A New Era of Cybersecurity

National Strategy for Cybersecurity 2025-2029

Government Offices of Sweden
Ministry of Defence

Contents

Foreword 7

Vision 8

Basic premises of the National Cybersecurity Strategy 9

Target Group 10

National security policy 10

International context for national cybersecurity 12

Cybersecurity landscape 14

Threats from state actors 16

Threats from cyber activists 16

Threats from cybercrime and criminal groups 17

Deficiencies in cybersecurity efforts 17

Complex regulation 19

Skills shortages 19

Inadequate incident management 20

Insufficient information sharing between the private and public sectors 20

Vulnerable supply chains, dependencies and products 21

Produced by: Alice Thoms and Niklas Forsström/Government Offices 2025
Photo: Ulf Grünbaum/Image Bank Sweden (cover), Kristian Pohl AB/ Government Offices (page 7)

Challenges related to the development of digital infrastructure and services 22

Challenges with the connectivity of devices and infrastructure 22

Technological development 22

The government's approach 24

Pillar A: Systematic and effective cybersecurity efforts 26

Target 1: Increased cybersecurity efforts among private and public organisations 27

Target 2: Strengthened cybersecurity in central and local government administrations' information management 28

Target 3: Strengthened cybersecurity efforts in critical infrastructure 31

Target 4: More robust digital supply chains and reduced dependency 32

Target 5: Simplified regulatory compliance and enhanced functional supervision 33

Target 6: Strengthened support for small and medium-sized enterprises' cybersecurity efforts 34

Pillar B: Advanced knowledge and skills development in cybersecurity 36

Target 7: Increased cybersecurity awareness and cyber hygiene in society 37

Target 8: Strengthened skills supply, education and continuous training in cybersecurity 38

Target 9: Strengthened research and innovation in the cybersecurity field 41

Target 10: Enhanced capability to manage the risks and opportunities of emerging technologies 42

Pillar C: Capability to prevent and manage cybersecurity incidents 44

Target 11: More effective and secure national and international information sharing 45

Target 12: Strengthened public-private management of cybersecurity incidents 46

Target 13: Enhanced capability to prevent and combat cybercrime 47

Implementation and follow-up 49

Glossary 50

Digital door lock.

Photo: Maskot/Folio/Image Bank Sweden

Foreword

Minister for Civil Defence
Carl-Oskar Bohlin

The era of cyber-complacency is over. Digital technology now affects almost every aspect of Swedish society and the economy. Technological advancements are emerging at a record pace, and there are no signs of them slowing down. On the contrary, we are facing continued acceleration. As the security situation has deteriorated and cyber threats have increased both in number and complexity, ever greater demands are being placed on Sweden's capability to secure, protect and strengthen society's functions – including in the cyber domain.

Sweden has long benefitted from the opportunities of digitalisation, but cybersecurity has often taken a back seat to other priorities. This is no longer an option. Every day, government agencies, businesses and private individuals are subjected to cyberattacks to varying degrees, and there are strong indications that this threat will continue to grow. AI, machine learning and future quantum computers are fantastic technologies, but they also bring additional risks. For this reason, cybersecurity can no longer be viewed as merely a technological issue; it is now a cornerstone of our society's resilience and a key part of the modern civil defence that Sweden is currently building up.

This new National Cybersecurity Strategy has been developed with important contributions from actors in both the public and private sectors. In the course of this work, one message has become increasingly clear: it is time to move from words to action and enhance Sweden's cybersecurity capabilities. This Strategy and the accompanying action plan are clear expressions of the Government's elevated ambition. They are based on the insight that strong cooperation, particularly between public and private actors, is essential to Sweden's resilience in a rapidly changing, technology-driven world.

This Strategy is a key element of the mobilisation that the Government is now undertaking to enhance cybersecurity. However, this Strategy is of little value without concrete implementation, tangible capacity-building and follow-up. For this reason, I want to urge our government agencies, the business sector and all citizens to realise that every single one of us also has an essential role to play in Sweden's cybersecurity – just like in all parts of Sweden's total defence. Only together can we ensure that Sweden is well-equipped to meet the cybersecurity challenges of both today and tomorrow.

Modern infrastructure.

