trade, Industry and Fisheries. Based on the broad consensus of the Committee, a security sub-committee under IKU (IKU-S) was set up in 2016. The purpose of IKU-S is to strengthen exchange of information between ministries and agencies, so that cross-sectoral vulnerabilities and security threats are highlighted. Furthermore, the Norwegian Space Centre has been commissioned by the Ministry of Trade, Industry and Fisheries to identify the current placement of regulatory responsibility as well as possible synergies between the various parties with such responsibility. The Ministries in IKU-S are responsible for collecting and coordinating contributions from their own sector for the mapping.

In addition, the Ministry of Transport and Communication has commissioned the Norwegian Space Centre to prepare a national, cross-agency and cross-sectoral PNT strategy (position finding, navigation and dating). The strategy will be based on today's situation and provide guidance for the development and use of ground-based and satellite-based navigation systems in the coming 10-15 years. The work will be completed by June 2017.

12 Energy supplies

12.1 Strengthen supervision and guidance in cyber security

Problem description (NOU 2015: 13, section 13.7.1)

The Norwegian Water Resources and Energy Directorate (NVE) has limited capacity to follow-up with supervision within cyber security and vulnerability. It is proposed to strengthen NVE significantly in the area of supervision and guidance.

A general trend is that there are ever closer links between operational control systems and business systems. NVE should be able to play an important role in communicating best practice and otherwise guiding affected businesses in secure implementation.

In the energy sector, like other sectors, there is an increased trend towards outsourcing. NVE together with stakeholders and the industry should prepare guides and requirements for outsourcing in the energy sector. The sector is recommended to look at international standards.

Status of measures

cyber security is a priority area for NVE. NVE has built up a case management team that has the expertise that is essential for the important work of supervision, guidance and regulatory development for cyber security in the energy sector. It is important to maintain this specialist community and in a long-term perspective further strengthen the Directorate’s cyber security expertise. In total, NVE has increased its personnel capacity in cyber security by two full-time equivalents. See also the account of establishment of a common arena for the various sectors’ key supervisory authorities in section 22.7.

NVE has been involved in the development work as a basis for providing guidance on cyber security. In the area, NVE cooperates with other authorities, with own sector and with suppliers.

An inspection of operational control systems is planned in 2017. In an award letter for 2017, the Ministry of Petroleum and Energy has requested NVE to consider the sector's set of rules and related guidance in order to strengthen the cyber security. In 2016, NVE started an ICT regulations project that has assessed existing ICT and operational control security. The ICT regulations project will end in 2017. The project has assessed the need for basic protection for all businesses, including protection when outsourcing IT and more stringent protection requirements for advanced measurement and control systems (AMS) and operational control systems.

The ICT regulations project has also assessed existing regulations against international standards and the regulations in other countries. The work shows that today’s contingency regulations have a high degree of compliance with the ISO 27001/2 standard for information security management and that through the contingency regulations Norway has good regulations for cyber security in the energy sector.

NVE will follow-up the results from the ICT regulations project with regulatory work and development of guides in 2017. In 2016, NVE established close cooperation with NSM, and future cooperation includes development of guides to the regulations.

12.2 Stimulate greater and specialist community with more resources within cyber security

Problem description (NOU 20 13, section 13.7.2)

Several units in the Power Supply Preparedness Organisation (KBO) are small with few employees, and it is a challenge with respect to expertise to establish and maintain the necessary specialist community. NVE in cooperation with the interest organisations should stimulate larger and more robust specialist communities in cyber security in the KBO units.

The trade organisations have a well-established system for courses and training. They should be able to help organise courses in cyber security, preferably in cooperation with other organisations, or refer to NVE, other authorities or educational institutions where this is appropriate. Courses and programmes should also be developed within process control, system integration and ICT.

Competence related to cyber security varies among businesses in the sector. It is recommended that through its guidance role, NVE is the driving force behind several exercises in the area of cyber security both within the sector and in cooperation with appropriate sectors.

Status of measures

NVE has dialogue with several specialist communities, cooperation alliances and professional and industrial bodies in the energy sector. Through the ICT regulations project in 2016/2017, NVE has conducted several brainstorming sessions with the sector and has had close contact with energy producers, network companies and IT providers.

A long term ambition of NVE is that good cooperation is established between the sector and the academia on cyber security and security in operational control systems, which the Ministry of Petroleum and Energy stands behind. Cooperation can be achieved through the industry contributing industry knowledge and practical insight into research, education and course development and through research projects where the sector, the authorities and the academia cooperate. Close cooperation will contribute to the development of relevant courses and further education opportunities, and the creation and dissemination of new knowledge about how the businesses in the energy sector protect themselves against cyber threats.

In 2017, NVE has a strategic focus on skills upgrading within cyber security in the energy sector through guidance, cooperation with academia on R&D and education and cooperation with industry associations on courses. NVE has also allocated funds to this in 2017, including development of an action plan to raise expertise in the industry. As part of these efforts, NVE will support the cyber security community at NTNU CCIS with a part-time post of approximately 20%, which can provide practical insight and relevant industry knowledge when developing educational programmes and courses within cyber security, initially for the academic year 2016/2017. The scheme will then be evaluated.

NVE also offers competence days and seminars for the sector and generally engages in educational work through lectures. In the years ahead, NVE will prepare and conduct exercises related to cyber security, about which the Ministry of Petroleum and Energy is positive.

12.3 Build a strong operational specialist community for ICT incident management

Problem description (NOU 2015: 13, section 13.7.3)
The sector should have a competent common community for incident management that can coordinate incidents internally within the sector and be the point of contact with other sectors. The Lysne Committee supports the idea of further developing KraftCERT as a strong specialist community within operational incident management. NVE must clarify requirements for connection to an operational specialist community for incident management, either with KraftCERT or other environments. The businesses should have a clear justification for the option they choose. It is important to clarify roles between the response environments, so that the energy sector acts uniformly towards other sectors.

Status of measures
It has been important for the sector to increase detection and management capabilities and together with other sectors contribute to good reports on the status of cyber security. NVE has been an important driving force behind the establishment of KraftCERT. An increasing number of energy companies are associated with Kraft CERT, which currently has 71 members. Today, NVE and KraftCert make up the sector’s response environment. KraftCERT is a private company that has been established by the sector, and which is part of KBO following a decision by NVE. The existing model has been based on cooperation and information sharing.

NVE will also work towards KraftCERT being a strong professional response environment for the energy sector with relevant services for the sector and good cooperation with NVE. It is an ambition that all relevant parties within the energy sector use KraftCERT, was supported by the Ministry of Petroleum and Energy, cf. the reference in the Energy Report (Meld. St. 25 (2015–2016)).

NVE is considering the proposal to require connection with a response environment. As a part of this, NVE is considering whether requirements should be set in general or based on how critical the businesses and the systems are for the secure supply.

12.4 Assess security issues by the processing and storing sensitive energy information abroad

Problem description (NOU 2015: 13, section 13.7.4)
What is considered to be sensitive energy information and therefore must be protected separately is evident from the Emergency Preparedness Regulations. At the same time, the technology development, greater system integration and organisational changes by suppliers change the scope of service development. The current regulations pose challenges for service development and efficient operation of the energy supply. It is recommended that NVE makes an assessment of the information that, given the changed technological and organisational frameworks, is so critical that it should not be stored and processed outside Norway's borders. NVE recommends looking at the whole value chain and identifying the information that must be under national control.

Status of measures

Through the ICT regulations project, NVE has been in dialogue with other authorities and the industry to assess the value chain for the energy supply and its vulnerabilities and identify which information in the value chain must be under national control and storage. This also means looking at whether the Emergency Preparedness Regulations are adapted to today's situation. Today, the Emergency Preparedness Regulations govern the type of information that is considered to be sensitive energy information, and set requirements for processing, protection and access to sensitive energy information. The information is subject to confidentiality. NVE will investigate whether there is a need for further restrictions on storage and access to sensitive energy information.

An overall assessment of value chains is discussed in section 22.1 and outsourcing in section 6.4 and 22.10.

12.5Conduct risk and vulnerability analyses for extended use of AMS

Problem description (NOU 2015: 13, section 13.7.5)

By 1 January 2019 all electricity customers in Norway will have smart meters installed. The new meters are included in “advanced measurement and management systems” (AMS), and this means that the consumers receive better information about their electricity consumption, more accurate bills and the possibility for automatic control of consumption. The decision to introduce AMS was made without a prior risk and vulnerability analysis. The transition to AMS involves a great potential for increased network utilisation, innovation and improvement of efficiency in the sector. Uncritical implementation of functionality that, for example, links AMS more closely with operational control systems, will lead to a building up of vulnerability with significant damage potential. It is important to have a good and wide-ranging risk and vulnerability analysis prior to technological changes, changes in use and system and organisational changes. NVE is recommended to conduct the necessary risk and vulnerability analyses for extended use of AMS against operational control systems.

Status of measures

This problem is followed-up in NVE’s ICT regulations project. NVE has conducted three trial inspections of AMS in 2016 and is preparing an updated guide for AMS security. NEW has made it clear to the industry that it is important to conduct risk analyses when introducing AMS and that the network companies are responsible for ensuring adequate security in the AMS solution. The recommendation that NVE should conduct a risk and vulnerability analysis before considering extended use of AMS is supported by the Ministry of Petroleum and Energy.

NVE will obtain one or two annual reports on AMS from all the network companies in 2017 and 2018, where the network companies’ assessment of different risk categories, including cyber security, is included. NVE will follow-up that the network companies maintain the information security both during installation of AMS and later the day-to-day operation.

12.6 Prepare an updated analysis of the power supply's dependence on electronic communication

Problem description (NOU 2015: 13, section 13.7.6)

Although the power industry has so far managed to handle critical situations without commercial electronic communication, this ability can be challenged in the future when even more ICT is added to and integrated into the power infrastructure. NVE and the industry are recommended to conduct a review to check whether today's requirements provide the "independence" the regulations require.

Status of measures

NVE has reviewed the current requirements. The thematic structure is also addressed when NVE implements changes in the industry. The power supply system has several barriers and safety measures to prevent the loss of control capability. The power supply system also has its own telecommunication circuit, in addition to the public communication network. However, operation, recovery and supplier support are becoming more demanding without access to the ordinary electronic communication services. Therefore, NVE has ordered all KBO units to strengthen own robustness by having several communication service providers and solutions. NVE monitors how the network companies have solved this.

Several KBO units are considering their solution for operational communications. In connection with this, the possibility of using the Norwegian Emergency Public Safety Network as an operating radio is also being considered. All companies, including those who choose the Norwegian Emergency Public Safety Network, must comply with regulatory requirements for emergency power in the operational communications, among other things. Companies who choose to use the Norwegian Emergency Public Safety Network must therefore set requirements for robustness in the Norwegian Emergency Public Safety Network.

In 2017, NVE will implement an R&D project on the future secure solutions for operating radio. This project will provide answers to how the requirement that the KBO units must be independent of the public communications network can also be safeguarded in the future.

13 Oil and gas

13.1 Transfer the security tradition in HSE to the digital area

Problem description (NOU 2015: 13, section 14.7.1)

The oil and gas sector has a long security tradition, a strong security culture and a high level of expertise as regards HSE. This good security tradition should be continued in the digital area.[21]

[21] Responsibility for the work on cyber security in the oil and gas sector lies with the Ministry of Labour and Social Affairs and is followed-up by the Petroleum Safety Authority.

Status of measures

The Petroleum Safety Authority (PSA) has contributed to transfer of the HSE traditions to the digital area by making the stakeholders responsible for development of good norms and standards, and to implementation of self-assessments based on the Norwegian Oil and Gas Association's guidelines, NOROG-104.[22] Important work in the future will be to develop and adjust the regulations with the field. Norwegian oil and gas published a new version of the NOROG-104.5 guidelines on 5 December 2016.

In November 2015, DNV GL took the initiative to prepare standardised cyber security requirements for the oil and gas industry based on the ISA/IEC standards. The operators, suppliers, engineering and consulting companies and a representative for PSA participate in this work. The work is expected to be completed in the summer of 2017 and will result in a recommended practice that will be included in DNV GL's portfolio.

