Norwegian Ministeries

Strategy

National Cyber Security Strategy for Norway

Foreword

Norway is one of the leading digital nations in the world. As politicians, we have a responsibility to ensure that we make the most of the resources invested in our society. We are encouraging both the public and the private sector to participate in digital innovation, to improve efficiency, increase competitiveness and create new jobs.

The digitalisation of Norwegian society also represents a challenge. Digital infrastructure and systems are becoming increasingly complex, comprehensive and integrated. Dependencies and vulnerabilities are progressively emerging across areas of responsibility, sectors and nations, and it is generally expected that digital services should be accessible anywhere and all times. Successful digitalisation also includes making sure that the solutions provided appropriately accommodate demands for the security and privacy of the individual, and that everyone can be confident that the digital services will function as they should.

The first national Norwegian cyber security strategy was introduced in 2003, making Norway one of the first countries in the world to have a national strategy in this particular area. In step with developments in the threat landscape, the national strategy was revised in 2007 and 2012.

The Committee on Digital Vulnerabilities in Society published its report on digital vulnerability in Norwegian society in 2015. As a part of the follow-up on the report, the first white paper to the Norwegian Parliament that focused exclusively on cyber security was prepared in 2017. The paper was entitled "Cyber security – a joint responsibility" – and with good reason, given that we all share an interest in, and a responsibility for, securing our digital assets. What was once a topic of interest to a select few has now become an issue that affects each and every one of us.

The present strategy is Norway's fourth cyber security strategy, and is intended to address the challenges that will inevitably arise in conjunction with the rapid and far-reaching digitalisation of Norwegian society. The developments in relation to previous national strategies are based on the need to reinforce public-private, civilian-military and international cooperations. The primary target groups for the strategy are authorities and companies in both public and private sectors, including the municipalities. Moreover, the strategy is to lay the foundations for ensuring private individuals have the necessary knowledge and understanding of risks in order to use technology in a safe and secure manner.

In preparing the strategy, we placed particular emphasis on applying an open and inclusive process so as to involve stakeholders from the public and private sector alike. A strategy conference involving more than 300 delegates, written input and high participation in a range of workshops clearly indicates there is great interest in identifying shared solutions. I extend my gratitude to everyone who has made a contribution during the strategy process.

The time has now come to make a start on the most important work – the follow-up. I hope that you will take ownership of the new national cyber security strategy, put it on the agenda and help ensure its implementation. By responding to cyber security challenges appropriately, we can make the very most of the digitalisation of society and benefit from new opportunities for us as individuals, as companies and as a society.

Erna Solberg
Prime Minister

Contents

1 Introduction

1.1 Challenges

Technology will give rise to far-reaching changes over the coming years. Robotisation, sensor technology, 3D printing, big data and artificial intelligence are all examples of technological advances that are likely to change society. We will have access to digital services we can barely imagine – services that will be available 24/7, wherever we may be. Our everyday life will become increasingly digital, primarily to the benefit of private individuals, companies and the authorities.

The digitalisation carries with it a range of challenges. Our society is becoming increasingly vulnerable to cyber threats, and thorough understanding of society's digital dependencies is becoming ever-more important. Digital infrastructures and systems are growing more complex, global and integrated. All kinds of devices are being connected to the internet and use of cloud solutions is on the rise. The need to reduce costs and increase access to competence is resulting in more and more digital services being outsourced to third parties, particularly in low-cost countries. Compound (hybrid) threats are blurring the traditional dividing line between peace and armed conflict, and challenging the conventional placement of responsibility between the civilian and military sectors.

The sheer speed of technological evolution makes it extremely difficult to forecast which threats will come to dominate the threat landscape of the future. Regardless, it is likely that specific types of threats such as ransomware, industrial espionage, sabotage, blackmail, cyber-bullying and identity theft will remain prominent over the coming years. These are threats that can be targeted at private individuals and companies alike, with severe consequences for those affected.

The Norwegian National Security Authority (NSM) publishes an annual report entitled the "Comprehensive Cyber Security Risk Assessment" (*Helhetlig IKT-risikobilde*). The report is built on a comprehensive portfolio of risk and vulnerability reports from authorities, the business community, academia and other stakeholders. The assessment for 2018 suggests that the digitalisation of society is changing the value of both new and existing digital solutions. Every time services are digitalised or automated, the level of digital dependency in society increases. When services are made available on digital platforms, the associated values are exposed to threat agents operating in the domain. This naturally generates new security challenges and alters the threat landscape.