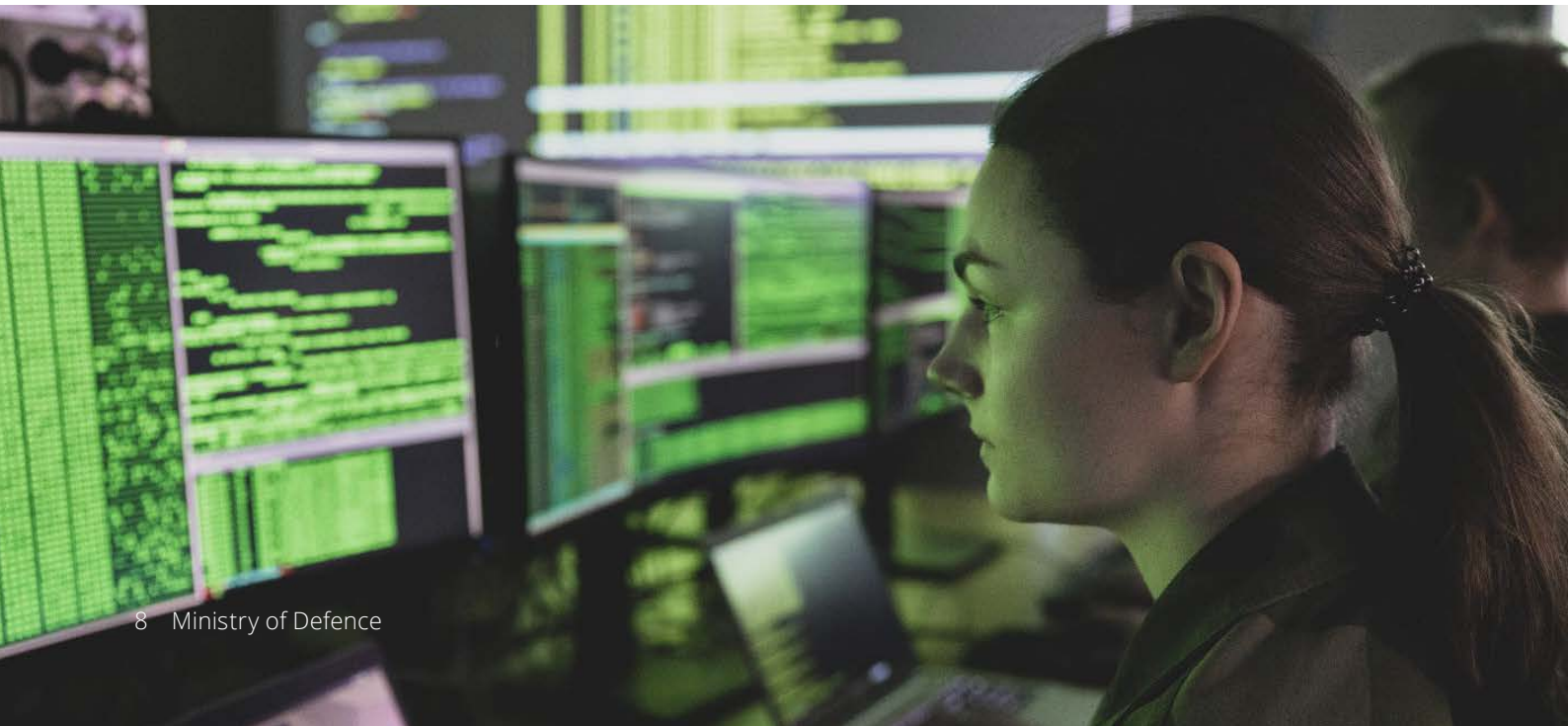
Photo: Felix Gerlach/Image Bank Sweden

Vision

The Government envisions a resilient Sweden with a high level of cybersecurity[1], where essential public services can be maintained even when severe cybersecurity incidents occur. In order to realise this vision, enhanced cybersecurity efforts and intensified, goal-oriented cooperation between central government, the business sector and academia is required. Sweden must draw the full benefit from international cooperation on cybersecurity within the EU, NATO and bilaterally with partner countries in order to actively strengthen both our own cybersecurity and that of other Member States, Allies and partners.

The vision underscores the importance of establishing fundamental and enhanced cybersecurity, and well-functioning cooperation between key actors in the area of cybersecurity, during both peace and war. An effective National Cybersecurity Centre (NCSC) that helps coordinate society's efforts to strengthen Sweden's national cybersecurity capability is needed and will also benefit government agencies with sectoral responsibilities in their efforts to set well-tailored cybersecurity requirements. This is a prerequisite for a high level of cybersecurity and increases Sweden's national capability to prevent, prepare for, address and evaluate cybersecurity incidents. This also helps establish a robust foundation for our civil defence and an effective cyber defence, and contributes to strengthening the position and competitiveness of Swedish businesses. All of this will together result in a more secure Sweden.