13.2 Assess the value of the sector's facilities and ICT systems and establish regulations for digital vulnerabilities

Problem description (NOU 2015: 13, section 14.7.2)

The main regulations for the digital vulnerability in the sector are found in the HSE regulations for the petroleum activities and in the working environment regulations. The regulations are not specific when it comes to cyber threats, but also include cyber security. The Committee is of the opinion that there should be a requirement from the supervisory authority (PSA) that barriers against digital vulnerabilities should be established.

In anticipation of a new Security Act and any orders and directives from the EU, the Committee recommends that work be carried out on valuation and classification of facilities and ICT systems.

Status of measures

PSA has prepared and circulated for comments a proposal for clarification of the application of the HSE regulations in the field of security, including cyber security. PSA is awaiting follow-up of the proposed new Security Act (NOU 2016: 19 *Cooperation for security*) before it determines legislative amendments.

PSA will clarify and further develop the regulations to address the challenges the industry faces as a result of changes in the threat situation and increased digitalisation. This means monitoring the development of industrial standards, among other things, that can be referred to in the regulations.

Anchoring cyber security measures in the enterprise's management is one of the topics PSA addresses in its inspections. In 2016, PSA has conducted five audits of operators, both regarding security in general and cyber security in particular. Cyber security supervision is conducted as specific audits, as part of a larger security inspection or together with other fields. Such system audits

[22] Norwegian oil and gas guidelines 104: *Recommended guidelines information security level requirement in ICT-based process control, security and support systems.*

of an operator cover all installations and facilities for which the operator is responsible. Meetings are also held with contractors where cyber security has been one of the topics.

13.3 Clarify the role and capacity of the Petroleum Safety Authority

Problem description (NOU 2015: 13, section 14.7.3)

The Petroleum Safety Authority (PSA) has value chain expertise and expertise in technical safety in the sector, but limited capacity when it comes to supervision of the sector's cyber security and vulnerability. The Lysne Committee proposes that PSA is strengthened significantly in this area.

Status of measures

PSA participates in professional forums, both nationally and internationally, to ensure expertise and build networks. PSA also see that capacity in particular, but also expertise within cyber security should be strengthened within the authority. In the summer of 2017, the staff will be strengthened further with expertise within technical automation systems and cyber security. See also the report on establishment of a common arena for the various sectors' key supervisory authorities in section 22.7.

PSA will look at the possibility to clarify challenges and prepare a risk picture within cyber security in the petroleum industry. The work involves method development, information gathering from the industry and authorities and analysis work. PSA will update the risk picture annually to monitor the effects of the industry's measures and identify the need for improvements.

13.4 Assess the connection to the response environment for ICT incidents.

Problem description (NOU 2015: 13, section 14.7.4)

The oil and gas sector lacks a common response environment for ICT incidents. A few businesses are associated with NSM, but the smaller companies in the industry in particular fall outside such cooperation. The Lysne Committee recommends that the businesses in the sector either enter into cooperation with KraftCERT or find other solutions for operational cooperation.

The industry has its own emergency preparedness organisation that will come into force in major incidents,cf. civil emergency preparedness system. The Committee is not aware that this organisation has practised dealing with major ICT incidents. Therefore, the Committee recommends that the sector conducts exercises in management of undesirable ICT incidents.

Status of measures

In the consultation statements to the Lysne Committee, the Norwegian Oil and Gas Association agrees that the current situation regarding cooperation and notification can be improved, but under-lines that the industry’s corporate structure may make it difficult to find a uniform national cooperation structure. In its consultation statement, KraftCERT welcomes the petroleum sector to cooperation.

The petroleum industry does not have a common emergency preparedness organisation, but has PISAS (Petroleum Industry Security Alert System). The system is owned by the Norwegian Oil and Gas Association and was used by PSA during the mapping campaign in 2014.[23] The system is run monthly.

The work within emergency preparedness and incident management will be further developed, including the operator’s duty to warn, including reporting channel and CERT solution. This also involves developing and implementing the necessary exercise activities with businesses in the industry and the competent authorities.

In meetings with the industry, PSA has discussed the need for a sectoral response environment in the petroleum industry, especially for operators with operational responsibility on the Norwegian Continental Shelf who do not have an internal global network. KraftCERT is now also available to the petroleum industry.

The petroleum industry sees so far that their needs have been met through the individual company’s cooperation or partnership agreements with NSM or because the foreign parent company has agreements with the national CERT environment. The industry’s need is first and foremost to establish secure communication channels for quick notification of cyber incidents and implementation of recommended measures.

The Ministry of Labour and Social Affairs is of the opinion that there is a need for improved coordination of cyber incidents between the petroleum industry and the authorities. For cyber incidents in the petroleum sector, PSA has had the role of information provider between NSM and the petroleum industry and has followed-up the companies’ measures in meetings and security supervision with the parties involved.

PSA participated together with the Ministry of Labour and Social Affairs in the "IKT16" exercise (see sections 7.2 and 8.7). A separate Exercise Directive was drawn up for the Ministry of Labour and Social Affairs’ sector with four sector objectives, which included role clarification, planning, cooperation, participant chart and criteria for notification of serious cyber attacks,

[23] Several parties actively map the Norwegian digital infrastructure. In the summer of 2014, an extensive mapping campaign was conducted involving several businesses within the energy and petroleum sectors in Norway.

14 Water supply

14.1Increase cyber security competence in Norwegian waterworks

Problem description (NOU 2015: 13, section 15.6.1)

Many small units make it a challenge to establish and maintain the necessary specialist environments within cyber security. The Committee is of the opinion that the Norwegian Food Safety Authority in cooperation with Norwegian Water should stimulate greater and more robust specialist environments in the municipalities. This can be done in several ways, such as increased inter-municipal cooperation or structural change.

The Committee also proposes that initiatives be taken to address the new challenges we face within cyber security. The authorities and Norwegian Water should be able to contribute by organising courses, preferably in cooperation with other organisations such as NSM or educational institutions where this is appropriate. Courses and programmes should also be developed within process control, system integration and ICT, which may help the industry to achieve the expertise required to operate the systems in the future.

Status of measures

New regulations on water supply and drinking water (the Drinking Water Regulations), which came into force from 1 January 2017, set preventive security requirements by ensuring that all water supply management systems are adequately secured against unauthorised access and use. It is also a requirement that the waterworks owner must ensure that the water supply system has, or through agreement has access to, the necessary expertise. It is also a requirement that everyone who participates in the activity covered by the regulations is familiar with the importance of the preventive security requirements. The Norwegian Food Safety Authority has prepared a guide to the regulations.[24]

The preventive security requirement is new in relation to previous drinking water regulations, and the competence requirement has been clarified. The regulations facilitate cooperation to strengthen expertise, for example, regarding cyber security.

As a professional body, Norwegian Water pays close attention to cyber security and publishes reports and guidance material and arranges courses.

Introduction of the said regulatory requirements and Norwegian Water's own initiatives are important steps on the road to increasing security expertise in Norwegian water supply. The industry must now be given the possibility to follow-up the requirements. The Norwegian Food Safety Authority conducted inspections throughout the country with the main emphasis on cyber security in 2016. After a suitable period, the Ministry of Health and Care Services will ensure that the Norwegian Food Safety Authority follows-up with a new national inspection project, and evaluate

[24] The Norwegian Food Safety Authority's guide to the regulations: http://www.mattilsynet.no/mat_og_vann/vann/ veiledning_til_drikkevannsforskriften__10_forebyggende_ sikring.25134.

whether the regulatory requirements have resulted in a changed situation. Additional measures will be assessed after this.

14.2 Strengthen supervision and guidance in cyber security

Problem description (NOU 2015: 13, section 15.6.2)

There is a need for increased attention from the Norwegian Food Safety Authority as regards cyber security. This includes drawing up regulations that define cyber security requirements and associated guidance material for waterworks. The waterworks seem to need additional information in addition to the general requirements that are imposed on the waterworks owner in the Drinking Water Regulations. Close cooperation between the various supervisory authorities should be considered in order for each supervisory authority to be better able to oversee its sector related to incidents across the sectors (water, electricity and electronic communication). Relevant authorities should clarify and adopt a necessary level of ambition for cyber security for the waterworks.

The Ministry of Health and Care Services has initiated work to revise the Drinking Water Regulations with associated guide. The revision must also include cyber security and ICT in addition to the general requirement that the waterworks owner is responsible for providing safe drinking water.

Status of measures

The cyber security requirement in the new Drinking Water Regulations applicable from 1 January 2017 makes it easier for the Norwegian Food Safety Authority to follow-up through supervision of whether the necessary cyber security is in place. In 2016, the Norwegian Food Safety Authority implemented a national inspection project aimed at the waterworks' emergency preparedness with special focus on the waterworks' preparedness with the ICT systems. Prior to the inspection project, the inspectors received training, which involved inspection of IT security. This resulted in strengthened expertise internally in the Norwegian Food Safety Authority.

The new Drinking Water Regulations set out clear requirements for preventive security and expertise at the waterworks, The requirements are explained in the Norwegian Food Safety Authority's guide to the regulations. The Norwegian Food Safety Authority is also required in accordance with the requirements of the Public Administration Act to be able to provide guidance about the requirements set out in the regulations. However, the Norwegian Food Safety Authority will probably not have sufficient expertise within cyber security.

The Norwegian Food Safety Authority has taken the first step to improve its own expertise in order to be able to provide guidance and oversee the waterworks' cyber security. In the short term, additional skills upgrading is necessary to strengthen the Norwegian Food Safety Authority's internal expertise. The Ministry of Health and Care Services expects the Norwegian Food Safety Authority to maintain such internal expertise, but no specific skills upgrading plan has been decided within this area. The Norwegian Food Safety Authority must cover a wide range of areas of competence, and it should find an appropriate level for adequate supervision. This should be done in close cooperation with NSM. See also the report on establishment of a common arena for the various sectors' key supervisory authorities in section 22.7.

14.3 Improved systems for incident management

Problem description (NOU 2015: 13, section 15.6.3)

There seems to be a need to establish a common response environment for incident management. A separate response environment for water is perhaps not realistic, considering the large number of small units in the water sector, and the Committee outlines three options.

The Committee recommends that the Ministry of Health and Care Services, in consultation with the Ministry of Justice and Public Security and the Ministry of Local Government and Modernisation, investigates the possibility for a response environment for incident management that takes care of water and drainage.

Status of measures

A common response environment for incident management that takes care of water and drainage has not been investigated and the Ministry of Health and Care Services has no specific plans to investigate this. The network for competence support to waterworks in the event of undesirable incidents was established from 1 January 2017 and is administered by the Norwegian Institute of Public Health. The scheme involves establishment of an emergency telephone, duty scheme and a network of experts in toxicology, microbiology, epidemiology and relevant water expertise. Initially, cyber security expertise will not be included. A reference group for the scheme has been set up where DSB is represented. An extension to include cyber security would probably be considered at the end of 2017.

14.4 Conduct risk and vulnerability analyses before possible introduction of smart water meters

Problem description (NOU 2015: 13, section 15.6.4)

Introduction of smart water meters, equivalent to the AMS introduced in the energy sector, link water meters closer together with operational control systems. This increases the vulnerability and may have significant damage potential. The necessary risk and vulnerability analyses should be conducted to prevent uncritical implementation of functionality by establishing smart water meters linked to operational control systems.

Status of measures

There is currently no requirement to introduce such meters. If the water sector wants to use smart water meters, the waterworks/sector itself has a responsibility to investigate and ensure that this does not weaken cyber security. This follows from the requirement in the new regulations that came into force on 1 January 2017. The proposal to conduct risk and vulnerability analyses has so far not been investigated, and the Ministry of Health and Care Services currently has no plans to investigate this.

15 Financial services

15.1 Strengthen efforts to assess future payment services

Problem description (NOU 2015: 13, section 16.7.1)

The development of new payment services is fast. New technology and solutions give individuals as well as industry and commerce many advantages. However, new payment services can lead to vulnerabilities when user friendliness and "*time to market*" have priority. Such services may lead to digital vulnerabilities, and the challenges may lie outside national control, so that Norway is not equally capable of influencing. Finance companies could be involved in facilitating solutions that are insufficiently secure.

