A national cyber security strategy

Skr. 2016/17:213

Government Offices of Sweden
Ministry of Justice

Regeringens skrivelse 2016/17:213

A national cyber security strategy

Skr. 2016/17:213

The Government hereby submits this Communication to the Riksdag.

Stockholm 22/06/2017

Morgan Johansson

Anders Ygeman
(Ministry of Justice)

Main contents of the communication

There is a great need to develop cyber security in Sweden. This national cyber security strategy is an expression of the Government's overarching priorities and is intended to constitute a platform for Sweden's continued development work within the area. The main aims of the strategy are to help to create the long-term conditions for all stakeholders in society to work effectively on cyber security, and raise the level of awareness and knowledge throughout society. By means of the strategy, the Government also wants to support the efforts and engagement that already exist in society for enhancing cyber security. The strategy thus encompasses the whole of society, that is to say central government authorities, municipalities and county councils, companies, organisations and private individuals.

Table of contents

1 A comprehensive cyber security strategy

1.1 The need for a strategy

Digital transformation is a global phenomenon, impacting basically every part of society. It presents us with major opportunities, but also risks. How we manage the risks inherent in digital transformation has a significant impact on our ability to maintain and enhance both our prosperity and our security.

Today, cyber security concerns the whole of society. Everyone needs to take responsibility for cyber security issues if we are to achieve an effective and secure management of information. No one can resolve the security challenges alone, and with many different stakeholders working in different ways and in different contexts, collaboration and a common direction become particularly important. In particular, the need for collaboration between the public and private sectors is growing in importance. Technological developments are essentially driven by private market stakeholders, and private stakeholders also own and run major parts of this critical infrastructure.

The challenges of the cyber security area are shared with other countries. For this reason, the strategic solutions must also be developed through international collaboration and dialogue on preventive measures, both within the EU and in other international bodies.

The demands on society's cyber security are increasing at an accelerating pace. This development and changes in the use of new technology and new innovations make threats more difficult to detect, risks more difficult to assess and dependencies more difficult to survey. The regulatory changes now being implemented both nationally and within the EU are a means of raising the security requirements and of strengthening the forms and structures for combined cyber security efforts.

Digital transformation is one of the biggest changes of our times, and the rapid development of information and communications technology has a major impact on our future. Sweden is at the forefront of technological development. The current expansion of fibre networks and greater mobile coverage represent upgrades to the electronic communications networks. Thus, digital development will be increasingly able to contribute to employment, innovation, efficiency and growth in Sweden.

Structured and risk-based cyber security efforts will enable us to ensure society's continued digital transformation, while also asserting Sweden's security and national interests, such as human rights and freedoms and the functioning of society. Structured and risk-based cyber security efforts are also an important prerequisite for Swedish growth and competitiveness and a necessity for the private sector to develop and provide competitive goods and services. In order to increase cyber security, there is a need for all the parties concerned to increasingly work together towards common objectives.

Against this background, the Government has decided to produce a national cyber security strategy. The strategy is an expression of the Government's overarching priorities and aims to constitute a platform for Sweden's continued development work within the area. The main aims of the strategy are to help to create the long-term conditions for all stakeholders in society to work effectively on cyber security, and raise the level of awareness and knowledge throughout society. By means of the strategy, the Government also wants to support the efforts and engagement that

already exist in society for enhancing cyber security. The strategy thus encompasses the whole of society, that is to say central government authorities, municipalities and county councils, companies, organisations and private individuals.

In this Communication, cyber security refers to a set of security measures to preserve the confidentiality, authenticity and availability of information. Confidentiality means that unauthorised persons cannot access the information. Authenticity means that the information is not modified, manipulated or destroyed in an unauthorised manner. Availability means that authorised persons can access the information in the manner and at the time offered by the services.

1.2 Starting points for Sweden's cyber security

Cyber security efforts are necessary for enabling society to function and develop in line with the goals of various policy areas. Digital transformation means that an increasing proportion of all activities in society is to varying degrees dependent on networks and information systems, and thereby on cyber security.

The cyber security strategy is based on the objectives for Sweden's security: protecting the lives and health of the population, the functioning of society, and our capacity to uphold fundamental values such as democracy, the rule of law and human rights and freedoms (Government Bill 2008/09:140, Committee Report 2008/09:FöU10, Riksdag Communication 2008/09:292). The strategy is also based on the overall IT policy objective – for Sweden to become the world leader in harnessing the opportunities of digital transformation (Government Bill 2011/12:1, Committee Report 2011/12:TU1, Riksdag Communication 2011/12:87).

The cyber security strategy builds on and embodies the focuses of cyber security set out by the Government in its national security strategy and in the digital strategy (N2017/03643/D).

The national security strategy states that Sweden is to actively safeguard our national interests and defend them whenever they are at risk of being undermined, including in relation to the threats and risks found in the area of information technology.

The digital strategy states that Sweden will provide the best conditions for securely taking part in, taking responsibility for and building trust in the digital society.

Today, provisions on information security are found in different regulatory frameworks. Information security is one of three fundamental protective security areas under the Protective Security Act (1996:627). The legislation applies to the most security-sensitive activities in Sweden and entails far-reaching requirements for various protective measures. Other central government authorities operate under the information security requirements set out in the Ordinance (2015:1052) on Emergency Preparedness and Surveillance Responsible Authorities' Measures at Heightened Alert. Provisions on information security are also found in the Archives Act (1990:782), the Personal Data Act (1998:204) and the Electronic Communications Act (2003:389). In addition to these statutes, there are authority regulations governing information security in a number of sectors.

Several statutes governing information security will be amended or added in the coming years. The protective security legislation is currently being reviewed, with proposals that include broadening the scope of application to achieve better protection for Sweden's security (SOU 2015:25). Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive), which is to have been implemented in Swedish legislation no later than

May 2018, includes an obligation for all Member States to adopt a national strategy on the security of network and information systems. Another piece of EU legislation, Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), will begin to be applied in May 2018 and entails higher requirements on the handling of personal data.

In recent years, several inquiries and reviews in the area of cyber security have indicated deficiencies in relation to current threats and risks. These include the Swedish National Audit Office's audits of information security in public administration (RIR 2016:8, RIR 2014:23). The report Cyber security in Sweden also contains several proposals in the area of cyber security (SOU 2015:23). In its defence policy bill, the Government assessed that Sweden's overall capability to prevent, counteract and actively manage consequences of civil and military threats, events and attacks in the cyber environment must be developed and strengthened (Government Bill 2014/15:109).

What is to be protected?

The open democratic society is dependent on the ability to maintain the desired confidentiality, authenticity and availability when handling information. This means that both the information itself and the systems used to store and transfer that information must be protected. Cyber security efforts are a necessary activity for safeguarding the quality and effectiveness of societal functions and a prerequisite for being able to harness the opportunities of digital transformation. Such opportunities involve everything from developed digital public services to connected and automated vehicles and factories. Ultimately, cyber security involves safeguarding fundamental societal values and goals, such as democracy, human rights and freedoms, Sweden's freedom, security and right to autonomy, and growth and economic stability.

If individuals are to be able to exercise their rights and freedoms, they need access to accurate and readily available information. This is a prerequisite for being able to make well-founded decisions and raises the quality and effectiveness of all types of activities and contacts in society.

Some information in society is sensitive and therefore needs to be protected. If sensitive information is lost, stolen, manipulated or disseminated to unauthorised persons, this can have serious consequences. There are large quantities of information that are of decisive importance to the functioning of society or that contain information sensitive with respect to privacy. Other examples of sensitive information have to do with law enforcement, technological products, business relations, total defence or circumstances concerning other states.