1 Cybersecurity: like Directive (EU) 2016/1148 (NIS 2 Directive), this Strategy uses the term 'cybersecurity' instead of 'information and cybersecurity'.



Cyber soldier.

Photo: Joel Thungren/Swedish Armed Forces

Basic premises of the national cybersecurity strategy

The National Cybersecurity Strategy is based on national needs and the NIS 2 Directive and its all-hazards approach to manage a wide range of challenges such as skills shortages, complex rules, vulnerable supply chains and insufficient systematic cybersecurity efforts. In light of the security situation, certain parts of this Strategy also focuses specifically on antagonistic threats across the entire threat spectrum.[1] This Strategy replaces the earlier national strategy for information and cybersecurity (2016/17:213).

The principle of responsibility also applies to the cyber area

A cybersecurity incident could result in a crisis situation in which the 'principle of responsibility' becomes applicable within public administration. This principle means that actors who are normally responsible for an activity, such as a government agency or municipality, are also responsible in a crisis situation. However, in special cases, such as the large-scale cybersecurity incidents and crises mentioned in the NIS 2 Directive, one or multiple cyber crisis management authorities shall be responsible for national incident management efforts. This applies in cases such as large-scale or cross-border incidents.

Systematic, risk-based cybersecurity work in all civil society organisations, together with protective security and cyber defence, compose Sweden's national resilience in the area of cybersecurity. In this strategy, 'organisations' is used as an umbrella term for everything from government agencies and state-owned enterprises to municipalities, regions and private and municipal companies. 'Systematic cybersecurity efforts' refers to protective measures that are systematically prioritised based on an assessment of what risks are most likely and have the greatest potential impact. 'Protective security' refers to protecting information and activities of importance to Sweden's security against espionage, sabotage, terrorist offences and certain other threats. Protective security also includes the protective measures implemented in the area of information and cybersecurity in order to maintain protective security. The Protective Security Act (2018:585) and the Protective Security Ordinance (2021:955) apply, inter alia, to actors undertaking security-sensitive activities[2]. Cyber defence is an integral part of military defence and contributes to Sweden's overall capability to counter an armed attack. Cyber operations are as much a part of warfare today as land, maritime, air and space operations. During peacetime, the cyber defence resources of the Swedish Armed Forces may be used to support society during crises and other serious events.

1 In 'The cybersecurity landscape' section, the Government identifies a number of different challenges, vulnerabilities and threats that make up the strategy's external context of.

2 Security-sensitive activities are activities that are of importance to Sweden's security or are covered by an international protective security commitment that is binding for Sweden.

Target group

The National Strategy for Cybersecurity and the accompanying action plan is intended to provide value for all of society and all types of organisations, for both their management bodies and for functions that work with cybersecurity. Nevertheless, the Strategy's primary target group comprises government agencies with specific responsibility for activities conducted within the framework of the NCSC, supervisory authorities within the collective cybersecurity regulatory framework and other organisations that are part of the preparedness and NIS 2 sectors.

National cybersecurity policy

Cybersecurity extends across numerous fields, policy areas and sectors. Cybersecurity issues thus demand cross-sectoral work based on various areas of expertise. This Strategy maps out the Government's long-term approach to systematic cybersecurity efforts and the Government's cybersecurity policy. The Government's efforts to strengthen and contribute to Sweden's cybersecurity are also reflected in the Total Defence bill 2025–2030 (Govt Bill 2024/25:34). The bill identifies information security and cybersecurity as important prerequisites for Sweden's total defence, including military cyber defence. The bill also emphasises the importance of the Swedish Armed Forces' ability to contribute to cybersecurity efforts during times of peace. Foreign and security policy aspects of cyber issues are primarily dealt with in the strategy Sweden in a digital world – a strategy for Sweden's foreign and security policy on cyber and digital issues (U2024:/16802). The latter strategy and the National Cybersecurity Strategy are mutually reinforcing, and have several points of intersection. National capability in areas such as situational awareness, attribution and incident response measures is an important part of foreign and security policy response to cyber threat actors. Coordination of foreign and security policy with measures at national level is a prerequisite for collective management of political attribution and contributes to enhanced awareness and resilience.