It is important that the financial industry focuses more attention on these problems to ensure that the regulations are also relevant and adapted to these challenges in the future, among other things. The Ministry of Finance should assume a clear role to keep track of new businesses that provide banking and payment services.

Status of measures

New technology challenges established business models in the financial industry. Use of new technology and new business models has many desired affects, and the legislation should not be an unnecessary obstacle to the development. The legislation should contribute to the development taking place within appropriate legal frameworks, so that security and preparedness considerations are taken care of. The challenge is to draw up regulations that balance precautionary concerns with the potential benefits of innovation and change in a good way. The relationship between innovation and regulation in the financial markets is discussed further in section 3.3.2 of Meld. St. 34 (2016–2017) *the Financial Markets Report 2016–2017*, where the Ministry of Finance points out that the authorities can contribute to a more diversified and robust offering of financial services, which in turn reduces systemic risk in the financial markets, by facilitating new participants and business models. The Ministry of Finance stated in the report that a low-threshold contact point should be established between the authorities and so-called Fintech companies in Norway. The Financial Supervisory Authority of Norway provides significant guidance to Fintech start-ups on regulatory issues today, but there may be a need to establish a clearer structure for guidance of innovative businesses. Therefore, on 5 April 2017, the Ministry of Finance sent a letter to the Financial Supervisory Authority of Norway requesting how a contact point with Fintech companies can be established in an appropriate way.

The emergency of new payment services is one of the reasons that the EU's revised Payments Services Directive 2 (PSD 2) has been adopted. The purpose of the Directive is to promote secure technical payment solutions and modernise the regulatory framework in line with the developments in the market. The Directive allows new payment services and also governs cooperation between the various service providers. Additional provisions have been laid down to safeguard security under the new solutions. The Directive is relevant to the EEA and it is expected to be incorporated in the EEA agreement. No implementation deadline has currently been set for the EFTA member states. The Financial Supervisory Authority of Norway has prepared a consultation paper with draft legislative and / or regulatory provisions that implement the anticipated EEA provisions in accordance with the Directive. The Ministry of Finance aims to distribute the matter for comment in 2017.

The Ministry of Finance, the Financial Supervisory Authority of Norway and the Central Bank of Norway monitor the developments in their respective areas of responsibility within banking and payment services. Analyses of risk developments are done on a regular basis. The Financial Supervisory Authority of Norway prepares an annual risk and vulnerability analysis of the financial sector's use of ICT. In the latest report, presented on 26 April 2017, the Financial Supervisory Authority of Norway assesses the payment systems in general to be solid and stable, and points out that in 2016 there were fewer and less serious ICT incidents than in previous years. Despite an increase in losses related to fraud and attacks against the payment services, the losses are still relatively low. Much of the reason for the low level of losses is preventive measures. The Central Bank of Norway presents an annual report on financial infrastructure as part of its work to promote financial stability and an efficient payment system in Norway.

15.2 Continue inter-disciplinary cooperation for good preparedness and management of serious intentional ICT incidents

Problem description (NOU 2015: 13, section 16.7.2)

There is good cooperation between FinansCERT and the Financial Infrastructure Contingency Committee (BFI). However, an area of improvement is to be more prepared for the rare, serious incidents, such as how to plan emergency preparedness if the electronic infrastructure is unavailable over a long period.

The Committee questions how well prepared the sector will be to manage the major crises, and is of the opinion that BFI, in cooperation with FinansCERT, must take the initiative to conduct more coordinated and complex exercises with sufficient gravity and realism. Furthermore, crisis communication with the customers should be practised.

Status of measures

Digital incidents are followed-up in the usual manner by the supervisory authorities (the Financial Supervisory Authority of Norway and the Central Bank of Norway) with the parties concerned. The Financial Supervisory Authority of Norway oversees the financial businesses and customer-based payment services, while the Central Bank of Norway oversees inter-bank systems. This involves supervision of emergency preparedness solutions. The ICT regulations set requirements for reporting serious and critical incidents to the Financial Supervisory Authority of Norway. FinansCERT has been established by the finance industry and has become a key player in the industry's management of security incidents. FinansCERT cooperates with the authorities and has gain a permanent observer place in BFI. The industry has a high level of ambition for its own and FinansCERT's efforts in this area. Nordic finance companies have recently agreed to establish a Nordic Financial CERT based on the current Norwegian activities in FinansCERT.

Exercises are necessary in order to be better at preventing and managing the serious and rare incidents. BFI conducts regular exercises and attaches great importance to the exercises that will be relevant and realistic and address serious scenarios. The exercises are in addition to exercises conducted by each enterprise and by the authorities. The Financial Supervisory Authority of Norway is the secretariat for BFI and has insight into the exercise activity of businesses and authorities. Therefore, the Financial Supervisory Authority has good prerequisites for organising exercises that help to complement other exercise activity. The Financial Supervisory Authority of Norway follows-up the businesses’ exercise activity and emphasises that such exercises help to strengthen the most operational part of the incident management in the financial sector.

15.3 Analyse the vulnerability consequences as a result of outsourcing out of the country

Problem description (NOU 2015: 13, section 16.7.3)

It may be a challenge that many businesses in the financial sector move parts of their ICT activities out of the country. Such outsourcing may be within acceptable risk for each enterprise, but the overall societal risk may be too high. It is important that the businesses are aware what expertise should not be outsourced. In particular, this could apply to emergency preparedness expertise, which should be business-related.

In the opinion of the Committee, the Ministry of Finance must instruct the Financial Supervisory Authority of Norway to assess what the long-term consequences of offensive use of outsourcing may be. It should be assessed whether outsourcing activities that may be important to society should have a requirement that there is always an active “*cold backup*” locally in Norway.

In the financial sector in Norway, there are outsourcing provisions in the ICT regulations and in the regulations relating to risk management and internal control, but it should be considered whether these should be further developed and detailed based on the proposed competence assessment. The Committee is of the opinion that it is important to show accountability regarding this issue, as in the long-term. widespread use of outsourcing may contribute to weakening the national ability to develop and follow-up key competence areas.

Status of measures

The Ministry of Finance and the Financial Supervisory Authority of Norway are aware that outsourcing may change the quality and stability of the ICT systems, and at the same time weaken insight into and control of the vulnerabilities in the systems on which the financial companies base their activities. Therefore, new legislation was adopted and came into effect regarding this in 2014. The provisions apply to the kind of tasks the financial companies may outsource, and authorise the Financial Supervisory Authority of Norway to check the outsourcing and take measures against unjustifiable outsourcing. In April 2016, the Financial Supervisory Authority of Norway received a report on outsourcing from a working group consisting of representatives from the Central Bank of Norway, the Ministry of Finance and the Financial Supervisory Authority of Norway. The report contains assessments that may provide guidance in practising the regulations. The Financial Supervisory Authority of Norway aims to follow-up the report in a circular in which the Authority will also take into account the forthcoming guidelines on outsourcing and cloud services from the European Banking Authority, EBA. Issues related to outsourcing are also discussed in sections 6.4 and 22.10.

15.4 Continue and strengthen commitment to influencing international regulations of cyber security mechanisms

Problem description (NOU 2015: 13, section 16.7.4)

We have increasingly a common regulatory framework with the EU and other international parties. There is concern that we can have lower security requirements in Norway as a result of common regulations in the EU. It is important that the Ministry of Finance reviews the arenas to which Norway has and uses the opportunities that exist to influence the development as early as possible. The Committee agrees with the Financial Supervisory Authority of Norway that the supervisory activities must be up-to-date with the best practice, and encourages the Financial Supervisory Authority of Norway to continue the extensive cooperation that is already under way internationally with other countries' and EU supervisory bodies.

Status of measures

It is important to have international cooperation in this area, and the Ministry of Finance will continue to develop Norwegian legislation within the EEA obligations and other frameworks. The EU's rules on cyber security involve extensive requirements for risk management, security measures and reporting undesirable incidents, and there are constantly evolving, cf. the discussion of PSD 2 in section 15.1 above. The Financial Supervisory Authority of Norway and the Central Bank of Norway have extensive international cooperation and will build on this in various forums.

15.5 Strengthen emergency measures for the development towards the cashless community

Problem description (NOU 2015: 13, section 16.7.5)

New technology and easy-to-use payment solutions mean that an increasing number of people in Norway do not use cash. However, from an emergency preparedness perspective, a full transition to digital solutions (electronic cash) may give increased vulnerability. There are many who will depend on cash in a serious emergency situation.

The Committee believes this is an example of a high level of vulnerability with a digital origin that Norway must be prepared for. The existence of cash in itself provides several opportunities in a crisis situation. The Ministry of Finance should take the initiative to see how this can best be solved, through looking at other countries' management of similar challenges, among other things.

Status of measures

The Financial Supervisory Authority of Norway and the Central Bank of Norway have worked on issues related to emergency preparedness in the payment system over a long period and have submitted a proposal to the Ministry of Finance regarding new provisions relating to the banks' contingency responsibility for distribution of cash. The Ministry of Finance has distributed the proposal for comments with a deadline of 2 May 2017. The Financial Supervisory Authority of Norway and the Central Bank of Norway have also provided information to the Ministry of Finance about how they - in line with their duties as supervisory authorities in the payment area - follow-up the emergency preparedness for the electronic payment system.

16 Health and care services

16.1 Stronger management of cyber security by the Ministry of Health and Care Services

Problem description (NOU 2015: 13, section 17.7.1)

Several parties would like to see stronger management of cyber security by the Ministry of Health and Care Services. The Committee questions why the Ministry's ability to coordinate between the regional health authorities has not been used to a greater extent. The Committee is of the opinion that there is a need for stronger national management to identify and meet common needs and to avoid divergent solutions in the regions.

Through its work, the Committee has registered that a large volume of reports have been published in recent years that deal with ICT in the health sector. Several of these seem to describe today's challenges in a good way, and there seems to be great awareness in the sector of what improvement measures are required. The Committee questions why several of the measures have not been followed-up, and whether the volume of reports in itself precludes effective implementation of the measures. The Committee believes it is important to have clear prioritisation of preventive measures to reduce the identified vulnerabilities, and efficacy for these must be ensured. As part of this work, the Committee proposes that the new Directorate for eHealth prepares an annual status report on the state of cyber security in the health care sector.

The Committee believes that simplifications of the Norm for Information Security in the Health and Care Services (the Norm) should be considered for the smallest health authorities to the extent this is possible without causing increased vulnerability.

Status of measures

Several measures have been implemented to ensure improved coordination and management of ICT development in the health and care sector, which also strengthens the cyber security.

The Norwegian Directorate for eHealth has been established from 1 January 2016 to contribute to improved management and coordination of the e-health area. ICT measures must be seen in context to ensure the best possible use of the suppliers' and own development resources. The Directorate in cooperation with other relevant parties will contribute to increased competence on information security and privacy. The Norwegian Directorate of e-Health has the role as authority and premise provider in the national work on ICT infrastructure.

The regulations on ICT standards in the health and care sector came into force on 1 September 2015. The regulations require the parties in the sector to use electronic medical records, to update the address register in the health network and to use standardised message formats for the exchange of patient information between the parties. The regulations will help ensure that electronic communication is effective and standardised. This is a beginning, and the regulations will be improved in line with the development and needs of the sector.

The Ministry of Justice and Public Security requires annual reporting of the security status in the sectors. This reporting is limited to the Security Act. The Ministry of Health and Care Services wants to assess what additional reporting is necessary and possibly implemented in the health and care sector, and who is best suited to taking care of this task.

Norsk Helsenett SF currently has an operational role in the work on information security in the health and care sector and operates HelseCERT, among others, which monitors the traffic on the health network, prepares vulnerability overviews, implements intrusion tests, assists with incident management, etc.

The Information Security Norm (the Norm) is an industry standard, and although the secretariat is currently at the Norwegian Directorate of e-Health, it is the industry itself that determines the content of the Norm. The Norm is based on applicable laws and regulations, but may, where appropriate, be more stringent than the laws and regulations require.