The threat landscape is characterised by the continuation of trends from previous years, combined with a reinforcement of some developments. Foreign intelligence activity targeted at public and private companies, along with cyber crime, constitute the predominant cyber threats to Norwegian society in 2018.

1.2 Strategy

The Norwegian Ministry of Justice and Public Security is responsible for coordinating public security in the civilian sector. The Ministry holds a special responsibility for national cyber security in the civilian sector, and will outline the Government's policy for cyber security, including national cyber security requirements and recommendations for public and private companies.[1] The Norwegian Ministry of Defence holds responsibility for cyber security in the defence sector. In order to address these responsibilities, the authorities have access to a broad range of tools: development of regulations and knowledge, supervisory activities as well as counselling and guidance.

However, the authorities will not be able to solve all challenges in cyberspace by themselves. Critical societal functions and other Norwegian interests are dependent on digital infrastructures that continue to increase in both scope and complexity. Long and less transparent digital value chains, which span multiple sectors and borders, are a core challenge in assessing digital vulnerability.

The cyber security challenges must therefore be resolved by placing a strong emphasis on collaboration and partnerships among relevant stakeholders at both national and international level. Challenges need to be addressed through joint input and across traditional sectoral boundaries, such that the security needs of all stakeholders are appropriately accommodated. Particular emphasis must be put on cooperations and partnerships within the prioritised areas of the strategy. These are described in detail in Chapter 3.

1 Cyber security has to do with protecting "everything" that is vulnerable because it is connected to or otherwise dependent on information and communication technology. The term is used synonymously with the terms "ICT security" and "digital security".

1.3 Vision

In Norway, it is safe to use digital services. Private individuals and companies have confidence in national security, and trust that the welfare and democratic rights of the individual are being safeguarded in a digitalised society.

1.4 Strategic goals

This strategy places emphasis on our working together to reinforce cyber security in society. Based on the current security challenges, the following strategic goals are considered fundamental:

1. Norwegian companies digitalise in a secure and trustworthy manner, and are able to protect themselves against cyber incidents

2. Critical societal functions are supported by a robust and reliable digital infrastructure

3. Improved cyber security competence is aligned with the needs of society

4. Society has improved ability to detect and handle cyber attacks

5. The police have strengthened their ability to prevent and combat cyber crime

2 A stronger cooperation

There are several governmental bodies with a cross-sectoral responsibility for cyber security (see Appendix A). It is important to ensure a good cooperation among these actors. One key collaborative hub is the Joint Cyber Coordination Centre (*Felles cyberkoordineringssenter* – FCKS), which comprises representatives from NSM, the Norwegian Intelligence Service, the Norwegian Police Security Service (PST) and the National Criminal Investigation Service (Kripos). The purpose of FCKS is to help improve the national capability to detect and withstand serious cyber attacks, provide strategic analysis and maintain a comprehensive threat and risk assessment for cyberspace.

The authorities cannot achieve good cyber security on their own. The business community has the requisite skills and resources and functions as a driving force for digitalisation and innovation. As such, it has a key role to play in the solution. In order to protect the digital society, private individuals, companies, sectors and nations must all look beyond the boundaries of their own interests. All companies have a responsibility to ensure their own cyber security, but the dependency of society on digital solutions makes it essential to establish stronger cooperations and partnerships both at international level and in all areas of society.

2.1 Public-private partnership

Digital services and products are often developed by private companies or research and development communities. A substantial part of Norway's critical digital infrastructure is owned and operated by private companies. Consequently, important decisions related to the development of – and security in – cyberspace are made by commercial, non-state actors, i.e. outside the conventional intergovernmental arenas. As a result, the role of the authorities in the development of cyberspace is limited, which in turn calls for an extensive public-private partnership.

Public and private companies have different capacities, knowledge and skills, which supplement one another. The authorities have an important role as legislator, facilitator and supervisory body; law enforcement have designated powers to investigate and prosecute cyber crime. Moreover, the authorities also has the duty to collect foreign and domestic intelligence, collaboration within international bodies and share information about potential threats.

Increased collaboration inevitably leads to better situational awareness and better decisions, as well as allowing greater access to resources. In order to tackle ever-changing security challenges, cooperations should be intensified and developed even further.