Today, the systems for handling information are mainly based on digital information and communications technology. This applies not least to the systems that Sweden depends on to govern and lead the country during extensive strains that might result from crisis or war. Such systems must be secured. Furthermore, many societal activities are based on functioning digital information and control systems that continuously handle large quantities of sensitive information in order to control, e.g. electricity distribution, water supply, transportation, transport infrastructure or hospital equipment. Industrial activities such as engineering and processing are also dependent on functioning digital information and control systems today. Incidents and attacks with regard to Swedish trade and industry can have far-reaching consequences, both for individual companies and entire value chains, thus threatening Swedish jobs.

Dependencies and links between different technical systems are in themselves a vulnerability factor since disruptions can have consequences that are difficult to anticipate and manage. This is particularly true as most networks and information systems are globally linked via the internet. The internet is today a global infrastructure, and Swedish society's critical infrastructure is highly integrated with the internet. The internet is so essential that an attack against or other incidents within this infrastructure could lead to serious consequences for Sweden's security and national interests.

What are the risks and threats?

The scale of threats and risks in the area of information technology ranges from less extensive risks for private individuals to well-planned and precision attacks against vital parts of the functioning of society. Various forms of disruptions to software or hardware, or disruptions in the operating environment are common. External physical events, such as fires, severed underground cables, floods or solar storms, are also a part of the threat scenario.

In principle all those connected to the internet, both private individuals and private and public operations, are currently exposed to risks since intrusion attempts are constantly being made against internet-connected systems. This type of mass attack is often more or less random. An example of this is the major increase in fraud and identity theft taking place via the internet. According to the Swedish National Council for Crime Prevention (Brå), statistics show that crime with elements of IT (computer fraud, fraud committed with the aid of the internet, data infringement and internet-related child pornography crimes) increased by 949 per cent between 2006 and 2015 (2016:17). The person responsible for an IT system must assume that intrusions and attacks can succeed, even though a great number of these are actually averted. Targeted intrusions and attacks can be performed by private individuals, groups of individuals, non-governmental organised groups or states and state-sponsored actors.

The possible action of states, state-sponsored actors or other actors of a similar capability constitute the most serious cyber security threat against Sweden. These qualified attackers have the capability, resources and perseverance to devise and use advanced methods. Cyberattacks and various forms of intrusion in IT systems can constitute a separate antagonistic threat as well as one of several political and military instruments of power. Espionage and attacks from state and state-sponsored actors against security-sensitive activities in Sweden or against Swedish interests abroad can, for example, have the aim of appropriating information about Swedish economic interests, Swedish companies, Swedish research, Swedish defence capability and planning, our security policy objectives, vital societal functions and critical infrastructure.

Covert intrusions and attacks can be used in order to prepare for sabotage against critical infrastructure in peacetime. These can also be used openly as a tool primarily in the initial stages of military operations. Cyberattacks can have major consequences for vital societal functions and critical IT systems similar to a conventional armed attack and can therefore, in some cases, be considered an armed attack.

Attacks can also be directed against our fundamental values and the democratic functions of society, e.g. through disinformation and influence campaigns. Disinformation can be used to intentionally disseminate untrue or misleading details in order to influence people's attitudes, standpoints and actions in a certain direction. An influence campaign is centrally controlled, while also offering the use of a broad spectrum of methods, both open and covert, a subset of which might be data intrusion and other cyberattacks. It can also include political, diplomatic, economic and military instruments of power. The dissemination of incorrect or misleading

information risks undermining confidence in our public institutions and challenges the security of society. Source criticism and access to a diversity of independent media and news agencies strengthen awareness and counteract the effects of disinformation and influence campaigns.

The number of cyberattacks aiming to influence the media is expected to increase. For example, these involve using denial-of-service attacks to prevent access to the media, but also more advanced attacks that use data intrusion to steal information or hijack websites or broadcasts in order to introduce false or misleading information.

How do we protect ourselves?

The work to protect ourselves is a responsibility shared by all of society and is conducted both by the Government and in the activities of municipalities, county councils, authorities, companies and organisations in Sweden. Systematic cyber security efforts are necessary for enabling stakeholders in society to maintain a well-balanced level of cyber security – not everything in society can be protected against all types of threats and risks. Technical security needs to be further enhanced while taking into account the fact that in many cases it is the human factor that is behind incidents or is exploited during attacks. For this reason, it is important to raise the awareness and ability of all users of IT systems and to create conditions for developing a security culture throughout society.

To reduce vulnerabilities and to promote the objectives of Sweden's security and IT policy, it is the Government's assessment that society's cyber security efforts above all need to prioritise

- securing a systematic and comprehensive approach in cyber security efforts
- enhancing network, product and system security
- enhancing capability to prevent, detect and manage cyberattacks and other IT incidents
- increasing the possibility of preventing and combating cybercrime
- increasing knowledge and promoting expertise
- enhancing international cooperation

In the following sections, the Government sets out a number of objectives for each of these priorities, indicating a direction for how these objectives are to be achieved.

2 Strategic priorities

2.1 Securing a systematic and comprehensive approach in cyber security efforts

Systematic cyber security efforts

Objectives:
- Central government authorities, municipalities, county councils, companies and other organisations are to have knowledge of threats and risks, assume responsibility for their cyber security and conduct systematic cyber security efforts.
- There is to be a national model to support systematic cyber security efforts.

Having good cyber security is important for most activities to achieve their quality and effectiveness requirements. Improving cyber security is therefore not only a matter of satisfying external requirements, but is also a way of improving an activity. At the same time, cyber security cannot be viewed as only being the concern of the activity itself. Services and products flow in several stages, and deficiencies in cyber security can therefore have repercussions far beyond the boundaries of the activity.

Responsibility, risk awareness and a comprehensive view

Successful cyber security efforts presuppose clarity in terms of who is responsible for them. This applies at all levels – both within organisations and in society as a whole.

Both public and private stakeholders need to be aware that risks related to cyber security have an effect on the goals of their activities and that their ability to handle information might also have an effect on other stakeholders in society. Investments to incorporate and improve security should always be compared to what it might cost not to make them. The goal is to find the right levels of security and for those responsible to be aware of the risks that exist so that they will be able to make active decisions to eliminate, reduce or accept these risks. Such risk awareness constitutes the foundation of effective investments in cyber security.

In order for information management and IT use in society to develop in a safe and secure manner, it is necessary for all stakeholders to have a comprehensive view of cyber security, which is a complex and multidisciplinary area, covering fields including technology, administration, economics and law. Cyber security is to be a natural and integral part of all work at all levels of society: within and between organisations and within and between the different sectors of society. Security measures should aim to create a more robust information management when society is in a normal state and to manage more serious disruptions and crises.

National model for systematic cyber security efforts

At present, the different stakeholders in society conduct their cyber security efforts in partly different ways, according to different conditions and needs, based on several different regulatory frameworks and partly different perceptions of threats and risks. The same information can receive different levels of protection in different organisations and many stakeholders have insufficient knowledge of which type of protection is appropriate and available for a certain type of information.

When many stakeholders are dependent on each other in their information management, it is also necessary to coordinate measures to reduce risks and maintain the level of security. Stakeholders whose cyber security is inferior can jeopardise the security of the others. This is of significance to the potential for a digitally collaborative administration, but also to the resumed planning of civil defence that is dependent on good conditions for sharing sensitive information within public administration.

Although the individual organisation is ultimately responsible for managing its information, in the Government's assessment it is important to improve the conditions for conducting systematic cyber security efforts in a more coordinated manner. To achieve this, there is a need to carry out activities such as performing risk assessments, mapping security-sensitive assets and determining levels of protection with associated security measures based on and supported by a common model for systematic cyber security efforts. Such a model aims to constitute a common platform for systematic cyber security efforts and to be able to coordinate and collate regulations, methods, tools, training, etc. at the authority level in a readily available manner. It is assessed that a national model will contribute to stakeholders making more uniform assessments of threats, risks and security measures, thereby attaining a similar and adequate level of protection for similar data and information systems at different operators.