The Ministry of Health and Care Services has required in award letters and letters of assignment to underlying businesses that they work purposefully on information security, cf. the Security Act, *National Strategy for Information Security* (2012) with its associated action plan and *The Action Plan for Information Security in Public Administration – 2015–2017* (2015).

16.2 More research on cyber security within new health and welfare technology

Problem description (NOU 2015: 13, section 17.7.2)

In the opinion of the Committee, health and welfare technology that changes society to a great extent, should be investigated and followed-up by a public debate before implementation. The Committee believes there is a need for a more focused research effort to examine the security aspects of the technology, while taking into account the opportunities and challenges new health and welfare technology will provide. Trials in progress involving new health and welfare technology should be coordinated nationally to ensure transfer of expertise. The new Directorate for e-Health should ensure that these initiatives are coordinated.

Status of measures

NOK 2 million has been granted as basic funds to NTNU CCIS at Gjøvik. The grant will support this work on information security and privacy in the health and care sector. Further initiatives regarding focused research efforts in addition to the basic grant to NTNU CCIS will be assessed later.

16.3 Establish solutions to meet the development within health and welfare technology

Problem description (NOU 2015: 13, section 17.7.3)

When introducing health and welfare technology the main rule should be that the service owner of such solutions should assume overarching responsibility for the security throughout the value chain and not merely assuming that security is taken care of by the underlying services such as electronic communication providers.

The Committee supports Norsk Helsenett's proposal that the health network, in cooperation with the sector, should consider whether there are key common components (within communication with the internet) that the sector needs to promote a secure introduction of welfare technology solutions.

Status of measures

The Norwegian Directorate of e-Health has initiated report on a national storage platform for data from welfare technology solutions through the National Welfare Technology Programme. A total of NOK 40 million has been granted to the security and coping assignment, which is part of the National Welfare Technology Programme. Development of a reference architecture and establishment of infrastructure in the area of welfare technology are key elements of the assignment. The purpose is to form the framework for development of welfare technology solutions and to ensure that data from such technology may be shared securely between various parties in the health and care sector. The Norwegian Directorate of e-Health is leading the work in cooperation with the Directorate of Health and the Norwegian Association of Local and Regional Authorities (KS). Such a platform links equipment and technology the users have together with the health and care services' professional systems and enables innovation and new development.

16.4 Conduct more ICT exercises where critical systems are down

Problem description (NOU 2015: 13, section 17.7.4)

There is a need for emergency preparedness in the event of loss of critical ICT services which is due to intentional or unintentional incidents. Fewer manual routines to fall back on may give new and greater vulnerabilities in the future. The Committee believes more ICT exercises should be conducted where critical systems are down

Status of measures

The sector practises cyber incidents on a regular basis and the ICT organisations in the regional health authorities participate in the emergency exercises that are held. Each hospital has plans and routines to manage situations where critical systems, such as patient records, are down. The Ministry of Health and Care Services participated in the nation "IKT16" exercise and an evaluation report is being prepared.

17 Transport

17.1 Strengthen ICT supervision and cooperation between the transport branches

Problem description (NOU 2015: 13, section 18.5.1)

The transport industry is characterised by increasing privatisation and internationalisation, which results in a number of challenges, especially for the authorities' crisis management. It is recommended that the sector reviews the emergency plans and checks these against digital vulnerabilities and back-up solutions. The emergency plan must also have plans to manage digital crises.

It is recommended that the Ministry of Transport and Communication strengthens the supervisory authorities for the transport sector within cyber security. The supervisory authorities must have the capacity and expertise to oversee and guide businesses on Norwegian territory and contribute in international forums.

Status of measures

The Lysne Committee's recommendation to strengthen the ICT supervisory authorities in the transport sector is initially followed-up through the management dialogue between the Ministry of Transport and Communication with underlying supervisory authorities and other businesses. However, there are significant differences between the four transport sectors as regards organisation and distribution of responsibilities and tasks between the different types of administrative bodies, including whether there is a pure supervisory body in each sector and whether ICT is a natural part of the supervisory authorities' task portfolios. In some of the transport modes it is therefore difficult to follow-up the recommendation to "strengthen the ICT supervisory authorities" in the transport sector.

As a basis for further follow-up, the Ministry of Transport and Communication will conduct a further survey within each transport mode as regards the various parties' responsibilities and tasks, mandates, existing requirements and ICT guidelines, etc. Supervisory tasks related to cyber security will form a natural part of such a survey, including the interface with supervisory authorities in other sectors. The Ministry of Transport and Communication will conduct such a survey in 2017. See also the report on establishment of a common arena for the various sectors' key supervisory authorities in section 22.7.

To strengthen cooperation on cyber security in the transport sector, Avinor AS, the Norwegian Coastal Administration, the Norwegian Public Roads Administration, Bane NOR SF (formerly Jernbaneverket) and NSB AS have established the Collaboration Forum on IT Security. At the forum the businesses meet to exchange information and experiences about cyber security in general and security threatening cyber incidents in particular.

17.2 Establish a joint reporting channel for ICT incidents within the transport sector

Problem description (NOU 2015: 13, section 18.5.2)

The Committee believes that there is a need for a common reporting channel both from the authorities to the sector and from the sector to the authorities as regards ICT incidents. It must be possible to alert all relevant parties in the sector. The Committee believes that the Ministry of Transport and Communication should investigate how reporting ICT incidents should be taken care of for the sector.

Status of measures

The Ministry of Transport and Communication, in consultation with relevant underlying agencies, has considered the question of how reporting cyber incidents should be taken care of for the transport sector. Establishment of a common response environment for the entire transport sector has been considered as one of several options. Due to major differences between the transport sectors, it is considered that in this context it is not appropriate to regard transport as one sector, but rather four sectors or transport modes: road, rail, air and sea. Consequently, it has not been considered appropriate to have a common “Transport-CERT”, but instead Avinor, the Norwegian Public Road Administration, the Norwegian Coastal Administration, Bane NOR and NSB have their own response environments that cooperate directly with NSM.

The organisation described above has been further developed and consolidated in connection with planning and implementation of the "IKT16" exercise in November 2016. As part of NSM’s work on establishing a national framework for cyber incident management, the Ministry of Transport and Communication and the agencies together with NSM have defined a participant chart for the transport sector, which describes common notification and reporting channels, among other things. The Ministry of Transport and Communication’s preliminary impression following the "IKT16" exercise is that the chosen organisation and the reporting channels function appropriately. The Ministry of Transport and Communication will use the final evaluation after the exercise as a basis for any action to further develop the transport sector’s capability to handle cyber incidents.

17.3 Special measures for sea transport

Problem description (NOU 2015: 13, section 18.5.3)

The maritime sector is highly dependent on digital systems to safeguard maritime security and efficiency. The Committee observes that different authorities have responsibilities in a complex shipping value chain, at the same time lacking an authority with an overall view of digital vulnerabilities in the entire value chain. It is recommended that the Norwegian Coastal Administration be given an overall responsibility for having a comprehensive overview of the cyber security in maritime value chains and to give advice to the Ministry on priorities that concern digital vulnerabilities.

There is an unsolved problem internationally related to secured digital exchange of passenger and crew information and cargo and customer data. The Committee recommends that the Ministry of Transport and Communication, in cooperation with other relevant authorities, takes the initiative to find a solution to this internationally.

Status of measures

Both the Norwegian Maritime Directorate and the Norwegian Coastal Administration have key responsibilities to safeguard efficient and secure transport by sea. The Norwegian Maritime Directorate is the administrative and supervisory authority for the work on safeguarding life, health, environment and material values on board vessels sailing under the Norwegian flag and foreign vessels in Norwegian waters. This mandate includes securing equipment and material on board, including cyber security. The Norwegian Coastal Administration is a national agency for coastal administration, maritime safety and preparedness against acute pollution and is working actively for efficient and secure transport by sea by taking care of the transport industry’s need for accessibility and efficient ports.

As shown in the Lysne Committee’s report (section 18.4.1), the responsibility for implementation of the international maritime security regulations is shared between the Ministry of Transport and Communication and the Ministry of Trade, Industry and Fisheries, as the Norwegian Coastal Administration is responsible for ports and port facilities, while the Norwegian Maritime Directorate is responsible for ships and personnel. The Norwegian Maritime Directorate is the coordinating authority here.

Future shipping will be heavily influenced by the major changes that take place within digitalisation and automation. Maritime authorities must contribute to development, approval and implementation of new solutions, and cyber security will be an important consideration. An example of this is the cooperation between the Norwegian Maritime Directorate, the Norwegian Coastal Administration and other parties on a pilot project for driverless/autonomous vessels in Trondheimsfjorden.

Establish a comprehensive overview of cyber security in maritime value chains

The Ministry of Transport will consider possible measures to reduce the digital vulnerability within sea transport. This implies that the measures' potential risk-reducing effect is compared with the costs of implementation.

The Lysne Committee's recommendation to give the Norwegian Coastal Administration the overall responsibility for having a comprehensive overview of cyber security in the maritime value chain could conflict with today's division of responsibilities between the Norwegian Coastal Administration and the Norwegian Maritime Directorate.

Matters concerning land, waterways or logistics based on land infrastructure, lie under the Norwegian Coastal Administration, while matters concerning ships, environment, seamen and passengers lie under the Norwegian Maritime Directorate. A national division of responsibilities for the cyber security in the maritime value chain should follow the same plan.

The Ministry of Transport and Communication, in cooperation with the Ministry of Trade, Industry and Fisheries, will conduct a further survey of the Norwegian Coastal Administration and the Norwegian Maritime Directorate's responsibilities and tasks, mandates, existing requirements and cyber security guidelines, cf. the status of the measure "Strengthen ICT supervision and cooperation between the transport modes" (see section 17.1). When the survey has been completed, we will have a better basis for assessing whether the overall responsibility for having a comprehensive overview of the cyber security in maritime value chains should be assigned to the Norwegian Coastal Administration, the Norwegian Maritime Directorate or another authority.

Facilitating a secure identity

Our international obligations require reporting from ship to shore. Transmission of the ship's required arrival and departure times to the Norwegian authorities and ports mainly takes place through SafeSeaNet. The information registered in the message system is made available to various national authorities. These authorities include the customs authorities, the police, the Norwegian Armed Forces, the Norwegian Maritime Directorate and the Norwegian Coastal Administration.

In future an increasing number of systems on board the vessels will have a connection to shore, and cyber security will become relevant in the development of this. The worse-case scenario is that ships may be overridden from shore, and if some manages to access these systems, this could have serious consequences. Internationally, the International Maritime Organisation (IMO) has prepared an overall guideline on the topic of "*cyber security management*".

Effective securing of digital exchange of information between ships and shore requires adoption of an international standard. The Ministry of Transport and Communication will request the Norwegian Coastal Administration to consider further how securing identity can be solved. This should be considered in consultation with the Norwegian Maritime Directorate and other affected authorities.

18 Competence

18.1Establish a general national skills strategy within cyber security

Problem description (NOU 2015: 13, section 19.8)

Cyber security expertise is in short supply in Norway, and it is necessary to implement long and short-term measures. Today, few are educated in ICT subjects, particularly within cyber security. A national competence strategy in the area of cyber security is necessary to ensure long-term funding and thus ensure development of permanent competence environments. If Norway as a nation is to be equipped to meet the increasing digital vulnerability in society, cyber security expertise must be developed throughout the entire education cycle.

Status of measures

The recommendation from the Lysne Committee has broad support in the consultation statements. Emphasis on competence needs for ICT and cyber security is also in line with the Government's overall ICT policy as this is set out in Meld. St. 23 (2015–2016) *Digital agenda for Norway* and Meld. St. 10 (2016–2017) *Risk in a safe and secure society*.

In future, the Government will implement measures to strengthen cyber security competence in Norway, including preparing a national cyber security competence strategy. The strategy will provide guidelines for future measures. See a more detailed discussion of the measure in section 8.1.