The Government's national security strategy (Govt Communication 2023/24:163) establishes the framework for efforts on national security. It describes the priorities and principles on which Sweden's security is based and is the starting point for the reflections in this Strategy. The National Security Strategy specifies that measures to make essential public services more resilient to serious disruptions during peacetime are a prioritised part of the work to strengthen civil defence. At the same time, the Government stresses in the national security strategy that Sweden's national security is of concern to the whole of society. Prioritising and managing security threats from authoritarian states such as China, Russia and Iran in cooperation with democratic countries is also an objective. In the national security strategy, the Government outlines its intent to strengthen the capability to identify, manage and counter hybrid threats and attacks, including cyberattacks.

Prime Minister Ulf Kristersson in the European Parliament during Sweden's Presidency of the Council of the EU.

Photo: Eric Vidal/EU

In 2023, the Government began developing the NCSC with the aim of it becoming the hub for Sweden's national cybersecurity efforts. In the same year, an Inquiry was appointed to review the NCSC's activities (Fö 2023:A). Based on the Inquiry's findings, the Government decided to place the NCSC within the National Defence Radio Establishment as of 1 November 2024 and that its director would be appointed by the Government. The Inquiry's other proposals are currently being examined by the Government Offices and will therefore not be addressed in further detail in this Strategy.

The NIS 2 Directive identifies measures for achieving a high general level of cybersecurity across the European Union. In 2023, the Government appointed an Inquiry whose remit included proposing the amendments to Swedish law as a result of the Directive; the Inquiry presented its interim report in March 2024 (SOU 2024:18). The division of responsibilities between the actors covered by the NIS 2 Directive will be defined in national regulation that incorporates the Directive into Swedish law. Annex 2 of this Strategy outlines the current status of the key actors that have specific roles and responsibilities for supervision, support and coordination of cybersecurity efforts.[1]

In addition to this Cybersecurity Strategy, the Government intends to produce a strategy in accordance with the Directive on the resilience of critical entities (CER Directive). [2] Cybersecurity is also linked to issues concerning digital transformation and digital infrastructure, which will be adressed further in the Government's forthcoming digitalisation strategy.

---

1 The Annex is based partly on the national regulation that incorporated the NIS Directive and will be updated after the divisions of responsibility for Swedish cybersecurity have been defined through implementation of the NIS 2 Directive.

2 The CER and NIS 2 Directives complement each other and include provisions requiring coherence in the implementation of both directives. For example, entities identified as 'critical' in accordance with the CER Directive must be considered 'essential' in accordance with the NIS 2 Directive. In addition, national strategies that contain strategic objectives aimed at achieving and maintaining a high level of cybersecurity (NIS 2) and a high degree of resilience (CER) must be adopted according to both directives.

International context for national cybersecurity

Sweden's cybersecurity as well as the regulatory framework within the field of cybersecurity are mostly governed at a national level, but they are increasingly affected by developments in the international context. For example, Sweden's cybersecurity policy is influenced by international regulatory frameworks, governing documents, policies and standards. In the legislative area, developments are driven primarily by EU cooperation. The European Commission has taken several initiatives on regulation and norms with respect to cybersecurity and digital issues. In particular, this includes the NIS 2 Directive. Moreover, the EU Cyber Resilience Act and Cybersecurity Act are both directly applicable in EU Member States. NATO is also increasingly focusing on strategic cybersecurity and technology issues and works extensively with cyber defence and strategic technologies. The civil-military link within cybersecurity issues underscores the importance of coordinated development efforts between NATO and the EU on cybersecurity and cyber defence.

There are additional international conventions and agreements that to a varying degree set out requirements and regulate cybersecurity for Sweden. Conversely, Sweden also places demands on partner countries. The applicability of international law in cyberspace has been confirmed in several reports adopted by the UN General Assembly[1]. Non-binding norms for responsible state behaviour in cyberspace have also been developed within the UN. Questions concerning how international law applies in various respects are the subject of ongoing discussions in UN contexts. In July 2022, Sweden published a national position paper on the application of international law in cyberspace, and in November 2024 the EU Member States agreed on a declaration on this issue.

Swedish flag raised at NATO headquarters in Brussels to mark Sweden's NATO membership.

Photo: NATO

1 For example, refer to resolution A/RES/76/19.

Shelter.

Photo: Niklas Forsström/Government Offices

The cybersecurity landscape

Sweden's cybersecurity is affected by various vulnerabilities that can originate and manifest themselves within several areas. These vulnerabilities can individually or collectively constitute strategic vulnerabilities in a digital society's cybersecurity landscape and risk harmfully impacting essential public services, and ultimately Sweden's security. Vulnerabilities are commonplace and may involve organisational, technological, infrastructural and human factors.