There are many advantages of a national model for systematic cyber security efforts. If the authorities that have a particular responsibility in the cyber security area, and the other authorities that, e.g., have a regulatory or supervisory role in the area, actively contribute to the national model, this can counteract fragmentation of steering and increase collaboration in the area. This will make it easier for organisations to address relevant requirements and control their cyber security efforts, while making more effective use of the competence of the expert and supervisory authorities. Since the national model will be based on recognised standards, and will be flexible and scalable, activities with different conditions can benefit from the model.

It is also expected that more uniform assessments of security measures will be able to bring positive effects both for those procuring security solutions and those supplying them. Developing a large number of unique but similar solutions is not rational for either customer or supplier. The national model's ability to contribute experience-based knowledge of appropriate requirements could help to increase overall procurement expertise.

The main purpose of a national model for systematic cyber security efforts is to raise the lowest level of cyber security. The first stage should focus the model on central government authorities, but the model should be designed with the goal of benefiting the entire public sector, other organisations and companies. The Government's intention is that a national model for systematic cyber security efforts will be able to develop in a way that also facilitates the Government's monitoring of cyber security efforts in public administration.

The Government will work to

- increase the clarity of authority governance and highlight the importance of satisfactory cyber security efforts internally at the authorities,
- improve the conditions for the different stakeholders in society to conduct systematic cyber security efforts and make more uniform assessments of threats, risks and security measures, through the development of a national model for systematic cyber security efforts.

Collaboration and information sharing

Objective:
Collaboration and cyber security information sharing is to be enhanced.

The complexity, multidisciplinary nature and rapid development of cyber security requires effective collaboration. Good collaboration on society's cyber security is important during a normal state, but also a necessity for being able to create good operational capability to manage serious disruptions. The collaboration built up as part of preventive efforts often lays the foundation for the collaboration needed during serious incidents. This involves collaboration between different stakeholders in Sweden, such as central government authorities, municipalities and county councils, trade and industry and interest organisations, but also international collaboration (Chapter 2.6).

There are several good examples of collaboration in the area of cyber security in Sweden. The Cooperation Group for Information Security (SAMFI) plays an important role through its work for secure information assets in society. SAMFI consists of a number of central government authorities that have particular tasks in the area of cyber security: the Swedish Civil Contingencies Agency (MSB), the Swedish Defence Materiel Administration, the National Defence Radio Establishment (FRA), the Swedish Armed Forces, the Swedish Police Authority, the Swedish Post and Telecom Authority (PTS) and the Swedish Security Service. MSB has administrative responsibility for the group. The collaborative forum, the National Cooperative Council against Serious IT Threats (NSIT), analyses and assesses threats and vulnerabilities regarding serious or qualified cyberattacks against our most security-sensitive national interests. NSIT consists of the Swedish Security Service, FRA and the Swedish Armed Forces through its Military Intelligence and Security Service (MUST).

The Government sees a need to develop and deepen collaboration between authorities in order to increase society's cyber security. One example of this need is that a number of new authorities will receive new tasks in the area of cyber security when the NIS Directive is implemented in Swedish legislation. It is important that collaboration is developed on the basis of a comprehensive perspective.

Public-private collaboration is a voluntary, agreed cooperation between public and private stakeholders. The cyber security area has several examples of platforms for public-private collaboration. One of these is MSB's establishment of a number of forums for information sharing (FIDI) in different sectors and areas: FIDI Telecom, Swedish CERT forum, FIDI Finance, FIDI Health and Social Care, FIDI Operations and FIDI Supervisory Control And Data Acquisition (SCADA). The area of electronic communications also has the National Telecommunications Coordination Group (NTSG). NTSG is a voluntary cooperation forum aimed at supporting the restoration of the national infrastructure for electronic communications during extraordinary events in society. There is a need to further develop information sharing regarding threats, risks and security measures in order to quickly adapt the protection of more stakeholders.

The Government will work to

- enhance collaboration between authorities that have particular tasks in the area of cyber security,
- ensure appropriate information sharing and collaboration between public and private stakeholders.

Supervision in the area of cyber security

Objective:
There is to be appropriate supervision to create conditions for increasing society's cyber security.

A prerequisite for the intended impact of the cyber security rules is the existence of supervision that can be performed in an effective and appropriate manner. In its report on information security in the civil public administration (RIR 2014:23), the Swedish National Audit Office pointed to the need for supervision and recommended a number of measures, including expanding supervision of information security in the civil public administration. It is the Government's assessment that several measures need to be taken. In the first instance, there is a need to develop the supervision of activities covered by the protective security legislation and critical infrastructure within the sectors identified in the NIS Directive.

Supervision under the protective security legislation

The Protective Security Act contains provisions on protective security, which refers to protection against espionage, sabotage and other crimes that might threaten the security of the realm, protection in other cases of classified information concerning the security of the realm, and protection against terrorism, even if it does not threaten the security of the realm.

According to the protective security legislation, there are two supervisory authorities that have the main responsibility, the Swedish Security Service and the Swedish Armed Forces. In consultation with the responsible authorities (the public utility Svenska kraftnät, PTS, the Swedish Transport Agency and the county administrative board), these can also exercise supervision of the authorities of the sectors concerned. The responsible authorities also exercise their own supervision of the sector. All supervisory authorities have the right to issue regulations.

The report A new Protective Security Act (SOU 2015:25) states, inter alia, that societal developments mean that security-sensitive activities are increasingly being conducted by private actors. A reasonable conclusion, according to the report, should be that the incidence of private forms of activity will probably increase within the supervisory area but that supervision will mainly continue to concern authorities and other public bodies. The inquiry stressed that access to intervention powers, e.g. in the form of sanctions, is characteristic of effective and appropriate supervision. Today, there are no such powers with respect to protective security. The inquiry nevertheless made the assessment that there were not sufficient grounds at that time for changing the focus and implementation of supervision. For this reason, no proposal to introduce sanctions was submitted. However, the inquiry pointed out that it is vital to closely monitor developments and to follow up the question in the not too distant future.

On 23 March 2017, the Government commissioned a Public Inquiry to, inter alia, investigate and propose a system of sanctions in the protective security legislation (ToR 2017:32). The Public Inquiry is also to perform a review of the supervision provisions under the Protective Security Act and submit proposals on how appropriate supervision of security-sensitive activities should be designed. The inquiry report is to be presented in May 2018.

Implementation of the NIS Directive

The NIS Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union. Under the Directive, each Member State shall designate one or more national competent

authorities on the security of network and information systems for certain services in designated sectors. The designated sectors are energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution, and digital infrastructure. The competent authorities shall monitor the application of the NIS Directive at national level.

In March 2016, the Government commissioned a Public Inquiry to propose how the NIS Directive is to be implemented in Swedish law (Ju 2016:11). The inquiry's findings were recently presented through the report Informationssäkerhet för samhällsviktiga och digitala tjänster [Cyber security for essential and digital services] (SOU 2017:36). The Public Inquiry's proposals include how to implement the Directive's requirements for designating authorities with responsibility for certain functions, with a focus on assigning MSB a coordinating role in the area but that other authorities be given responsibility for supervision within the various sectors. The Public Inquiry further proposed how the identification of operators covered by the Directive, and the requirements on them, can be implemented in one comprehensive regulatory framework, taking into account existing provisions, sector responsibility and what is most effective on the basis of different perspectives.

The Government will work to

- ensure that the protective security legislation more effectively meets the changing demands on protective security in the area of cyber security, in part through an adequate system of sanctions and an effective supervision,
- ensure the effective implementation of the NIS Directive and to establish an adequate steering and supervision of the security of network and information systems in critical infrastructure for certain operators within the designated sectors,
- monitor the need for further measures to develop the supervision of cyber security throughout society.