19 Crisis management

19.1Increased cyber security competence at local and regional level

Problem description (NOU 2015: 13, section 20.3.1)

Digitalisation of society leads to many challenges at regional and local level. The municipalities are responsible for many important systems and services, and for small municipalities in particular it may be difficult to have adequate cyber security competence. There is a need for increased guidance of the municipalities so that they are able to conduct good risk and vulnerability analyses and develop management systems that take care of cyber security.

The Committee recommends that the Ministry of Justice and Public Security, in cooperation with the Ministry of Local Government and Modernisation, takes the initiative to establish a common area for cyber security at local and regional level. The Committee further believes that there is a need to clarify which requirements and expectations for cyber security are to be placed at local and regional level.

Status of measures

For a long time, the Ministry of Local Government and Modernisation has drawn attention to how the county administration takes care of information security. The Ministry of Local Government and Modernisation has established its own Information Security Committee, and separate seminars have been held in recent years. The Ministry of Local Government and Modernisation has pointed out to the county administration their responsibility in this area.

The Ministry of Local Government and Modernisation has also implemented separate requirements for the county administrations as regards information security. All county administrations are now obliged to use their own management tool to document compliance with requirements and reporting within information security. The requirement means that all county administrations must have started using this tool by the end of 2017.

The Ministry of Justice and Public Security has not yet considered establishing a common arena for cyber security at local and regional level. DSB follows-up the county governors' work on public security, including security related to critical societal functions, including cyber security. Where relevant, questions about cyber security will be a part of DSB's follow-up of the county governors' work regionally and aimed at the local authorities.

19.2 Strengthen emergency preparedness at regional and local level

Problem description (NOU 2015: 13, section 20.3.2)

There is a need to strengthen the ability to detect and manage cyber security incidents at regional and local level. The county governor and the municipalities have not defined reporting lines during cyber security incidents or any response environment that can manage them.

The Lysne Committee believes it should be considered whether the County Preparedness Council should be expanded with representatives from other infrastructures and important suppliers. The Committee also believes that a mechanism must be established to detect and manage cyber security incidents for the municipal sector, and points out the importance of conducting cross-sectoral exercises at local and regional level, which have cyber security as an objective.

Status of measures

In addition to dealing with cyber incidents against own businesses, the local authorities and the county governors play a key role in dealing with the serious social consequences of cyber incidents. In November 2016, the County Governor of Hordaland and the County Governor of Rogaland participated in the national security exercise "IKT16". Unlike businesses, the county governors and the local authorities are not connected to a sectoral response environment. They are also not connected to a sectoral response environment by virtue of having the local and regional coordination role. The Ministry of Justice and Public Security will initiate a process to establish a structure for the local authorities and the county governors' role in the response environments and in the national framework for cyber incident management.

Regional and local level must be ensured access to the same and alternative communication channels (as backup) in the event of loss of electronic channels of communication. This may be the

Norwegian Emergency Public Safety Network, but also satellite telephones, etc. In addition to the County Governor and the local authorities, this also applies to the Civil Defence Force, which during incidents and crises largely cooperates in crisis management and leadership.

19.3 Establish a common classified ICT infrastructure

Problem description (NOU 2015: 13, section 20.3.3)

The Ministry of Justice and Public Security should clarify which ministry will have the overall responsibility for establishing a common classified ICT infrastructure for central administration and clarify the roles and responsibilities the Ministry of Local Government and Modernisation and the Ministry of Defence have in this situation.

Status of measures

The Government has commissioned the Ministry of Defence to be responsible for development and operation of a National LIMITED network (NBN) and National SECRET network (NHN) for the central administration and other selected users. It is important that these information systems are also used in a normal situation, so that the personnel who will use the solutions, have practised and know the system if it is to be used in connection with a possible crisis or war. In addition, the Ministry of Local Government and Modernisation is investigating the possibilities for a common unclassified/low-grade solution for everyone in the new government quarter which is under planning.

In the 4th quarter 2016, the Ministry of Justice and Public Security initiated work to prepare the ministries' offices for a high-grade ICT solution through installation of fibre cables, crypto equipment, etc. The work has meant that all ministries can now receive a high-grade ICT solution as soon as a solution is ready. Preliminary estimates indicate that NHN can be ready for introduction mid-2018.

The Ministry of Justice and Public Security together with the Ministry of Defence and the Ministry of Local Government and Modernisation will assess the existing division of responsibilities at ministry level related to further initiation, introduction, operation and administration of classified ICT solutions, as well as services on the individual platforms.

19.4 Assess means of communication with the public

Problem description (NOU 2015: 13, section 20.3.4)

In the event of major crises and incidents, the authorities must be able to reach the public with information and warnings. Common to most means and channels of communication is that they depend on available electronic communication infrastructure. The Committee recommends that DSB considers using means of communication with the public in crises and in this context also consider the emergency role of national broadcasting company, NRK, in cooperation with the Ministry of Culture.

Status of measures

The Civil Defence Alert Systems (air horns) consist of 1,250 sirens and are an important means for the authorities to alert acute hazard situations. Up until recently, the warnings were given using signals transmitted over the FM network. When the FM network is closed down around the country in 2017, the Norwegian Emergency Public Safety Network will take over this role.

In a crisis situation, the authorities' ability to inform the public will be of great importance. Today, there are three parallel channels for broadcasting government information: radio, TV and internet. The three channels can to some extent replace each other as information carriers. That is to say if radio broadcasts were to fall out, it would still be possible to broadcast the information via the TV and over the internet and vice versa. DSB has been commissioned by the Ministry of Justice and Public Security to initiate an investigation of additional warning methods. One option may be a mobile-based public alert system where it is possible to receive a warning of undesirable, potentially dangerous incidents on your mobile phone.

The Government's strategy to maintain and strengthen the ability for communication with the public has three elements: Firstly, to strengthen the robustness within each of the three channels. Secondly, to strive for a high degree of autonomy for each of the channels, so that not one fault can cause failure in all. Thirdly, to make plans for how such a failure may be dealt with. In Meld. St. 15 (2016–2017) *A modern and future-oriented NRK* the Government emphasises that NRK must still have a special preparedness responsibility. Kriseinfo.no is a channel for government information in crisis situations. DSB is responsible for ensuring that these websites publish verified information from the authorities.

20 Cyber attacks

20.1 Establish and practise a comprehensive framework for cyber incident management

Problem description (NOU 20 13, section 21.11.1)

National security depends on the security of each enterprise, and effective combating of cyber attacks requires good cooperation between the authorities and between the authorities and private stakeholders. Today, there are reports of uncertainty and inadequate coordination between government agencies responsible for combating cyber attacks. It is important to maximise the possibilities within the existing scope for sharing information. Initiative should be taken to establish and practise a comprehensive framework for dealing with cyber incidents on a national level to clarify the efforts between relevant stakeholders within cyber incident management and prosecution. The Committee proposes a bullet list for a level of ambition for the authorities' operational ability to detect, manage and investigate serious incidents.

Status of measures

National incident management is currently based on guidelines provide in the *National Strategy for Information Security with action plan* (2012), *Guidelines for cooperation between the intelligence and security* *services on prevention and management of serious cyber incidents* (2013), *The Ministry of Defence's information security and cyber operation guidelines* (2014), *Model for dealing with cyber security incidents -recommendations and guidelines* (2014) as well as relevant measures in the legislation in the national preparedness plans.

The consultation responses show that there is broad support for the initiative to establish a national framework for dealing with cyber incidents. In 2016, NSM was commissioned to prepare, in cooperation with affected stakeholders, a draft of such a framework. The purpose is to clarify the efforts of the relevant stakeholders within incident management and follow-up the Lysne Committee's recommendations related to the framework. A draft framework was used during the national "IKT16" exercise in November 2016. The evaluation of the exercise and the framework will be completed in 2017 (see sections 7.2 and 8.7).

In the opinion of the Ministry of Justice and Public Security, the Committee's ambition level points are covered by other initiatives in this report.

20.2 Improve the national operational capability through co-location (majority and minority)

Problem description (NOU 20 13, section 21.11.2)

The Lysne Committee addresses two issues in particular: 1) the use of co-location as a means of achieving good cooperation, sharing of information and better use of resources, and 2) whether the police or NSM should coordinate dealing with cyber incidents and be the host of a possible co-location.

There are several small operational environments in Norway today that will cooperate with each other during a cyber incident. A key question is whether Norway is able to exploit the total national capacity to prevent, detect and manage cyber attacks, both in the public and private sector. Private and public stakeholders should share information from open sources and lawfully shareable information to a far greater extent. Co-location may be an important means of achieving good cooperation and use of resources. The Committee proposes facilitating so that those who want co-location can join forces to achieve this.

The majority of the Committee recommends that co-location should be based on the environment that has a tradition for public-private cooperation and is part of the EOS environment, and which currently has the coordinating responsibility for handling cyber incidents. The majority considers NSM the most natural host for co-location. The Ministry of Justice and Public Security must follow-up, particularly with the civil stakeholders in the cooperation, and define clear, measurable success criteria for the cooperation, which will be evaluated within two and five years respectively. The minority of the Committee recommend establishing a Cyber Crime Centre with the police, while emphasising equal cooperation between the public and private sector.

Status of measures

Several of the consultation statements emphasise the importance of fast information sharing, good and clarified cooperation and a good overview of each other expertise and capacity.

A national Cyber Crime Centre has not been established, see section 20.5. The incident management model in Norway has been developed and strengthened over several years, and is a room of opportunity room in today's structure. The Government wants to use the scope in today's structure, with NSM as the national hub, and has therefore prioritised the work on a national framework for cyber incident management and implementation of the national "IKT16" exercise. Through the work on a comprehensive incident management framework, good cooperation between businesses, sectoral response environments, national response environment and the police are strengthened and further developed. Experience from the exercise will be important for further development and improvement of today's model.

Other follow-up related to this point is discussed under sections 6.1, 6.2, 7.3 and 7.6.

20.3Increase detection capabilities and compile a situational picture

Problem description (NOU 2015: 13, section 21.11.3)

Effective detection of cyber attacks requires good detection devices that cover the channels through which the attacks are carried out. This involves more than technological measures. Information sharing in connection with incidents should start earlier than today.

The main recommendations include the following areas:

1. Active and timely information sharing by establishing an appropriate technical platform. NSM must establish a technical information sharing platform for unclassified information with businesses in order to be able to share information quickly and securely.
2. To strengthen detection capabilities through adapted monitoring in each sector.
3. To establish a common situational picture and automatic information sharing.

Status of measures

The consultation statements provide broad support for the initiative. Several measures have been initiated to accommodate the main recommendations. The Government's decision to report on and clarify how a type of digital border defence can be established and regulated by law is discussed in section 7.4. NSM has also prepared an unclassified national situational picture, available via a portal with a login option for response authorities in the various sectors and national decision-makers. NSM will also establish a platform for sharing technical information. The platform will quickly and securely receive and share structured data about threats and other technical indicators with the sectoral response environments. See also section 7.3.

The Government wants to further develop VDI to strengthen the detection capabilities in each sector. The sensor technology will be upgraded. VDI is discussed further in section 7.1.

20.4 Strengthen capacity and expertise related to management of cyber attacks

Problem description (NOU 2015: 13, section 21.11.4)

There are capacity and expertise challenges related to management of cyber attacks. It is important that the specialist environments play an active role towards the academia in order to provide practical experience of value for development of knowledge and to ensure recruitment. Two key areas are covered by the initiative:

1. Evaluate the arrangement with sectoral response environments set up against the cross-sectoral need for incident management. This should be done after the "IKT16" exercise. It is a prerequisite that the sectoral response environments are closely involved in the evaluation. The evaluation should examine whether the division into sectoral response environments is appropriate, or whether the response environments for sectors with similar challenges should be merged.
2. Report on a national cyber-reserve for dealing with cyber incidents, a reserve that should be able to scale the efforts in the event of major incidents and crises.

Status of measures

The consultation statements show that there is broad consensus on strengthening the national capacity and expertise related to dealing with cyber attacks and to establish a national cyber reserve.

The Government follows-up the national incident management model and the recommendation from the Lysne Committee through the evaluation of the "IKT16" exercise and the development of a national framework for management of cyber incidents (see section 7.2). This includes a review of the establishment and organisation of sectoral response environments. The evaluation of the exercise and the development of the framework take place in close cooperation with the affected stakeholders.