Guiding principles:

- The authorities and the business community work together to identify and discuss cyber security challenges, and to exchange experience about them.
- This cooperation should carry obligations for both parties and be based on transparency, trust and mutuality.
- The authorities contribute to establishing a business community where cyber security services are in demand, developed and provided.
- When building up national capacity in cyber security, is should be facilitated for inclusion of capabilities from the business community.

2.2 Civilian-military collaboration

The defence sector is dependent on civilian digital infrastructures and services. As a result, cyber security challenges in the civilian sector are also of significance to Norway's ability to handle security-political crises and to carry out military operations. In a worst-case scenario, cyber attacks on civilian infrastructures may challenge Norway's ability to safeguard national security.

The total defence concept encompasses both military support for civilian society and civilian support for the Armed Forces. The contribution of the Armed Forces to public security also translates into improved ability to safeguard state security, given that a well-functioning civilian society and robust public security form an important foundation for well-functioning military defence. In order to meet common cyber security challenges, military and civilian actors must work more closely together. This includes conducting exercises in how to handle crisis situations, development of joint competence, mutual incident notification, and exchanging information about threats and vulnerabilities.

NATO is putting civilian emergency preparedness and civilian-military collaboration on the agenda to a much greater extent than previously. Emergency preparedness, crisis management and robust critical societal functions constitute a precondition for the overall preparedness and defence of the individual country – and thus of the alliance.

Guiding principles:

- Civilian support of the Norwegian Armed Forces in the event of cyber security challenges in times of crisis and armed conflict is provided within the framework of the total defence concept.
- Companies in the defence sector work with civilian counterparts to identify, exchange experience about and find solutions to cyber security challenges that may be of significance to the ability to carry out military operations.
- Companies in the defence sector and the civilian sector should make use of each other's capacities to address common cyber security challenges.
- Companies in the defence sector share information and experience with their counterparts in the civilian sector in order to raise the level of national security.

2.3 International cooperation

Norway's international cyber policy is to serve Norwegian interests, ensure robust and predictable framework conditions, and contribute to preventing and protecting against cyber vulnerabilities and threats. The governing document is the "International Cyber Strategy for Norway" (*Internasjonal Cyberstrategi for Norge*), published by the government in August 2017. The strategy clearly states that a sustainable global internet is dependent on finding an appropriate balance between transparency, security, robustness and freedom.

Digitalisation has changed the global digital landscape in just a short time. Digital value chains span national borders, and mutual dependencies are being established that challenge the control of the national authorities. At the same time, cyber crime and cyber attacks from both state and non-state actors constitute extremely serious threats to national security and economy. In order to achieve the best possible protection, it is essential for Norway to participate in international arenas to reinforce cyber security at global level.

Guiding principles:

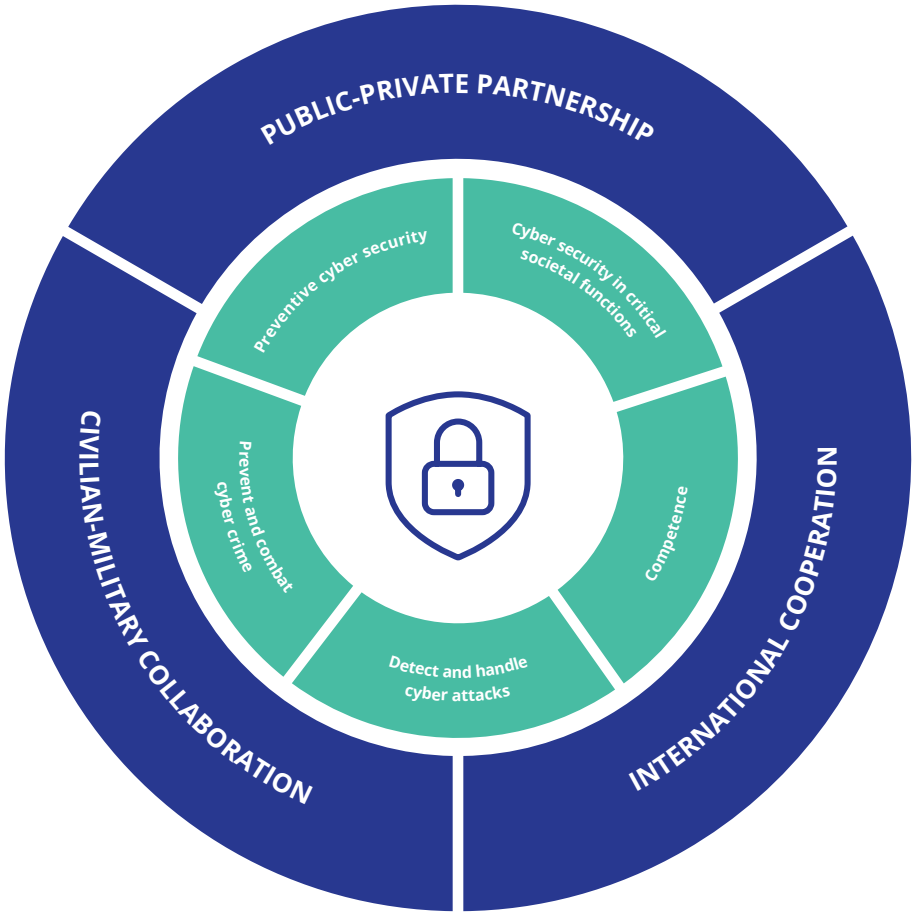
- The authorities work with other nations to reinforce Norwegian ability to prevent, detect, alert and handle cyber incidents.
- The authorities promote international cooperations on cyber security, agreements on state behaviour in cyberspace, and collaboration on combating cyber crime in international arenas such as the UN, NATO, the EU, the OECD and the OSCE. In addition, dialogue is established with other states bilaterally and at regional level, including Nordic collaboration.
- The authorities ensure active Norwegian participation in relevant international arenas so as to ensure the internet remains an open, accessible, secure and robust platform, based on international standards and collaboration between authorities, the business community, academia and other parts of civilian society.
- The authorities ensure close coordination between bodies that represent Norway in arenas where international cyber security policy and cooperation on cyber crime and handling cyber incidents are developed.

3 Prioritised areas

From a national perspective, it is important to ensure a comprehensive approach to cyber security challenges, irrespective of whether these take the form of intentional (e.g. cyber attacks) or unintentional (e.g. natural disasters, technological errors or accidents) cyber incidents. We can achieve comprehensive protection against cyber incidents through the interaction between the preventive measures, a robust digital infrastructure, the ability to deal with cyber attacks, the fight against cyber crime, and sufficient cyber security competence.

The digitalisation of society increases the importance of cyber security, given that robust cyber security is a particularly important precondition for maintaining trust and confidence in ICT systems and digital services provided by the public sector. A digital public sector contributes to increased efficiency, innovation and economic growth.

This strategy is supported by a two-part list of measures. Part 1 describes the authorities' selected key measures related to the prioritised areas described in this chapter, while Part 2 presents ten basic measures for improving companies' own ability to protect themselves against cyber incidents.



3.1 Preventive cyber security

Strategic goal:
Norwegian companies digitalise in a secure and trustworthy manner, and are able to protect themselves against cyber incidents.

Cyber security is primarily a responsibility at company level. Corporate managers are responsible for conducting risk assessments and then, on the basis of these, implementing appropriate measures. The authorities are to provide conditions that enable companies to protect themselves against cyber incidents in order to uphold their own security and to increase the robustness of society as a whole. Preventive cyber security and a systematic approach to address risk will help reduce the possibility of cyber incidents having negative consequences for businesses, private individuals, or society as a whole. Prioritised advice and recommendations better enable companies and private individuals to initiate appropriate measures to increase the level of security in society. Part 2 of the list of measures is therefore a key resource to increase companies' own ability to protect themselves against and handle cyber incidents.

Preventive cyber security in society entails ensuring that digital services and products are secure and reliable from the moment of creation, and throughout their lifespan.

Subsidiary goals:

1. Companies take a risk-based approach to cyber incidents and use recognised frameworks, standards and management systems for cyber security.

2. The public sector exercises strong management and control of its cyber security. The companies' cyber security management systems underpin their primary function and contribute to ensuring that cyber security incidents in one company do not cause serious damage to others.

3. Private individuals, the business community and the public administration have confidence that public digital services are secure and reliable.

4. The authorities and the business community share information about threats, vulnerabilities, incidents and efficient measures with relevant actors to make society better able to withstand cyber incidents.