2.2 Enhancing network, product and system security

Secure infrastructure for electronic communications

Objectives:
- Electronic communications are to be effective, secure and robust and are to meet the needs of their users.
- Electronic communications in Sweden are to be available independent of functions outside the country's borders.
- The supervisory authority's need for being able to take adequate measures is to be met.

Private individuals, central government authorities, municipalities, county councils, companies and other organisations are today dependent on reliable electronic communications services that function in all conditions. Electronic communications with high operational reliability and strong protection are also of very high importance to the functioning and security of society and to the ability to manage various crises. Critical infrastructure relating to public order, safety, health and defence are in particularly great need of security and robustness.

Operators of electronic communications are a heterogeneous group that currently work in a competitive market. Some of them own their networks, while others rent the networks of other operators. Ownership structures can vary from major publicly listed companies to urban networks and village cooperatives. This in itself means that the stakeholders have different conditions for preventing and managing incidents and serious events.

Ensuring confidentiality, authenticity and availability in electronic communications networks and services both in everyday conditions as well as serious crises and heightened alert requires continuous efforts based on the operators' risk and vulnerability analyses and security analyses under the Protective Security Act. All operators also bear a responsibility for developing the capability to prevent, detect and manage incidents.

External changes affect security demands

The extent of data management is increasing in all parts of society, with demands for increased capacity, coverage, availability and not least security in electronic communications systems. The old copper networks are being phased out and replaced with fibre and mobile communications networks. To drive digital development and harness its opportunities, the Government adopted the strategy A Completely Connected Sweden by 2025 − a Broadband Strategy (N2016/08008/D) in December 2016 and For sustainable digital transformation in Sweden – a Digital Strategy (N2017/03643/D) in May 2017. The EU is currently reviewing the regulatory framework for electronic communications, and the OECD has initiated an extensive digital transformation project. Policy and regulatory frameworks need to be renewed more frequently in light of technological development and external changes.

Security policy developments have resulted in the resumption of total defence planning. If stakeholders in the areas of public order, safety, health and defence are to be able to fulfil their commissions, they need to be able to communicate securely with each other, both in everyday conditions and in crises. The ambition is to as far as possible be able to maintain electronic communications within the country even in situations where the surrounding region or parts of Sweden have been hit by various types of attack. This means that electronic communications are to be able to function independently of functions in other countries. It also means an increase in the demands on operational reliability and robustness to make us better able to resist attacks and ultimately war.

Support in the procurement of secure electronic communications and other IT-related services should be enhanced

It is important for the activities needing a high level of operational reliability in communications networks and IT-related services to set requirements to this effect in their procurements. This might, for example, concern the capability to quickly and effectively establish alternative links. It is also important to be able to identify and procure a level of operational reliability that is appropriate to the activities concerned. This requires expertise. PTS is the supervisory authority for the areas of postal services and electronic communications. The Authority's work includes helping stakeholders in the sector to enhance their capability to manage serious operational disruptions, for example by providing support in the acquisition of external electronic communications. MSB also provides support regarding the secure procurement of IT-related services. The support of both authorities now needs to be developed further. In this context, it may also be mentioned that the National Agency for Public Procurement has overall responsibility for the development, administration and support of the procurement carried out by procuring authorities.

The need for better decision-making documentation and targeted measures

A prerequisite for effective work to prevent threats and vulnerabilities regarding electronic communications is developed coordination and collaboration between relevant stakeholders in order to identify what is to be protected and which further security measures need to be deployed. The ability to analyse current threats and vulnerabilities requires adequate information, for example, information from electronic communications operators through incident reporting and information

from expert authorities. Under the NIS Directive, several providers of electronic communications will be imposed with expanded incident reporting. Incident reporting under the NIS Directive is described in Chapter 2.3. However, further measures might be necessary in order to improve the information needed to support the preventive work.

As supervisory authority, PTS needs to be able to obtain, coordinate and forward information and, in certain circumstances, take measures to enhance society's access to secure electronic communications. Furthermore, in order to assess any consequences for society as a whole, PTS needs to obtain information from the operators concerning events with an impact on network security or cyber security. This also includes being able to create and forward relevant and current status reports in a crisis situation. There is also a need for PTS to be able to impose specific security measures on one or a limited number of operators in order to manage identified vulnerabilities or deficiencies that might entail serious risks to societally important electronic communications. In these cases, ordinary regulations are not appropriate since they apply to the market in general, and not only with respect to designated stakeholders, and they do not usually contain detailed requirements for specific networks and services.

The need for enhanced collaboration

In order to identify appropriate measures to minimise the threats and vulnerabilities that exist within the electronic communications sector, PTS needs access to relevant expertise. This expertise can be obtained from stakeholders in the sector and from expert authorities, for example. For this reason, an in-depth and systematic collaboration both with the sector's stakeholders and between authorities in the area of cyber security and supervision constitutes a good basis for increasing expert support to the cyber security efforts of authorities that have sectoral responsibility.

The Government will work to:

- ensure that electronic communications networks are built in such a way that they can function independently of functions in other countries,
- ensure that stakeholders in the areas of public order, safety, health and defence have access to modern, secure and robust communications solutions,
- enhance the authorities' expertise regarding the procurement of networks, products and systems and to ensure that the authorities guarantee that security aspects are taken into account in procurements,
- enhance the conditions of PTS to pursue a high level of network and cyber security within the electronic communications sector.

Secure data encryption systems

Objective:
Access to secure data encryption systems for IT and communications solutions are to meet society's needs.

A common security measure to increase cyber security is the use of data encryption. Information that needs to be protected by means of data encryption might, in addition to information that is vital to the security of the realm, consist of healthcare data, risk and vulnerability analyses, preliminary investigations or asylum cases, for example.

Data encryption solutions are currently used not only for communications in the traditional sense of protecting information that is classified or otherwise sensitive from a security perspective. Data encryption is also used to protect, for example, the signing of information (authenticity), automated processes in vital societal functions

such as critical infrastructures (availability) and the monitoring of how and when information has been managed and communicated.

Some organisations have a need to protect information that is classified with reference to the security of the realm and have a need for communications security. The term communications security refers to the mandatory protection of electronic communications of classified information concerning the security of the realm. The protection level of the communications security systems is dimensioned to meet the threat scenario from other countries' intelligence services and therefore requires extensive protective measures. Sweden needs to have access to technical expertise in the area of data encryption to guarantee necessary communications security, for ordinary activities and when society is subjected to stress. The maintenance of such national expertise over time is therefore important for safeguarding Swedish security interests in the area.

The need for secure data encryption solutions is increasing in pace with digital transformation. The resumption of civil defence planning will also entail a greater need for secure data encryption systems, especially communications security, for the stakeholders in society affected by this planning work. There is also a greater need for communications security to enable developed collaboration with other states and international organisations, particularly within the EU and NATO.

To meet this greater need for data encryption solutions, the Government has recognised a need for a national strategy and action plan for secure data encryption systems. In its appropriation directions for 2016, the Swedish Defence Materiel Administration was therefore commissioned to present a detailed proposal for a national strategy and action plan for this, after consultation with the Swedish Armed Forces, FRA and MSB.

The Government will work to

– implement a national strategy and action plan for secure data encryption systems.

Security in industrial information and control systems

Objective:
Security in industrial information and control systems is to increase.

Industrial information and control systems, often termed Programmable Logic Controller (PLC) or SCADA, are used in critical infrastructure to control and monitor central physical processes. These control systems (software and computers) are integrated into, and interact with, physical objects. With the emergence of the Internet of Things, there is also a sharp increase in the number of connected control systems in many areas.