The Ministry of Defence and the Ministry of Justice and Public Security have requested NSM, during the long-term plan period 2017-2020, to consider a cross-sectoral cyber-reserve for incident management in the event of particularly major crises that require additional personnel. The report will examine the requirements that must be set for personnel in such a model and the environments or persons it would be natural to involve in such an initiative. Other aspects that must be clarified include legal matters, the need for personnel clearance, and exercises and training to maintain expertise.

NSM has established a pilot project with a quality system for providers of cyber incident management services. The purpose of the scheme is two-fold: Firstly, the scheme will help businesses that experience an cyber security incident to choose a service provider that satisfies NSM’s technical requirements at the time of application. Secondly, the scheme will help raise the security expertise within incident management in Norway. If it becomes well-known, the scheme may also represent a national increase in capacity within national incident management.

20.5 Establish a national Cyber Crime Centre

Problem description (NOU 2015: 13, section 21.11.5)

It is the opinion of the Committee that police preparedness capabilities and task-solving in the digital space are far from adequate and not adapted to society's expectations and the risk society faces. The Committee supports the proposal in the Ministry of Justice and Public Security's strategy from 2015 for combating cybercrime to establish a new national centre to prevent and combat cybercrime. The centre should be organised under Kripos. The Specialist Agencies Committee (Særorganutvalget) should consider whether alternative forms of organisation are more appropriate than building capacity.

Status of measures

A national Cyber Crime Centre has not been established. The National Police Directorate (POD) has drawn up a specific proposal for how to establish such a centre in the police to prevent and combat cybercrime, including the tasks that should be assigned to the centre, organisational anchorage and resource requirements. The proposal implies that the police must allocate significant resources,which for some functions requires external recruitment of competence the police does not have today. Therefore, the proposal must be dealt with in the ordinary budget work, and assessed against other important initiatives.

In 2016, the Ministry of Justice and Public Security set up a committee to examine the function and capacity among the police specialised agencies. The Committee reports that combating cybercrime is a main challenge for the police. In May 2017, the Committee submitted its report to the Ministry of Justice and Public Security, and the report is being distributed for broad consultation.[25]

20.6 Ensure strong specialist cybercrime units in the police districts

Problem description (NOU 2015: 13, section 21.11.6)

Digital expertise in the police must be established in all the police districts. In the police districts there is a need for improved and more specialised expertise and skills and increased quality of police work. The Committee recommends that a major promotion of post-qualifying and further education for fully fledged police officers. The Committee also believes that the Ministry of Justice and Public Security should provide clear guidelines to the police districts to ensure the necessary interdisciplinary expertise in the police, including civil employees with a technical background.

The Committee recommends that the police districts' specialist environments are significantly strengthened. In the work of the police on the internet, the open presence, including "police station and patrolling online" should be assigned to each police district. The Committee believes that a

[25] NOU 2017: 11 *Better assistance Better preparedness. The future organisation of police specialist agencies.*

clear interface between what the Cyber Crime Centre deals with, and what the police districts themselves are expected to deal with, is crucial.

The present management model in the police must not prevent assessment of various models for organisation of combating cybercrime, including in the specialist agency report.

Status of measures

The police must be put in a better position to operate in the digital landscape. Police cyber expertise and capacity must be strengthened in all the police districts. In accordance with the Ministry of Justice and Public Security's strategy of 2015 to combat cybercrime a plan has been drawn up to strengthen the investigation capacity. The police will prioritise resources to combat cybercrime and use digital footprints to a greater extent than today.

The foundation for stronger specialist cyber environments in the police districts will be established through the Community Police Reform. A functional description of digital police work has been prepared as part of the reform. The digital police work function will ensure broad, efficient and appropriate use of digital information and electronic footprints in the police work, including investigation, prevention, stopping criminal offences, assistance to the public, returning the situation to normal, investigation and bring cases to trial. Through use of technology and electronic footprints the function will ensure that more criminal cases can be investigated quickly and with good quality of the methodology, securing of evidence and analyses.

POD has drawn up a strategy for digital skills upgrading in the police training. The strategy covers the basic training and post-qualifying and further education and is based on the work done at the National Police Academy.

20.7Ensure an ICT infrastructure to support police crime prevention

Problem description (NOU 2015: 13, section 21.11.7)

The Committee finds that the ICT situation in the police is critical. There is a need for long-term and extensive efforts in terms of stability in the fundamental infrastructure and security in applications and services. In addition, there is a need to establish common national solutions as a substitute for various local solutions.

The Ministry of Justice and Public Security should implement measures to ensure police a technological boost, with focus on the ICT management and supervision, an increase orderer expertise and give clear priorities for use of resources in a long-term perspective.

Status of measures

The basic infrastructure of the police has been gradually modernised in recent years, but there is still some catching up to do and there are shortcomings in several areas. In recent years there have been several serious incidents where the operational capabilities of the police have been affected by faults in the ICT systems. In addition, employees in the police force too often find that they do not get done what they are supposed to do, or are being seriously delayed due to the systems.

Strengthening the police ICT infrastructure is a priority area for the Ministry of Justice and Public Security. A good ICT infrastructure is necessary so that the police are able to realise benefits related to the Community Police Reform, working efficiently on combating cybercrime and making use of appropriate applications and equipment.

20.8Ensure the balance between privacy and a more secure society

Problem description (NOU 2015: 13, section 21.11.8

To achieve a more secure society, invasive methods are often proposed without adequately considering or accounting for the balance between privacy and freedom of speech. The Committee believes there is a need to maintain the balance between privacy and a more secure society through studies and public debate The Committee points in particular to two areas where important considerations must be made to find the right balance between conflicting interests:

1. Report on the introduction of digital border monitoring through an NOU, or other public report
2. Report on the police and PST's covert use of methods on the internet

Status of measures

The consultation statements show that there is broad consensus on these recommendations. The Norwegian Data Protection Authority in particular is critical to mass monitoring of the general public and believes that new and invasive methods should always be reported on. See the reference to privacy in Chapter 4.

Report on digital border monitoring

As a follow-up of the recommendation by the Lysne Committee, the Ministry of Defence set up a committee to report on key issues related to digital border monitoring. The Committee presented its report to the Ministry of Defence on 26 August 2016. The report recommends the establishment of a digital border defence that gives the Intelligence Service access to digital data streams that cross national borders in fibre optic cables. The prerequisite for the recommendation is that a strict control regime is established consisting of technological and human control mechanisms.

The Government supports the conclusion of the Committee and believes there is a need to establish a form of digital border defence. Therefore, the Government will investigate and clarify how such a digital border defence can be established and regulated. See a more detailed discussion of this in section 7.4.

Report on police covert techniques on the internet

The Government agrees with the Committee's recommendation to report further on PST and police covert techniques on the internet in case PST proposes registering opinions voice on social media and analyse information from open channels.

21 Common components

21.1 Monitor the development of ICT outsourcing of common components

Problem description (NOU 2015: 13, section 22.6.1)

The public sector has established a number of open, reusable solutions that meet typical needs in the field of digitalisation, such as login, authentication, registers and the like. For example, this applies to the ID port, which the public the same login functionality regardless of which agency or municipality you log into.

It is reasonable to believe that there will fewer data centres, that more of the data centres will be operated by external businesses, and that more community functions will share infrastructure as data centres. This may change the vulnerability situation. The Ministry of Local Government and Modernisation should monitor the vulnerability development related to outsourcing ICT services for public registers and community services.

Status of measures

The Ministry of Local Government and Modernisation follows the work in dialogue meetings with other ministries that are joint component owners, but have no activities other than this, as it is the responsibility of the sector ministries. The Ministry of Local Government and Modernisation follows-up its own components in dialogue with Difi and makes continuous assessments of security, operation and administration. See also sections 6.4 and 22.10 on outsourcing and section 22.1 on ensuring a comprehensive assessment of value chains.

21.2 Develop common protection measures against sophisticated cyber attackers

Problem description (NOU 2015: 13, section 22.6.2)

It requires expertise to identify and deal with sophisticated attackers. The current capabilities and capacity to detect these attackers is not adequate in Norwegian businesses. There is a need to start development of mechanisms that the owners can use to secure common functions against sophisticated attackers. Difi should play a coordinating role in this work, and it should be done in cooperation with the research environments and with assistance from NSM.

Status of measures

The Committee proposes that Difi plays a coordinating role in the work on developing mechanisms that the enterprise owners can use to secure common functions against sophisticated attacks. The Ministry of Local Government and Modernisation agrees with this. According to the principle of responsibility, it is the enterprise and the sector ministry that will protect (national) common components. All common components can link to NSM's Early Warning System for Digital Infrastructure (VDI). This is one of several initiatives available to the businesses responsible for national common components. Other initiatives are valuation and risk analysis, security audits, cooperation on strong cyber security environments and intrusion testing. Difi's role in this context is to provide advice and guidance to the businesses on how they should approach the work, and facilitate exchange of experience. This is done in cooperation with the research environments and with assistance from NSM.

21.3Regulate electronic identity

Problem description (NOU 2015: 13, section 22.6.3)

The Lysne Committee writes that the field of e-ID has been characterised by some indecision since the work began around the new millennium. A public ID card with associated e-ID has repeatedly been on the cards, without coming to fruition. There are currently several private parties that issue e-ID, and there are different needs for e-ID between businesses and sectors. The Committee recommends following five initiatives regarding e-ID:

1. Identify personal information that the e-ID providers receive through use. Solutions with trusted third parties mean that the e-ID provider gets to know what the users are doing with their electronic identity online. Nkom, together with the issuers, should prepare a comprehensive overview of how much personal information the various e-ID providers receive through use of the e-ID and how this information is stored. Furthermore, the Ministry of Local Government and Modernisation should review the regulations in this area, so that the e-ID providers are not forced to store unnecessary personal information.
2. The Ministry of Local Government and Modernisation should prepare a clear definition of the security levels. This should be based on combinations of the attacker's capabilities and the consequence of the attack. It must be easy to decide whether an e-ID achieves a security objective. This should be done at the same time as the adaptations in connection with the new EU regulation.[26]
3. Use of single login portals should be limited, as such portals observe all logins to very many services, and incorrect integration of the e-IDs may undermine the security.
4. Existing e-ID solutions should be improved rather than waiting for the national ID card. Difi should further develop the existing MiniID solution, by providing a more secure method of issuing identities, equivalent to "qualified certificates", and improved technical solutions. Difi and Nkom together should encourage and require greater security and openness with private providers, preferably based on standard technical solutions.
5. The authorities should exercise caution when offering services with sensitive personal information to the general public.

[26] Electronic identification and trust services (eIDAS).

Status of measures

Electronic identity is governed by the *Electronic Signature Act* (2001), the *Framework for authentication and non-repudiation in electronic communication with and in the public sector* (2008) and through the *Requirement specification for PKI in the public sector* (2010). The Electronic Signature Act comes under the Ministry of Trade, Industry and Fisheries. The requirement specification is pursuant to section 27 of the e-Administration Regulations. Both the framework and the requirement specification come under the Ministry of Local Government and Modernisation's area of responsibility and are part of the current strategy for use of e-ID.

Several processes are now in progress that will affect regulation of electronic identity and the Lysne Committee's five-point list with recommendations. The Government has decided that a national ID card will be equipped with an e-ID, and that this e-ID will be a supplement to the current market solutions used for login to the ID port. The launch will be in 2018.

The Government wants Norway to be part of the digital internal market in Europe. A main element of this is that the European countries will approve each other's electronic identification solutions, e-ID, and a number of so-called trust services that facilitate electronic cooperation. The EU regulation on e-ID and electronic trust services (eIDAS) will be implemented as a separate Act and replace the current Electronic Signature Act. The Ministry of Trade, Industry and Fishing is responsible for implementation of the regulation in cooperation with the Ministry of Local Government and Modernisation. The Ministry of Justice and Public Security will follow-up that the public security perspective is ensured in the work.