5. The authorities share advice, recommendations and guidelines on cyber security to provide companies with knowledge for their security work.

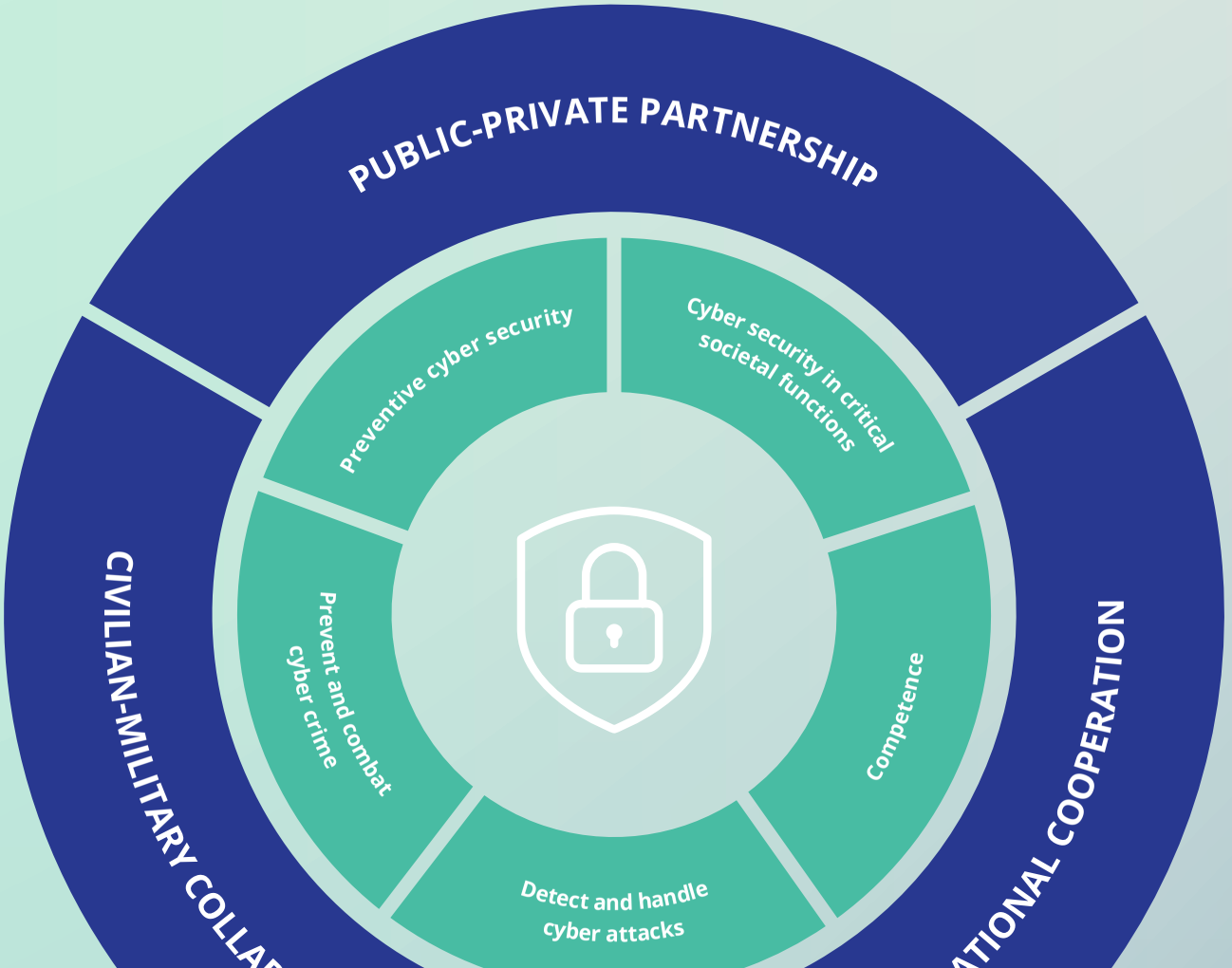
6. The authorities act as a driving force for cyber security in digital consumer services and products.

7. The authorities establish conditions conducive to cooperations within the public sector and between public and private sectors.