Both the report Cyber security in Sweden (SOU 2015:23) and the report on a new Protective Security Act (SOU 2015:25) stress the critical infrastructures' dependence on industrial information and control systems and the importance of maintaining a strong national expertise in the area of control systems. Securing the functionality and security of industrial information and control systems constitutes a very important part both of preventive work and of the management of disruptions to central societal functions, such as the electricity and drinking water supply. Disruptions in areas such as transport systems, industrial production and healthcare are also examples where preventive work is important. Disruptions might have their origin in mistakes of operation or be due to faults in hardware or software, but might also be the result of antagonistic activities.

Industrial information and control systems are characterised by technical complexity and by very diverse ownership and operating conditions. Managing the challenges in this area requires a comprehensive effort that includes both the private and public sectors. The work needs to be cost-effective and cross-sectoral. In order to achieve adequate protection, there is a need for greater collaboration and cooperation between system providers, technical consultants, procurers, operators, relevant authorities and academic environments.

A high level of cyber security in industrial information and control systems has the potential to constitute a significant competitive factor for Sweden. If high-security products can be developed in Sweden, they will be more internationally competitive and thereby contribute to employment in Sweden.

Today, a large part of the training, research and development in this area is conducted under the National Centre for Security in Control Systems for Critical Infrastructure (NCS3), which is jointly run by MSB and the Swedish Defence Research Agency (FOI). NCS3's activities aim to reduce the risks that the use of industrial information and control systems entails for modern society, especially with regard to intentional disruption. The Swedish Governmental Agency for Innovation Systems (Vinnova) and the Research Institutes of Sweden (RISE) are also working actively on projects for developed security in industrial information and control systems.

The Government will work to

- ensure that companies and authorities that own or work with critical infrastructure that include industrial information and control systems receive support in their efforts to enhance cyber security,
- ensure that companies with activities in industries such as engineering and processing, where industrial information and control systems have important functions, receive developed conditions for support to enhance their cyber security efforts.

2.3 Enhancing capability to prevent, detect and manage cyberattacks and other IT incidents

Objectives:
- The capability to prevent, detect and manage cyberattacks and other IT incidents in society is to be improved.
- Relevant stakeholders are to be able to take coordinated action to manage cyberattacks and other serious IT incidents.
- There is to be a developed cyber defence for the most security-sensitive activities in Sweden, with a strengthened military capability to meet and manage attacks from qualified opponents in cyberspace.

The basis for reducing the effects of cyberattacks and other IT incidents consists of the capability to prevent, detect and manage them.

A large part of the preventive work has been described in Chapter 2.1 about securing a systematic and comprehensive approach in cyber security efforts and in Chapter 2.2 about enhancing network, product and system security. Another important component of the preventive work consists of IT incident reporting, which includes facilitating a continuous learning from events that have occurred. Since April 2016, most central government authorities have been required to report IT incidents that might seriously affect the security of the authority's information management to MSB. In order to improve awareness of the national situation, MSB's instructions

include the annual submission of a report to the Government compiling the incidents that have been reported to the authority. Prior to this compilation, MSB is to obtain information from the Swedish Security Service and the Swedish Armed Forces about the incidents that have been reported to those authorities under the protective security legislation. The next step in developing IT incident reporting will be taken through the NIS Directive. This will include making it mandatory for stakeholders within the NIS sectors to report incidents that have a significant impact on the continuity of essential services. All in all, this IT incident reporting will improve the general knowledge of incidents that have occurred and effective security measures. In order to support the stakeholders' preventive cyber security efforts, the Government considers it important to develop methods to provide reporting stakeholders with feedback on IT incidents that have occurred.

If it is to be possible to detect attacks, there needs to be access to sensors and other mechanisms that detect events and such traffic that is part of an attack. FRA provides a technical detection and warning system (TDV) focusing on the most security-sensitive activities among central government authorities and state-owned companies. In spring 2017, the Government referred a memorandum on technical sensor systems (Ju2017/02002/L4) for consideration, proposing that MSB may support the cyber security of operators in critical infrastructure by providing sensor systems that can enhance the opportunity of society to detect and manage IT incidents. MSB's sensor systems are not to be provided to the organisations that are offered TDV. Specially designed security networks can be a further method for safeguarding security-sensitive activities from attack. Such networks can be common to several authorities so as to allow them to detect and impede attacks in a cost- and resource-effective manner.

Managing IT incidents requires a capability to withstand the consequences of the event and to restore systems. To be able to manage serious cyberattacks or other IT incidents, every stakeholder conducting activities that are security-sensitive or that are part of a critical infrastructure has a responsibility to develop contingency and continuity plans based on relevant risk analyses, including risk and vulnerability analyses and protective security analyses. In connection with an IT incident, the affected organisation might be in need of external support to manage the incident. Such support can be obtained from private companies, but MSB also offers support through CERT-SE, which is Sweden's CSIRT unit (Computer Security Incident Response Team). Some central government stakeholders with particularly security-sensitive activities have the opportunity to receive support from FRA. If it is a question of an IT incident concerning the security of the realm, it is managed by the Swedish Security Service and the Swedish Armed Forces. Where the event has its origin in criminal activities, the Swedish Police Authority or the Swedish Security Service performs a criminal investigation.

It is the Government's assessment that there is a need to develop the capability of society to act in a coordinated manner to resist a cyberattack or other serious IT incident. A developed capability of this kind is an important part of strengthening Sweden's total defence capability.

Cyber defence

A Swedish cyber defence that is sufficiently robust to withstand and manage cyberattacks while also being prepared for any need to quickly take active measures, requires coordination of competencies, as well as designated and exercised decision paths between different authorities and societal functions. Sweden's overall cyber defence capability is therefore based on a broad understanding of the existence and nature of the relationship between, for example, measures taken to raise the lowest level of cyber security efforts, and the work of protecting society against cyberattacks.

The foundation of a robust cyber defence capability is securing the functionality of vital societal functions and protecting security-sensitive activities, including systems that are vital to the total defence, against antagonistic attacks from qualified state or state-sponsored actors and from other actors with similar capability. It is the Government's assessment that a developed cyber defence is a cost-effective way to further raise the threshold for an antagonistic actor who is considering attacking Sweden or Swedish interests or exerting pressure using military or other instruments of power.

An effective national cyber defence is developed and strengthened in peacetime and as part of total defence planning and must be capable of functioning in peace, crisis and war. The activities using information systems that must be able to withstand qualified attacks from state and state-sponsored actors must develop their protection in peacetime. A national cyber defence presupposes a strong national security service and defence intelligence capability to identify threatening activity, regarding actors and methods, a strong protection of the most security-sensitive societal infrastructures, a high capability to detect, warn of and manage intrusions and attacks, as well as a robust capability to conduct active operations in the cyber environment.

The Swedish Armed Forces is to maintain and develop a military defence that might ultimately encounter an armed attack. Cyberspace is one of several arenas in which the Swedish Armed Forces must be able to act. The Swedish Armed Forces is the authority that is to operate in all parts of computer and network operations and with a capacity for the higher levels of conflict. Support from the other relevant authorities is necessary.

International collaboration is important for developing capabilities including national cyber defence and is to be sought where this is appropriate.

The Government will work to

- ensure coordinated planning between authorities in the event of a cyberattack or other serious IT incident,
- ensure that activities in need of continuous monitoring and with particular needs of protection receive access to a sensor system or detection and warning system,
- ensure the continued development and strengthening of an effective and seamless cyber defence with the capability to prevent, detect and manage cyberattacks, both for military and civilian activities, which also includes the Swedish Armed Forces developing its capability to defend Sweden against qualified attackers in cyberspace.

2.4 Increasing the possibility of preventing and combating cybercrime

Objectives:
- The law enforcement authorities shall have the preparedness and capability to combat cybercrime in an effective and appropriate manner.
- The work to prevent cybercrime shall be developed.