The purpose of the amendments is to facilitate increased electronic cooperation between businesses, citizens and public authorities across national borders in the EU/EEA and thereby contribute to stronger economic growth in the internal market.

22 Cross-sectoral initiatives

22.1 Establish a national framework to ensure a comprehensive assessment of value chains

Problem description (NOU 2015: 13, section 23.1)

Long and complex value chains make it difficult to have an overview of digital vulnerabilities. The value chains may span over several stakeholders and sectors that may be subject to different legislation and supervisory authorities. A national framework to ensure a comprehensive assessment of value chains may contribute to valuation of the information carried in the value chains, and to set an acceptable risk level for digital vulnerability.

The Committee proposes measures that provide a fundamental approach in order to grasp how digital vulnerability occurs and develops in the value chains. The Committee believes the Ministry of Justice and Public Security should develop a framework to address comprehensive perspectives in valuations and vulnerability assessments. The Committee also proposes using this framework for further initiatives that contribute to the greatest possible transparency about the residual vulnerability that you have accepted as a user of equipment and services and which assets you entrust to your sub-contractors.

Status of measures

DSB's rapport, *Critical societal functions* (2016) points out that all businesses that are responsible for essential functions must plan to be able to maintain their business. Identification of own vulnerability and implementation of measures to reduce this vulnerability are part of this. The report states that it is the owners and operators of the infrastructures who are responsible for the security and the functionality of the systems. The role of the authorities in this context is to be a driving force, guide, set requirements and supervise.

The Ministry of Justice and Public Security will request DSB to report on the question of establishing a national framework to ensure a comprehensive assessment of value chains, and whether a set of standard formulations should be drawn up to define different levels of robustness.

22.2 Clarify requirements for business management systems

Problem description (NOU 2015: 13, section 23.2)

Business management systems must be able to show a vulnerability picture based on risk assessment of intentional and unintentional ICT incidents. The business management systems should also provide a basis for considering the impact of various preventive measures in the cyber security area and the consequences failure would have for society. This will provide a better basis for prioritising different cost-driving preventive measures.

The Committee recommends that the different ministries clarify requirements and guidelines in the business management systems, both at central level and out in the various sectors. The supervisory authorities must follow-up that this is taken care of. The Committee recommends that the Ministry of Justice and Public Security draws up a set of minimum requirements for the elements to be included in the business management systems, and guidance materials should be prepared that can strengthen expertise in the area.

Status of measures

The Committee's recommendations points primarily at the ministries and that they must clarify requirements and guidelines for business management systems in their own sector. The consultation statements show that there is broad consensus on these recommendations.

Section 15 of the e-Administration Regulations contains a requirements regarding use of an information security management system. All administrative bodies that use electronic communication must have a described objective and strategy for information security. The Ministry of Local Government and Modernisation has selected Difi as the agency that will provide recommendations in the area to the public administration. In 2016, Difi launched its guide *Internal control in practice - information security*.[27] The guide is primarily aimed at public businesses, but is available to everyone on Difi's website. NSM also administers a guide to security management (last updated in 2015).[28] The purpose of the guide is to give advice to businesses on how a security management system may be established and further developed.

NSM is working to establish a comprehensive and systematic set of the most important minimum requirements and measures to secure ICT that are important to society through basic principles of cyber security. The basic principles will facilitate reuse in and across the various sectors by building on established international standards. The principles will make it easier for sectors and businesses to meet the requirements in various regulations and in this way facilitate common technical solutions. The purpose of this is to provide decision-makers in public and private businesses with a package of measures to secure their businesses and information systems. The first package of measures will be published in 2017 with subsequent regular revisions and updates.

22.3 Conscious use of standards

Problem description (NOU 2015: 13, section 23.2.1

The cyber security requirements in the public sector are usually function-based and have defined overall objectives. There is usually reference to use of standards in areas where function-based regulations exist. Norway should implement to a great extent standards that are international recognised, and in the field of ICT it is not very appropriate or necessary to produce special Norwegian standards. However, it is important that Norway contributes and is active in drawing up standards internationally. The Ministry of Justice and Public Security has a special responsibility for the standards that deal with cyber security, and which are not directly related to a specific sector. The Committee recommends that the Ministry of Justice and Public Security has a strategic approach to how it will contribute to the standardisation work.

Status of measures

The consultation statements provide broad support for the initiative and point out that standards contribute to common use of terms and definitions. Internationally, good standards have been developed, which are revised regularly in line with the technological development. Development of own Norwegian standards within cyber security is therefore not appropriate.

The Government wants Norway to be present at international arenas where cyber security standards are developed. The Ministry of Justice and Public Security has entered into cooperation with Standard Norway for this purpose and in 2016, the Ministry has granted Standard Norway funding for the work programme *standardisation in cyber security*.

[27] Difi’s guide material “Internal control in practice”: http://internkontroll.infosikkerhet.difi.no/.

[28] Guide to security management, NSM (2015).

Standard Norway organises the work for international influence with relevant stakeholders to ensure Norwegian interests in the development of international cyber security standards. Re-establishment of a Norwegian Mirror Committee will help clarify the need for standards within the field of cyber security. It will develop a separate work programme with an overview of the work to be followed up on the Norwegian side. The work programme is long-term and will be in line with Norway's digital efforts, but also European work and the EU Commission’s cyber security plan.[29]

The Ministry of Local Government and Modernisation also provides Standard Norway with an annual grant via Difi. The purpose of the grant is to support Standard Norway in the dork on ICT standardisation in general and follow-up work within cyber security standardisation and to contribute to transfer of expertise in the area between Standard Norway and the administration. Several government agencies are also contributing in the standardisation work.

22.4 Clarify the Ministry of Justice and Public Security’s role and area of responsibility

Problem description (NOU 2015: 13, section 23.2.1)

In the view of the Lysne Committee, the Ministry of Justice and Public Security’s coordinating responsibility for preventive cyber security in the civil sector includes the public and private sector. Each specialist ministry is responsible within its own sector. The Committee recommends further clarifying the responsibility for cyber security, so that it is clear that the Ministry of Justice and Public Security’s coordinating responsibility applies to both the public and private sector. If necessary, such clarification may be in the form of a revision of the Royal Decree of 22 March 2013.

Status of measures

The Ministry of Justice and Public Security has a coordinating responsibility for cyber security in the civil sector. Roles and responsibilities are specified in Meld. St. 10 (2016–2017) *Risk in a safe and secure society* and the Royal Decree of 10 March 2017 relating to responsibility for public security in the civil sector at national level and the Ministry of Justice and Public Security’s coordination role within public and cyber security's coordinating role within public and cyber security.

To create a common approach to cyber security in the public administration, the specialist authorities must provide recommendations that are coordinated. The Ministry of Justice and Public Security, the Ministry of Local Government and Modernisation, NSM and Difi meet regularly to coordinate the efforts and benefit from each other’s expertise.

[29] *Rolling Plan for ICT Standardisation*, European Commission (2017).

22.5 Strengthen the Ministry of Justice and Public Security's policy instruments

Problem description (NOU 2015: 13, section 23.3.2)

The Ministry of Justice and Public Security must take further steps to gain an overview of digital vulnerabilities across sectors. It is recommended that the Ministry requests NSM and DSB in cooperation to prepare a common methodological framework that may form the basis of a comprehensive annual overview of digital vulnerability. Furthermore, that the Ministry of Justice and Public Security prepares a comprehensive overview of digital vulnerabilities. The overview will contribute to comparative cross-sectoral comparisons and provide a knowledge base for the use of policy instruments and priorities across sectors.

The Ministry of Justice and Public Security's coordinating responsibility should include coordination of minimum cyber security requirements in the civil sector. The Ministry of Justice and Public Security is recommended to actively follow-up the process regarding the EU's NIS Directive and consider the consequences the Directive may have for Norway, and how this may affect the Ministry of Justice and Public Security's coordination role in the area, especially with regard to providing guidelines, and setting requirements for other ministries and preparing the sectors for implementation of the Directive.

Society's technological dependence means that technology and major structural changes have consequences for the digital vulnerability. The Committee recommends looking at how the Norwegian Competition Authorities addresses competition considerations in the event of organisational and structural changes in the market. The scheme should be taken care of by the Ministry of Justice and Public Security.

The Committee points in particular to the importance of cooperation with the private sector. The Committee recommends that the Ministry of Justice and Public Security considers whether the public-private cooperation in the area of cyber security is adequately addresses and appropriate, and whether there is a need for a strategic arena for cooperation with owners of critical infrastructure and information and with academia, under the management of the Ministry of Justice and Public Security.

Status of measures

Prepare a common methodological framework for, and an annual comprehensive overview of, digital vulnerabilities

In 2015, NSM prepared its first *Comprehensive ICT risks* report. The purpose of the report is to establish a common situational picture that enables businesses and authorities to make the right decisions. In addition, it provides a tool for businesses in their work on preparing risk assessments. The report is published annually. NSM has been commissioned to further develop the report in cooperation with other relevant businesses, including DSB. More information on this is found in section 6.6.

Coordination of minimum ICT requirements in the civil sector and follow-up of the NIS Directive

On 6 July 2016, the European Parliament and the European Council's Directive (EU) 2016/1148 concerning measures for a high common level of security in network and information systems across the union (the NIS Directive), was adopted by the EU. The Government believes that the NIS Directive is EEA relevant and acceptable.

The purpose of the Directive is to improve the internal market's function. A high common cyber security level will strengthen European the competitiveness of European businesses in a globalised world, create trust in a globalised world and contributed to economic growth in Europe. Furthermore, an increased level of security will reduce the costs associated with security breaches and cybercrime.

The Directive lays down obligations for all member states to adopt a national strategy on the security of network and information systems, to establish a computer security incident response teams (CSIRT) and to establish security and notification requirements for operators of essential services and for digital service providers; The Directive establishes two international cooperation groups - one at strategic level and one at CSIRT level.

The Ministry of Justice and Public Security is responsible for following-up the NIS Directive. It has not formally been decided that the Directive will become Norwegian law. However, Norway participates as an observer in NIS' expert group, the NIS committee and NIS' cooperation group. Through the Ministry of Justice and Public Security's participant in these groups Norway will contribute to further work on the Directive in the future. The international participation provides a good basis for possible implementation of the Directive in Norwegian law. Implementation will mean that through the law a minimum level of computer security and notification requirements will be introduced for operators of essential services and digital service providers. The authorities will check that the Directive is complied with as provided-

Take into account cyber security in the event of technology changes and structural changes in society

Section 6.4 of Meld. St. 10 (2016–2017) *Risk in a safe and secure society* states that all ministries in the civil sector are responsible for following-up requirements and recommendations given by the Ministry of Justice and Public Security for own businesses and in their own sector. The ministries will involve the Ministry of Justice and Public Security in processes where cyber security considerations are of national importance, particularly in the event of technological and structural changes in society.

Establish an arena for public-private cooperation

The Government is committed to strengthening public-private cooperation, and a special forum will be set up to support the national work on cyber security. See a more detailed discussion of this in section 5.1.

22.6 Increase cyber security capacity in the Ministry of Justice and Public Security

Problem description (NOU 2015: 13, section 23.3.3)

The Committee recommends strengthening the Ministry of Justice and Public Security's resources in the field of cyber security to attend to the Ministry's role and implement the measures that follow from the Lysne Committee's report.

Status of measures

The Ministry of Justice and Public Security supports the Lysne Committee's assessment related to the need to strengthen the Ministry in this area. The Ministry of Justice and Public Security experiences a steady increase in the inflow of tasks, expectations and needs within follow-up of national cyber security, also related to follow-up of the Lysne Committee's report.

The Ministry of Justice and Public Security has experienced significant strengthening in the area since the Ministry took over coordinating responsibility in 2013. It is important to note that this strengthening on its own creates challenges for partners who have not experienced the same strengthening, and who are noticing an increased inflow of tasks as a result of the Ministry of Justice and Public Security's increased activity. In the view of the Ministry of Justice and Public Security, the capacity needs within cyber security in the central ministry and specialist environments must be seen in context.