8. The population has good judgement on cyber-related issues and a good cyber security culture.

Backside of poster

National cyber security strategy for Norway



START-UP TIPS	✕ ✓
Establish sufficient systematics for security management, and make sure that an expert in the field supports the management in this work.	
Include cyber security in the work on risk at the company. Establish clear responsibility at the company, with effective reporting lines to the senior management and board of directors.	
Prepare a list of the company's key goals, the values and value chains involved, where key data are stored, and who has access to these data.	
Map the companies security culture and identify what can be improved. Define the desired culture and carry out adapted annual training programmes to promote appropriate security culture.	
Focus on expertise in procurement and implement risk assessment that is deployed among the management.	

START-UP TIPS	✕ ✓
Upgrade hardware and software. Eliminate unnecessary complexity and unused functionality. Block the running of non-authorised programs.	
Install security updates as soon as possible. Protect wireless networks with strong security mechanisms. Plan and document changes. Switch on logging, and review important logs regularly.	
Use the latest version of your internet browser. Protect email with DMARC. Encrypt important information when it is stored on portable media and when it is sent via the internet.	
Change standard passwords and do not grant administrator rights to end users. Use 2-factor authentication or, as a minimum, strong passwords.	
Establish an emergency response plan for different types of incidents, and run drills to test the plan.	

See Part 2 of the list of measures for additional information.

Backside of poster

3.2 Cyber security in critical societal functions

Strategic goal:
Critical societal functions are supported by a robust and reliable digital infrastructure.

Society is dependent on critical societal functions being maintained, and this requires the digital infrastructures that support them to work everywhere and at all times.[2] Mutual dependencies across digital infrastructures represent a particular challenge. This applies in particular to the power grid and electronic communications networks, which constitute fundamental infrastructure for almost all digital infrastructures. An incident occurring in one digital infrastructure may generate negative impact on another. Companies should therefore be aware of which services they themselves are dependent on, and what potential consequences incidents in their own digital infrastructure may have on others.

Subsidiary goals:

1. The authorities ensure that frameworks and methods for identifying critical digital infrastructure are in place and provide guidance to make sure that critical digital infrastructures are identified.

2. Public and private companies that own critical digital infrastructure perform risk assessments to identify vulnerabilities and mutual dependencies between infrastructures so as to ensure comprehensive securing of digital value chains.

3. The authorities maintain an overview of critical national digital infrastructure.

4. The authorities define security requirements for critical digital infrastructure, provide guidance and conduct audits to ensure security requirements are met. Public and private companies that own critical digital infrastructure implement measures that ensure appropriate security in these.

5. Public and private companies participate in contingency exercises related to critical digital infrastructure.

2 This strategy also includes critical social functions beyond what is covered by the Security Act. This can be functions that fulfil the fundamental needs of society and the population's sense of security (banking and financial services, health services and the like). See DSB's report "Society's critical functions" for an overview of these.

3.3 Competence

Strategic goal:
Improved cyber security competence is aligned with the needs of society.

Competence and knowledge about threats, vulnerabilities and effective measures constitute a precondition for the ability to protect digital values against cyber incidents. This requires that everyone – private individuals, companies and the authorities – have access to information about cyber security challenges and the appropriate measures to address them. Specialisation within cyber security of vital importance to national security is to be accorded special priority.

The national strategy for cyber security competence (2019) elaborates the competence goals in this strategy and sets out conditions for a long-term build-up of competence, encompassing national capacity in the fields of research, development, education and measures designed to raise awareness in the business community and among the general public.

Subsidiary goals:

1. Provide attractive and competent research environments for prominent researchers and postgraduates.

2. The number of specialists within the field of cyber security covers the needs in the labour market and accommodates national security considerations.

3. Cyber security competence is sufficiently addressed in study programmes where ICT constitutes a key component, including ICT and technology courses. In addition, study programmes within other disciplines that include significant ICT elements also include cyber security to a relevant extent.

4. Good post- and supplementary education in ICT and cyber security at vocational colleges, universities and university colleges.

5. Cyber security is included in relevant professional training courses and vocational courses to a sufficient extent.

6. Pupils and apprentices have digital skills, including competence in secure use and security, that enable them to experience life skills and to succeed in further education, working life and participation in society.

7. Private individuals have knowledge and skills that provide them with good judgement concerning digital issues, and which contribute to protecting their privacy and assets online.

3.4 Detect and handle cyber attacks

Strategic goal:
Society has improved ability to detect and handle cyber attacks.