Brå concludes that the elements of IT in the reported crimes are increasing sharply (2016:17). These include crimes committed with the aid of the internet, such as fraud, and crimes entailing that the content conveyed via the internet is criminal, e.g. child pornography or agitation against a national or ethnic group. Another example is attacks on IT systems as such, e.g. through intrusions or denial-of-service attacks. A special category of cybercrime is also that entailing an infringement of intellectual

property rights. Other types of crime, such as unlawful threat and defamation, also occur via the internet.

In addition, in many preliminary investigations, relevant information or evidence can be obtained on the internet or in an information system, even if the offence itself has not been committed in such an environment.

A characteristic feature of cybercrime is that it is cross-border, e.g. through denial-of-service attacks from one country to another or fraud carried out from a server in a country in which it can be very difficult to investigate the crimes. There are also many examples of crimes that have no link to countries other than Sweden, but where information decisive to the investigation is held by a company in another country. This might, for example, involve threats and violations on social media.

In its report Elements of IT in criminal activity (2016:17), Brå makes the summary assessment that the judicial system faces major future challenges and that the investments made so far in the IT area do not correspond to the need. Brå finds, inter alia, that there is a great need for training within the Swedish Police Authority and the Swedish Prosecution Authority, that the cutting-edge expertise of IT investigators needs to be ensured, that the staffing of IT forensic activities needs to increase and that knowledge at the authorities' expert functions needs to be utilised better.

In its audit of whether the Swedish Police Authority and the Swedish Prosecution Authority have preparedness for processing and investigating cybercrime appropriately and effectively, the Swedish National Audit Office draws conclusions that are partly in accord with those of Brå (RIR 2015:21).

Adaptation of legislation

In order to create better conditions for combating cybercrime, the Government has taken a number of measures to obtain a better adapted legislation. In recent years, several amendments have been made in the penal legislation. These include the introduction of a new crime in the Swedish Penal Code, unlawful use of identity. Furthermore, on 1 July 2017, the Penal Code will introduce a new crime, gross invoice fraud, in order to resolve the problems of fraud using "scam invoices".

Work is also under way to produce proposals to enhance the penal protection of personal privacy. In a referral to the Council on Legislation of 8 June 2017, the Government proposed that protection against threats and violations be enhanced and modernised. The proposal includes a new crime making it punishable to disseminate certain images and data that are sensitive in terms of privacy. Furthermore, proposals are currently being produced for amendments to the legislation concerning contact with a child for a sexual purpose, known as grooming, which often takes place via the internet. A review of the child pornography crime has also been initiated. Work is also being done to ratify the Council of Europe's Convention on Cybercrime (ETS 185).

Furthermore, a number of issues aimed at modernising the legislation on coercive measures are currently being investigated. For example, the rules on seizure in criminal investigations were mainly designed before the advent of IT in society and are therefore not adapted to application in IT environments. Another issue being investigated involves the increasing difficultly to execute decisions on the covert interception of electronic communications since suspects are increasingly encrypting their communications.

For the law enforcement authorities, access to information on electronic communications is very important to their ability to investigate both cybercrime and other crime. However, in a preliminary ruling of 21 December 2016 (in joined cases C-203/15 and C-698/15), the Court of Justice of the European Union came to the

conclusion that the general and indiscriminate retention of electronic communications data is not compatible with EU law.

A Public Inquiry is therefore to propose the amendments that are necessary for the Swedish regulations to be proportionate and have an appropriate balance between the protection of individual personal privacy and the need for information in order to prevent, impede, detect, investigate and prosecute crimes.

The Government believes that it is important for the regulations to be effective and appropriate and for the legislation to be designed to allow new types of crime to be counteracted.

Development of activities at the authorities

A better ability to prevent, detect, investigate and prosecute cybercrime requires not only appropriate legislation but also that the law enforcement authorities develop the organisation and expertise that are needed. In their appropriation directions for 2017, the Swedish Police Authority and the Swedish Prosecution Authority were commissioned by the Government to secure adequate expertise and preparedness with regard to cybercrime. This commission took into account the reviews by the Swedish National Audit Office and the Swedish National Council for Crime Prevention.

As regards sexual crimes against children, the Government has commissioned the Swedish Police Authority to identify areas where there is a need for development and to implement appropriate measures. The commission's focus includes internet-related sexual crimes against children and documented sexual assault of children. The commission will be carried out at the national cybercrime centre established at the Swedish Police Authority on 1 October 2015: Swedish Cyber Crime Center (SC3). SC3 was formed in order to use its expertise to ensure and develop investigative support, working methods, uniformity and international cooperation with regard to all forms of cybercrime.

The rapid development of cybercrime places great demands on the capability of the law enforcement authorities to continue developing their activities. This work should, according to the Government, be conducted continuously.

Crime prevention

As with other crime, when it comes to cybercrime it is important to first reduce the inflow to the judicial system and prevent crime at an early stage. More stakeholders beyond the law enforcement authorities need to actively participate in prevention; not least trade and industry plays an important role. Non-law enforcement authorities and industry can, for example, be involved in prevention by helping to enhance society's control functions and develop technical solutions for increasing security. In order to create better conditions for a structured and long-term crime prevention throughout society, the Government has, inter alia, submitted a communication to the Riksdag containing a national crime prevention programme in March 2017 (Communication 2016/17:126).

International cooperation against cybercrime

The explicit cross-border dimension of cybercrime means that international cooperation has increased in both scope and importance. Opportunities for cooperation through the EU and its authorities, Eurojust and Europol, are those which are the most important for Swedish law enforcement authorities. Eurojust's measures have included the establishment of a special network for prosecutors specialising in cybercrime, and Europol set up a cybercrime centre a few years ago. Both of these cooperation mechanisms are important for legal assistance, e.g. seizures and information exchange.

On the political level, the EU Member States adopted in June 2016 Council conclusions on improving criminal justice cooperation in cyberspace. The three different sections of the conclusions treat the development of voluntary cooperation with service providers, the streamlining of mutual legal assistance and the issue of enforcement jurisdiction (authorities' right to independently secure evidence) in cyberspace in situations where existing frameworks are not sufficient.

Furthermore, in September 2016, an evaluation was made of Sweden's capability to combat cybercrime as part of the EU's mechanism for mutual evaluations. A report containing recommendations will be treated in spring 2017, and 18 months after the adoption of the report Sweden is to report on the measures taken to rectify identified deficiencies.

As many of the problems faced by the Swedish law enforcement authorities are also found in other countries, the Government believes that there is an explicit need for continuing to develop the international cooperation in this area, particularly within the EU.

The Government will work to

- adapt the legislation to allow it to counteract cybercrime effectively,
- provide the law enforcement authorities conditions, with reference to the protection of personal privacy and legal certainty, to maintain their capability to obtain information,
- ensure that the law enforcement authorities guarantee an adequate organisation and sufficient resources to effectively prevent and combat cybercrime,
- ensure that the law enforcement authorities work systematically to develop expertise and working methods to prevent and combat cybercrime,
- increase the awareness and knowledge of non-law enforcement authorities regarding how they can contribute in the work to prevent cybercrime,
- strengthen the international cooperation against cybercrime in order to increase legal proceedings in Sweden.

2.5 Increasing knowledge and promoting expertise

Mapping of vulnerabilities and needs for measures

Objectives:
- Knowledge in society as a whole regarding the most urgent vulnerabilities and needs for security measures is to increase.
- The knowledge of individual digital technology users regarding the most urgent vulnerabilities and needs for security measures is to increase.

There is a great potential for development regarding cyber security in Sweden, both at the societal level and at the individual level. However, cyber security knowledge and resources possessed by various organisations, and not least by private individuals, are often limited, for which reason it is important to be able to focus on the most urgent needs. The Government believes it is central that the cyber security measures taken are cost-effective.