22.7 Adapt the supervisory activities to include cyber security

Problem description (NOU 2015: 13, section 23.4)

The Committee recommends that when the supervisory authorities formulated new requirements and guidelines for regulated businesses, they must take into account the assessments of function-based regulations. When setting cyber security requirements, function-based regulations and supervision should be considered - this is in order to be able to keep up with fast technological changes and to facilitate security measures that are tailored to each enterprise.

According to the Committee's assessments, there is a need to strengthen cyber security competence within several sectoral supervisory authorities. In the short-term, it will be important to have shared resources so that expertise may be supplied to various sectoral supervisory authorities from, for example, the National Security Authority in individual cases. In the long-term, developments indicate that the supervisory authorities must establish their own expertise. The Committee recommends that the Ministry of Justice and Public Security takes the initiative to establish a common arena for supervisory cooperation in the field of cyber security.

Status of measures

The consultation statements show that this is an important measure, and there is good work on skills upgrading in several sectoral supervisory authorities. For example, NVE has increased the number of personnel and a similar process is in progress in PSA. Nevertheless, the shortage of cyber security competence in society makes it difficult to staff all sectoral supervisory authorities with adequate expertise in the field.

To improve cyber security and the quality of cyber security supervision conducted in the various sectors, the Ministry of Justice and Public Security and the Ministry of Defence will investigate and establish a common arena for the various sectors' key supervisory authorities. The purpose is to contribute to information sharing and transfer of competence and in this way increase the quality of the sectors' supervision of cyber security. The ministries have requested NSM to establish and lead such an arena.

Difi and FFI have been commissioned by the Ministry of Justice and Public Security to evaluate the supervisory activities that DSB carries out on behalf of the Ministry of Justice and Public Security. Within the field of cyber security, the evaluation shows that more than half of the ministries see a need for intrusion testing in addition, or as an alternative to the current supervision Use of intrusion testing may be an effective means of detecting vulnerabilities in an information system. However, it is important that use of such testing is in addition to, and not as a substitute for systematic work on cyber security in the businesses. Section 6.5 provides a more detailed description of intrusion testing. Section 8.6 provides a more detailed description of expertise in supervision.

22.8 An account of cyber security should be included in annual reports

Problem description (NOU 2015: 13, section 23.5)

Responsibility for cyber security lies with senior management in public and private businesses. The Committee's investigations indicate that the work on cyber security does not always receive the priority it should have. To ensure that the work on cyber security is given higher priority, a requirement should be introduced that ensuring cyber security is described in the businesses' annual reports. The Committee calls on the Ministry of Trade, Industry and Fisheries and the Ministry of Local Government and Modernisation to prepare an amendment in the public and private sector legislation respectively.

Status of measures

The consultation statements have a somewhat divided view on this measure. The reporting obligations in the annual report should be assessed based on whether it provides a good enough benefit compared with the costs and time spent on the reporting.

The Ministry of Finance has laid down requirements for government agencies' annual reports in the financial regulations. It is a stated goal that reporting must be kept at a moderate level. The requirements for content of the annual accounts and reports for accountable businesses are governed by the Act relating to annual accounts, etc. Chapter 3 (the Accounting Act). This Act belongs under the Ministry of Finance's area of responsibility, but other requirements for presentation of annual accounts are also found in other legislation. The requirements should be harmonised, but each ministry is responsible for following-up the regulations within its area of responsibility, including also in accordance with the central guidelines that are given.

22.9Industrial and commercial development and cyber security

Problem description (NOU 2015: 13, section 23.6)

A strong cyber security industry in Norway will be a positive contribution to reduce digital vulnerabilities. This will ensure expertise and contribute to awareness and dissemination of knowledge throughout Norwegian society. Therefore, the Committee recommends that the Government strengthens the work by looking for means of stimulating industrial and commercial development in this area, for example, through fiscal policy, subsidy schemes and competence building in dialogue with industry and commerce.

Status of measures

The main objective of business policy is to facilitate the greatest possible value creation in the Norwegian economy within sustainable frameworks. The business policy must facilitate the use of resources where they are best used to ensure the greatest value creation. Therefore, the objective of the business policy is to facilitate good framework conditions and policy instruments that have a wide scope, and seek actively to facilitate well-functioning markets by correcting market failure where appropriate. The Government's policy on taxes, research & development and innovation must facilitate competitive development within all industries, including the cyber security industry. The Government will facilitate for future industry and commerce by ensuring access to expertise and continuing to focus on research, innovation and technology development.

In addition, innovation in industry and commerce is facilitated through the Research Council of Norway and Innovation Norway's schemes. Business stimulating means that may be used within the cyber security industry are the general schemes Skattefunn and User-managed Innovation Area (BIA) from the Research Council of Norway.

22.10 Outsourcing and cloud services

Problem description (NOU 2015: 13, section 23.7)

Use of outsourcing and cloud services in public and private businesses is expected to increase in future. Although outsourcing and use of cloud services may contribute to increased technical cyber security, the enterprise is not exempted from cyber security responsibility and the work.

The Lysne Committee believes the Government's work to remove unnecessary obstacles, clean up statutory barriers and facilitate secure solutions is important. In particular, the work that deals with what kind of information may be stored where, including the provisions of the Archives Act and the Bookkeeping Act, should be highlighted. There should also be a joint assessment across the sectors to establish a common inspection practice for data stored in cloud services. This includes use of third-party auditors.

In a special note from one of the members of the Committee, it is emphasised that in the policy formulation related to digital vulnerabilities and cloud services, the Ministry of Justice and Public Security must also see the possibility the technology provides to increase security. This should be done in consultation with the Ministry of Trade, Industry and Fisheries and the Minister of Local Government and Modernisation.

Status of measures

In 2016, the Ministry of Local Government and Modernisation presented a national strategy for use of cloud services. The goal of the strategy is to make it clear how public and private businesses can benefit from using cloud services, and when such services are suitable for use in the public sector, The Ministry has commissioned Difi to establish a competence environment and guidance resources related to procurement of cloud services. This includes assessments related to security and risk, including valuation of information, and to collect recommendations from the various sectors in this area.

The Ministry of Local Government and Modernisation is also considering whether to develop a market place or other mechanisms that make assessment and procurement of cloud services easier for the businesses.

The Ministry of Local Government and Modernisation has begun work on harmonising the way the different supervisory authorities work when they supervise information security in cloud services. Experience so far is that the differences in supervisory practises are smaller than previously thought. The Ministry of Local Government and Modernisation finds that the supervisory authorities are interested in sharing experiences and learning from each other in this area.

The Ministry of Local Government and Modernisation has discussed use of third-party audits with supervision- There are few supervisory authorities that have specific experience with this, but those that do, have generally positive experiences. This is also an area that is important for the EU Commission, and the Ministry of Local Government and Modernisation participates in and follows the work that takes place within cloud services and free flow of data in the EU. The Government considers that it would not be expedient to initiate a separate report in this area, but will continue to assess the status and participate in relevant EU work in this area.

The Ministry of Culture has distributed revised archive regulations for comments. The consultation deadline was 15 January 2017. The revised regulations allow storage of digital public archives abroad (section 22), given that the service provider satisfies the requirements set for storage of archive material. The Ministry of Local Government and Modernisation will now look at a possible expansion in where to store accounting data. Today, it is only allowed to store this in the Nordic countries.

The Ministry of Justice and Public Security, the Ministry of Defence and the Ministry of Local Government and Modernisation will consider the possibility of establishing a cloud solution with a high security level. An important purpose is to consider how central authorities with special security requirements may also use the efficiency possibilities that cloud services provide. NSM and Difi are carrying out the assessment.

See a more detailed discussion of outsourcing in section 6.4.

22.11 Regulation of cryptography

Problem description (NOU 2015: 13, section 23.8)

Cryptography is techniques that will secure the origin of the information, prevent access and detect change. Use of cryptographic mechanisms is of great importance to cyber security and is a prerequisite for secure electronic communication. The Lysne Committee is of the opinion that use of cryptography must not be regulated or forbidden in Norway. Norwegian authorities should work actively against regulation or prohibition internationally. In the event of increasing use of cryptographic mechanisms to protect information and communication new investigative methods should developed to ensure efficient police and intelligence work.

Status of measures

Use of encryption must not be forbidden or regulated

The Government concludes that the Committee believes that encryption must not be forbidden or limited by law. This does not affect the current regulation of crypto-security in the Security Act. The Government also concludes that when the Committee writes “not to be regulated” /”work actively against regulation”, it does not mean regulation in the form of an order on encryption by law, such as is required by the various regulations to secure personal data.

The Government generally agrees with the Committee’s conclusions not to prohibit or regulate use of cryptography. Encryption and access to robust encryption methods are a prerequisite for communicating securely so that the communication content is not intercepted.

Norwegian authorities should work actively against regulation or prohibition internationally.

The authorities maintain their views in relevant international forums, such as the EU and OECD.

Development of new investigative methods

The need for development of new investigative methods is closely linked to the above point about the spread of encryption. Increased use of encryption creates challenges for the police and the prosecuting authority.

In Prop. 68 L (2015–2016) *Amendments to the Criminal Procedure Act, etc. (covert coercive measures)* the Government proposed legislative amendments granting the police extended access to use covert coercive measures in investigation, avoidance and prevention of serious offences. Among other things, it was proposed to introduced data reading as a new, covert coercive measure pursuant to sections 216 o and 216 p of the Criminal Procedure Act. The proposal was based on “a great and unmet need for effective access to electronically stored and communicated information. Today, information is often produced, processed, communicated and stored electronically and by using mobile services. At the same time, the use of encryption solutions and other methods for protection of such information is increasing”. The proposal was adopted with broad support in the Storing, with some minor changes. Act no. 4 of 17 June 2016. 54 relating to amendments to the Criminal Procedure Act, etc. (covert coercive measures) entered partly into force on 17 June 2016, with the exception of the provisions on data surveillance, which due to regulatory amendments did not come into force until 9 September 2016.

In other respects, the Government would like to point out that when assessing new investigative methods it is crucial to thoroughly assess the consequences of the new methods on privacy and look at the intervention the new methods represent in the context of existing privacy concerns.

Norwegian crypto-policy

NSM has close cooperation with the Norwegian crypto-industry to develop high-grade crypto solutions. Establishing expertise and research environments is a long-term process and knowledge of encryption must be maintained if it is to be relevant. Without competent national specialist environments the Norwegian authorities and companies will have to be in contact with foreign parties to obtain qualified assessments and advice on cryptographic systems. This will be unfortunate seen from a national security perspective.

To help secure the necessary national crypto-competence and stimulate innovation and product development, the Ministry of Defence and the Ministry of Justice and Public Security will revise the national crypto policy.[30]

[30] Meld. St. 10 (2016–2017) *Risk in a safe and secure society*.

Part IV
Financial and administrative consequences, etc.

23 Financial and administrative consequences

In the Government's political platform *safety and security in everyday life and enhanced preparedness* are highlighted as one of eight important priority areas. This report to the Storting explains the Government's policy for the cyber security work.

Cyber security is a broad subject area that affects most sectors and many different areas of society. The report is not intended to provide an exhaustive account of all of matters of importance to cyber security, but highlights some important priority areas.

Significant parts of the cyber security work takes place in each sector, based on relevant sectoral legislation as well as specific requirements for the ministries' public security work and work on cyber security. The work will be an integral part of the ordinary management. If the risk and vulnerability situation changes, it is important that the measures and the public policy system are adjusted accordingly. Change in use of policy instruments and possible measures implemented as a result of changes in the risk and vulnerability situation, will be covered within the applicable budget limits. If measures result in an increase in expenditure over the national budget, the Government will come back to this in connection with the annual budget proposals.

The Government aims to strengthen the cyber security work in several key areas. The report points out strategies and action plans, among other things, for the next few years that could involve additional expenses. The measures will initially be covered within the applicable budget limits. The Government will come back to any expenses or savings that go beyond the current budget limits in connection with the annual budget proposals. Therefore, it is not possible to state exactly when the measures can be implemented.

The Ministry of Justice and Public Security

recommends:

The recommendation by the Ministry of Justice and Public Security of 9 June 2017 on Cyber security - a joint responsibility, will be sent to the Storting.