Cyber attacks can constitute a threat to critical national functions, the security of society in general and Norwegian sovereignty. The ability to withstand cyber attacks in order to ensure freedom of action has become a key element of our national defence. Threat agents may be other states, non-state groups or private legal entities. The possible objectives of cyber attacks span a broad spectrum: from crime for profit to state-sponsored espionage, sabotage and hybrid operations. Cyber attacks can interrupt, influence and obstruct national decision-making processes.

The use of cyber capacities has increasingly become an integrated part of military operations. Depending on conditions such as the purpose and legitimacy of the attack, its strength and consequences, a cyber attack may be considered an "armed attack" – in which case it triggers a nation's right to self-defence (see Article 51 in the UN Charter).

Norwegian emergency preparedness follows the principle of responsibility, in that whoever is responsible for an organisation under normal condition is also responsible in a crisis situation. The authorities will improve national preparedness and the ability to detect and handle cyber attacks. To do this, roles and responsibilities must be defined, and relevant stakeholders must have a good understanding of the situation and consequences. There must be adequate coordination, collaboration and sharing of information between the key actors responsible for identifying and dealing with serious cyber attacks. See section 3.5 about police responsibility.

Subsidiary goals:

1. Norwegian companies take responsibility for handling cyber attacks targeted at their own business and for sharing information about these with the authorities and other relevant actors.

2. The authorities continue developing frameworks that define roles, responsibility and governance structures for handling serious cyber attacks.

3. The authorities have improved capacity to assist with and coordinate measures to counter cyber attacks.

4. The authorities facilitate the sharing of information and transfer of experience between relevant parties with the purpose of detecting and countering serious cyber attacks.

5. The authorities continue developing international collaboration to increase national ability to prevent, detect, alert, attribute and counter serious cyber attacks.[3]

6. The authorities facilitate national exercises and establish conditions for Norway to participate in international exercises.

3 In this context "attribute" is taken to mean identifying the actor or actors responsible for a cyber attack.

3.5 Prevent and combat cyber crime

Strategic goal:
The police have strengthened their ability to prevent and combat cyber crime.

The police are able to protect society and prevent, detect, investigate and prosecute crime. This task is the same in cyberspace as in the physical world. The rapidly advancing technological development creates significant challenges for combating cyber crime. The police are faced with new demands in their work due to the current threats, e.g. regarding access to new technology, need for specialist skills and collaboration with other actors.

It is essential that the population trusts that all types of crime is handled responsibly and effectively. The authorities will improve the conditions for the police to carry out their tasks in line with technological developments and crime trends.

Subsidiary goals:

1. The police have strengthened their competence and capacity to prevent and combat cyber crime.

2. Society trusts the ability of the police to prevent and combat cyber crime.

Appendix A: Selected national contacts

Cyber security is primarily a responsibility at company level. Corporate managers are responsible for conducting risk assessments and then, on the basis of these, implementing appropriate measures. In addition, all government ministries are responsible for enforcing cyber security in their own sector. The list below presents some ministries and selected national contacts with cross-sectoral cyber security responsibility.

THE MINISTRY OF JUSTICE AND PUBLIC SECURITY (JD)	THE MINISTRY OF DEFENCE (FD)	THE MINISTRY OF LOCAL GOVERNMENT AND MODERNISATION (KMD)	THE MINISTRY OF TRANSPORT AND COMMUNICATIONS (SD)	THE MINISTRY OF FOREIGN AFFAIRS (UD)
Coordination responsibility for cyber security in the civilian sector, as well as a general coordination responsibility for the civilian security of society.	Responsibility for cyber security in the defence sector. Responsibility for the Security Act.	Special responsibility for working to promote a stronger, more comprehensive approach to cyber security in public administration. KMD also holds coordination responsibility for the government's ICT policy.	Responsibility for cyber security in electronic communication networks and services, including the internet.	Responsibility for Norwegian foreign and security policy, including coordinating Norway's input and positions in international arenas where global challenges in cyberspace are discussed.