In cooperation with relevant stakeholders, MSB maps and examines society's cyber security efforts. Among other things, MSB has in close collaboration with the Swedish Association of Local Authorities and Regions (SALAR) examined systematic cyber security efforts in the municipalities (MSB943). MSB's analysis of this examination has culminated in eight recommendations to the municipalities (MSB1045). In the Government's assessment, it is important to continue developing

and deepening the work to analyse vulnerabilities, deficiencies and needs linked to Sweden's cyber security in order to support and increase awareness of long-term cyber security efforts at all levels of society.

In the same way as the functioning of society is dependent on IT systems and IT services, individuals are also reliant on such systems for managing more and more parts of their everyday lives. These involve payments, education, contacts with authorities and municipalities, etc. Today, almost everyone in Sweden has access to high-capacity broadband both at work and at home.

The digital strategy (N2017/03643/D) emphasises that the goal is for people, companies and organisations to have trust and confidence in the use of digital services. Individuals always have a responsibility of their own for protecting their information and their connected devices, but it is also important that society addresses threats and risks that are specifically directed against individuals in their use of IT systems and digital services. There are, at present, various initiatives for the cyber security of individuals, for example, by the Internet Foundation in Sweden, MSB, the Swedish Police Authority and other stakeholders. These initiatives are important and need to continue being developed.

The Government will work to

- ensure that relevant authorities develop the work to implement and support the mapping and investigation of vulnerabilities and appropriate security measures in society,
- increase people's knowledge of vulnerabilities and appropriate security measures that everyone can take to protect themselves.

Higher education, research and development

Objective:
Higher education, research and development of high quality are to be conducted in the areas of cyber security and of IT and telecom security in Sweden.

Development of IT and telecom is a natural step in the increasingly globalised infrastructure that is being built up. This entails many opportunities, but also demands an increase in research on digital security to ensure that cyberspace remains open, free and secure.

Today, research on cyber security is conducted to varying degrees at several Swedish higher education institutions. Applied research on cyber security is conducted at institutions including the Swedish Defence Research Agency, the Swedish Defence University and the Swedish Institute of Computer Sciences (RISE SICS).

Efforts to safeguard society's cyber security need to be conducted in a long-term and effective manner, and serve the interests of fundamental societal values, such as the protection of personal privacy. This presupposes that these efforts are based on a knowledge base that is both deep and broad with regard to needs, risks, vulnerabilities, threats and opportunities. The need for skilled personnel in the area of cyber security is also great. A lack of cutting-edge expertise affects both the private and public sectors. It should thus be in the interest of all relevant stakeholders to find long-term solutions to satisfy the increasing needs for skilled labour.

The area of cyber security brings to the fore many complex research questions that often require a multidisciplinary approach. Research in fields such as data encryption is of an advanced technical nature, while research focusing on the

individual relates to subjects such as organisational and behavioural science. The development of self-driving cars and intelligent cities raises, for example, sociotechnical, legal and ethical issues that relate directly to cyber security.

The Government Bill Collaborating for knowledge – for society's challenges and strengthened competitiveness (Government Bill 2016/17:50) presents a number of strategic research investments focusing on particular areas, one of which is the Research Centre for Future Digital Transformation Technology. In the bill, the Government points out that it is very important that new technology forming the basis of critical infrastructure is robust and secure since adequate security must be built into these systems from the beginning. To facilitate such a development, open access to research results is very important. The Government believes that research results, such as research data and academic publications, that are produced with public funding should be openly available as far as possible.

On 1 June 2016, the Government presented five strategic innovation partnership programmes to help meet a range of the societal challenges that Sweden is facing. The fifth innovation partnership programme, Connected industry and new materials, focuses on stimulating broad digital transformation of Swedish industry through mobilisation in the form of cooperation between actors. Partnership must be strengthened between established industry, IT and telecom companies, service companies, innovative young companies at the forefront of digitalisation and various research environments to better help maintain and increase Sweden's competitiveness. A special working group under the innovation partnership programme is working to propose solutions in the area of cyber security. The strategic innovation partnership programmes are an important instrument for increasing the quality and benefit of higher education, research and development. One aspect of this is the potential to coordinate the investments of different stakeholders and generate synergy effects.

It is the Government's assessment that long-term partnership and cooperation between relevant stakeholders needs to continue being developed in the area of cyber security.

The Government will work to

- enhance partnerships between higher education institutions, industrial research institutes and the private and public sectors in order to increase utilisation and innovation in the area of cyber security,
- take cyber security into account in all strategic innovation partnership programmes.

Training activities

Objective:
Both cross-sectoral and technical cyber security training is to be carried out regularly in order to enhance Sweden's capability to manage the consequences of serious IT incidents.

A significant component for increasing knowledge and enhancing the capability of activities to manage serious IT incidents is education and training. Regular national and international training is a prerequisite for developing and evaluating structures to manage serious IT incidents and for identifying organisational, technical and administrative development needs. Training can be used to

- validate policies, plans, procedures, equipment and agreements between organisations,
- train personnel with respect to their roles and responsibilities,

- improve coordination and communication between organisations,
- identify resource deficiencies, and
- identify opportunities for improvement at both the individual and organisational levels.

The Government therefore considers it urgent for relevant authorities and other organisations to prioritise participation in cyber security training. MSB, in collaboration with other relevant authorities, maintains the capability for long-term planning and coordination of training activities in order to build expertise and guarantee a good capability to manage serious IT incidents in society. The Swedish Armed Forces maintains a corresponding capability within the scope of its responsibility.

Cyber security training activities should encompass several types of training in order to achieve all the levels and competencies that are needed to manage serious IT incidents. These training activities include everything from seminars to cross-sectoral collaboration. Access to a virtual training environment significantly increases the opportunities for carrying out technical cyber security training. Such an environment makes it possible to practise the management of simulated technical problems under conditions that reflect realistic technical infrastructures and systems. This allows participants to test their processes and technical capability for managing incidents and to develop collaboration with other stakeholders at the same time. The planning for training activities should be long-term so that each individual element contributes to increasing or maintaining capability. Systematic experience management becomes an important part of implementing training results in existing plans, working methods and other activities. Where necessary, the training activities should also take into account other threats and risks that might have a close link to the area of cyber security. One example of this is disinformation and influence campaigns. The training scenario in the area of cyber security, including disinformation and influence campaigns, can help to increase society's overall capability to resist these threats, both in the Swedish Armed Forces' defence planning and total defence planning. Today, a large part of national and authority-specific technical training is carried out with the support of FOI's technical platform CRATE (Cyber range and training environment).

The Government will work to

- maintain the capability to manage serious IT incidents through coordinated training activities.

2.6 Enhancing international cooperation

Foreign and security policy

Objective:
International cooperation on cyber security is to be enhanced, as part of the objective of a global, accessible, open and robust internet characterised by freedom and respect for human rights.

Cyber security – a part of foreign and security policy

Digital transformation and globalisation have an accelerating importance for international relations in general. They create new opportunities, but also new areas of conflict, tensions and vulnerabilities. From having been a delimited and technical matter, focusing on system and operational reliability, cyber security has become an issue of fundamental relevance to peace, security and global development. The

actions of states in the cyber area are having increasingly wider and more comprehensive repercussions in foreign and security policy.

Globally, there are tensions between states regarding the management of cyber security aspects. One main area of tension concerns the view of the role of states and their right to monitor, limit and control both infrastructure and information flows.

Today, cyber security issues are treated from different perspectives in a large number of international organisations and formats, e.g. the UN, EU, OSCE, Council of Europe, OECD, NATO, the Nordic-Baltic cooperation, and in several specialised international organisations and processes (e.g. ICANN, IETF, ITU and IGF), which treat questions of the operation, control and administration of the internet. In addition to this, there are initiatives and processes of significance to the international discussion on rules and standards, such as the "London Process", Freedom Online Coalition (FOC) and the Swedish initiative Stockholm Internet Forum (SIF).

The Government stresses the importance of further developing Sweden's capability to act consistently and effectively in international processes. This requires a better overview, where Sweden's long-term interests can be safeguarded in the context of a large number of processes encompassing political, legal and technical aspects. It also requires better coordination and dialogue between relevant stakeholders nationally.

Freedom and security

The Government's goal for the development of the internet is a global, accessible, open and robust internet characterised by freedom and respect for human rights. The credible and effective promotion of the freedom aspect requires a developed international cooperation to manage the security challenges. External developments, including those in Sweden's surrounding region, underline this need. Adequate security measures will continue to be needed with reference to national security or for combating cybercrime.

At the same time, there is a risk that the desire to control information flows will gain the upper hand in the actions of many states. Tendencies towards the fragmentation and restriction of the internet go against Sweden's fundamental values and long-term economic and security-policy interests. The Government maintains that such a development must be addressed by means of developed international cooperation.

There are also fundamental tensions between states in their view of the roles and responsibilities of non-state actors. The Government wants to counteract a state-led administration of the internet and stresses the central roles and responsibilities of non-state actors for a free and secure internet, where the private sector and civil society can assert their legitimate interests. It is clear that both vulnerabilities and security measures concern and involve the private sector and civil society as a whole. Cooperation and dialogue with non-state actors thus need to continue being developed at the international level.

International law and international standards

Within the UN, there is consensus in principle that international law is applicable in cyberspace, but that there are significant difficulties and challenges in ensuring that the rules are interpreted in unison. Against this background, international discussions are being held on the interpretation and application of international law in cyberspace and on the possibility to establish voluntary international standards and confidence-building measures for the responsible behaviour of states. There is also discussion in this context on the possibility of using international regulations, standards and agreements to verify, designate and demand accountability. The Government stresses the importance of Sweden taking an active role in these discussions and processes, with the aim of preventing conflicts and supporting international consensus on standards for the responsible behaviour of states.

Threats and vulnerabilities

Cyberattacks constitute a growing challenge. States will therefore want to develop international cooperation in order to reduce their vulnerability and enhance their resilience, including those of the EU and NATO for cyber security and cyber defence.

Cyber security must also be taken into account in the context of emerging threat scenarios that are characterised by a combination of open and covert instruments used in an antagonistic and destabilising manner, which also explicitly encompasses and concerns civil society as a whole. International cooperation thus also increasingly encompass the broader issue of influence campaigns and disinformation, with a potential impact on democratic processes, traditional media and social media.

The Government is pursuing developed cooperation within the EU, OSCE and with NATO, and in relation to selected strategic partner countries that share Sweden's interests. Cooperation on the conditions in Sweden's surrounding region have special priority, e.g. the Swedish-Finnish, Nordic and Nordic-Baltic cooperation.

International standards are an important issue in the area of cyber security. Developed and negotiated within Europe and in other international contexts, standards are a prerequisite for cross-border solutions.

Human rights and global development

Human rights apply universally, including online. The Government maintains that a rights-based approach should be a starting point of discussions concerning the opportunities and challenges of digital transformation. Privacy and security in the cyber area are a prerequisite for enabling individuals to exercise their rights and freedoms and to make use of the possibilities of information technology.

Access to an open, free and secure internet constitutes an important instrument for the global enhancement of human rights, democracy, the rule of law and development. The internet opens new channels for people to communicate, interact and express their opinions and to promote their interests in a globalised world to an extent that has not previously been possible. Greater access to information and knowledge also promotes gender equality. Digital transformation and developments in information technology are increasingly a significant engine for economic and social development, not least in terms of creating conditions for the independence of poor people and women and their opportunities for work, and for innovative solutions to development problems in education, finance, agriculture, health and the environment.

The Government will work to

- enhance Sweden's overall action as a stakeholder within relevant international processes (including the UN, EU, OSCE and in partnership with NATO) and in cooperation with like-minded countries (in the Nordic region, the surrounding region, within the EU and with global partners),
- counteract tendencies towards the fragmentation of the internet and the restriction of global flows,
- counteract a state-led administration of the internet and safeguard the roles and responsibilities of non-state actors,
- enhance international cooperation on cyber security and cyber defence in order to manage threats and vulnerabilities,
- enhance international cooperation on the application of international law and the prevention of conflicts, e.g. through the establishment of voluntary standards and confidence-building measures,

– promote an open, free and secure internet in support of human rights and global development.

Trade and economic cooperation

Objective:
Cyber security is to be promoted as part of the ambition to safeguard free flows in support of innovation, competitiveness and societal development.

A free trade that makes full use of the opportunities of digital transformation has great potential for contributing to new job opportunities, enhanced competitiveness and sustainable growth. Regardless of sector, most companies are now dependent on free, cross-border data flows in their activities. At the same time, digital transformation means a greater interest in safeguarding intellectual property rights and security for companies in international competition. This is particularly relevant for a country like Sweden, which has innovation- and knowledge-driven companies on a global market. A robust infrastructure and a well-developed cyber security are also essential for Sweden's ability to attract investments in competition with other countries. The Government stresses the importance of safeguarding cyber security as part of an overarching ambition to promote innovation, competitiveness and societal development.

Free data flows are a prerequisite for an effective digital single market and for trade with the rest of the world. The EU's digital single market strategy aims to enhance and deepen the single market with particular relevance to policy areas affected by digital transformation from a cross-border perspective. Free data flows are also an important offensive interest for the EU in the external trade relations between the EU and the rest of the world. The Government stresses the importance of continuing the work to ensure that there are no barriers to data flows on the single market or between the EU and the rest of the world. Barriers might, for example, consist of unjustified or disproportionate localisation requirements. The purpose of localisation requirements is to force companies to localise data in their own country that would have otherwise been placed in other countries. Such barriers should be eliminated at the same time as it must be possible to consider certain localisation requirements justified with reference to national security and other public interests.

The Government will work to

– continue Sweden's digital leadership within the EU and drive the digital agenda forward by completing the digital single market and by being a driving force as regards discussions on future issues,
– ensure that the EU actively and offensively counteracts digital protectionism and at the same time respects legitimate public interests, such as data protection and national security.

3 Follow-up of the strategy

The Government's aim with this strategy is to create an explicit platform for Sweden's long-term cyber security efforts. The strategy sets out the overarching areas that the Government wishes to prioritise and the objectives for each area. The Government also indicates an overarching direction for how each of these objectives is to be achieved. The strategy will be followed, as needed, by specific commissions and other steering measures to relevant authorities in order for the objectives to be achieved.

The security challenges will not be able to be resolved once and for all. The development of technology and threats means that the area of cyber security is changing and evolving at a rapid pace. This is inter alia reflected in amendments to rules and requirements at the EU and international levels. The strategy must have a flexibility to adapt to rapid external changes and therefore has no fixed duration, but will need to be updated as and when necessary. The Government's intention is to implement a first update of this kind in 2018 in order to adapt the strategy to the new provisions and other consequences of the implementation of the NIS Directive in Swedish law.

Ministry of Justice

Excerpt from the minutes of the Cabinet meeting of 22/06/2017

Present: Minister M Johansson, chair, and Ministers Lövin, Hultqvist, Andersson, Hellmark Knutsson, Ygeman, A Johansson, Bolund, Damberg, Bah Kuhnke, Strandhäll, Fridolin, Eriksson, Linde, Skog, Ekström

Rapporteur: Minister Ygeman

The Government adopts Communication A national cyber security strategy (Nationell strategi för samhällets informations- och cybersäkerhet)