The Norwegian National Security Authority (NSM) is the national specialist organisation for cyber security and the national warning and coordination body for serious computer attacks on infrastructure critical to society and other key societal functions. NSM runs the national response function for serious computer attacks on critical infrastructure (NorCERT) and the national warning system for digital infrastructure (VDI). It has recently been decided to establish a national cyber security centre linked to the NSM.

www.nsm.stat.no

The National Police Directorate (POD) is responsible for management, governance, follow-up and development of the police districts and special police units. It has recently been decided to establish a national cyber crime centre (NC3) under the National Criminal Investigation Service (Kripos) to develop the skills and capacity of the police to tackle a more digitalised crime and evolving threat landscape. The work to establish the unit was commenced in 2018 and is scheduled to be completed before the end of 2021. The principal tasks of NC3 will be to prevent and combat crime through investigation, securing evidence, developing methodology and providing support to other sections of the police force.

www.politiet.no

The Norwegian Police Security Service (PST) has responsibility for the domestic security of the nation. PST prevents and investigates crimes that threaten national security, including collecting information concerning individuals and groups who may pose a threat, developing various analyses and threat assessments, conducting investigations, applying other operational countermeasures and providing advice.

www.pst.politiet.no

The Norwegian Intelligence Service (E-tjenesten) is responsible for charting foreign actors who pose a threat, and for analysing their motives, capacity and methods. The purpose of intelligence activities is to help provide the Norwegian authorities with a solid basis for decisions in cases involving foreign, security and defence policy.

www.forsvaret.no/organisasjon/etterretningstjenesten

The Agency for Public Management and eGovernment (Difi) works to promote a stronger, more comprehensive approach to information security in public administration through providing advice, guidance and recommendations.

www.difi.no

The Norwegian Data Protection Authority is both the supervisory- and the representative authority. The Data Protection Authority is an independent administrative body tasked with checking privacy regulations and ensuring that the rights of individuals are not violated through the use of information that can be linked to them.

www.datatilsynet.no

The Norwegian Communications Authority (Nkom) holds a separate authority linked to security and preparedness in electronic communications networks and services.

www.nkom.no

The Norwegian Directorate for Civil Protection (DSB) is to maintain an overview of risks and vulnerabilities in society, and to promote the work to prevent accidents, crises and other undesirable incidents, as well as to ensure a high level of preparedness and effective accident and crisis management.

www.dsb.no

The Norwegian Centre for Information Security (NorSIS) is an independent organisation that is working to improve knowledge about and understanding of cyber security, for example by providing advice and guidance to private individuals and companies (especially SMB companies). NorSIS holds editorial responsibility for the slettmeg.no and nettvett.no services. Slettmeg.no is a free advice and guidance service for people who feel their rights have been violated on the internet, while nettvett.no provides information, advice and guidance about how to use the internet more safely.

www.norsis.no
www.slettmeg.no
www.nettvett.no

Appendix B: Relevant political and strategic documents

The present strategy is part of a larger context of political and strategic documents that lay down guidelines for the national work with cyber security, including:

DOCUMENT	
White paper No. 38 (2016–2017) Cyber security – a joint responsibility	The first white paper to focus exclusively on cyber security.
White paper No. 10 (2016–2017) Risk in a secure society	White paper on public security, including cyber security.
White Paper No. 27 (2015–2016) Digital agenda for Norway	White paper on the government's digitalisation policy, where privacy and cyber security are key elements.
Proposition No. 151 S (2015–2016) Capable and Sustainable	Long-term plan for prioritisations in the defence sector, including cyber security.
Proposition No. 153 L (2016–2017) Act on National Security	New security act that is to contribute to safeguarding our overarching national security interests.
Instructions for the work of the ministries on public security	The public security instructions are to reinforce the ability of society to prevent crises and to deal with serious incidents. Cyber security is an integral part of the work to increase public security.
International Cyber Strategy for Norway	Strategy published in 2017 containing guidelines for the work on international cyber policy, where cyber security is one of several prioritised areas.
Proposition No. 56 LS (2017–2018) Act on the processing of personal data	New personal data act that implements the EU's general data protection regulation (GDPR).
Comprehensive Cyber Security Risk Assessment	Annual report that is to help raise awareness about and promote increased cyber security in Norwegian companies, and in society in general.

Notes

Notes

Published by:
Norwegian Ministeries

Additional copies may be ordered from:
Norwegian Government Security and Service Organisation
www.publikasjoner.dep.no
Telephone: + 47 22 24 00 00
Publications are also available on:
www.government.no
Publication number: G-0444 E
Design and layout: Konsis Grafisk
Print: Norwegian Government Security and Service Organisation
01/2019 – Impression 500