Like other countries, Sweden faces a dynamic and evolving threat landscape in which cyber threat actors continuously develop new methods and adopt new technologies. Both detecting sophisticated cyberattacks and definitively attributing attacks to a specific threat actor is complex, which contributes to cyberattacks often carrying a low risk of repercussions, countermeasures or personal consequences for threat actors.

The following section outlines several typical threat actors and vulnerabilities that affect Sweden's cybersecurity. Both vulnerabilities and antagonistic threats can cause serious consequences. When an incident occurs, it can also be difficult to directly determine whether the cause is external influence or some other malfunction. It should also be emphasised that it is often difficult to clearly delineate between state, criminal and other actors. There are multiple examples of organised criminal actors with close but clandestine links to antagonistic state actors.

- Threats from state actors
- Threats from cyberactivists
- Threats from cybercrime and criminal groups
- Deficiencies in cybersecurity efforts
- Complex regulation
- Skills shortages
- Inadequate incident management
- Insufficient information sharing between the private and public sectors
- Vulnerable supply chains, dependencies and products
- Challenges related to the development of digital infrastructure and services
- Challenges with the connectivity of devices and infrastructure
- Technological development

Threats from state actors

Cyberattacks carried out by state[1] or state-sponsored[2] actors against Swedish entities have increased in scope and can have serious consequences. State actors possess sophisticated offensive cyber capabilities that can be used for technology theft, intelligence gathering or operations that temporarily disrupt or destroy parts of systems or entire systems, often within critical infrastructure and essential societal functions. Cyberattacks can be conducted independently of, or in connection with, an armed conflict, complementing political, diplomatic, economic, military and other means employed by a threat actor. State actors also carry out malign information influence activities, often supported by cyberattacks, and exploit the free flow of information on the internet for antagonistic purposes. The broad spectrum of methods that actors use to influence Sweden can be categorised under the term hybrid threats. Through such threats, an adversary seeks to exploit all vulnerabilities in our society to achieve, among other things, their political objectives. Various forms of cyberattacks are often employed in these hybrid activities. Robust cybersecurity thus impedes threat actors from conducting hybrid activities against Sweden and Swedish interests.

Threats from cyber activists

Cyber activists use cyberattacks to further political or ideological objectives through measures such as exposing or manipulating data. Based on political or ideological motives, cyber activists may sympathise with, or act on behalf of, various state actors.

---

1 State actors are directly operated by intelligence and security services or their front companies, or through organisations and non-organised individuals acting as proxies.

2 State actors can also support criminal groups based in their own country or originating from countries that do little or nothing to prevent such criminal activity.

Dock cranes at Port of Gothenburg.

Photo: Sofia Sabel/Image Bank Sweden

Health care.

Photo: Melker Dahlstrand/Image Bank Sweden

Threats from cybercrime and criminal groups

The number of criminal groups engaged in cybercrime in the form of attacks on IT systems has steadily increased. An increasing share of crimes are being committed in digital environments or using digital tools. IT-dependent crime can constitute a threat to individuals, businesses and other organisations, as well as society as a whole. Particularly notable examples of this are ransomware attacks and data theft. These types of crime can bring major consequences for individuals and entail major costs for both private and public actors. Distributed denial of service (DDoS) attacks carried out by criminal groups also risk affecting essential digital public functions and undermining confidence in them. Criminal activities initiated by criminal groups on their own initiative and those that they carry out on behalf of other actors against payment both play a significant role in the cybercrime ecosystem.

Cybercrime takes place across borders and is carried out using tools such as generative AI and new communications services. Information required for criminal investigations is often found in other countries, which limit law enforcement authorities' ability to prosecute.

Deficiencies in cybersecurity efforts

Many organisations have shortcomings in their preventive systematic cybersecurity efforts, which leads to an inability to implement fundamental security measures. This is a strategic vulnerability. Small municipalities and actors such as small and medium-sized enterprises may lack satisfactory cybersecurity efforts due to inadequate resources or skills. Moreover, the level of knowledge concerning which assets require protection within an organisation is often low, and many entities face challenges in identifying which parts of their operations that are security-sensitive, essential public services, or both, particularly from an availability perspective. This makes it difficult to make informed decisions on information management in general and dimensioning of security measures in particular.

Organisations lacking adequate preventive cybersecurity efforts often also have shortcomings in analysing the requirements their IT systems need to fulfil based on operational needs.

To effectively comply with legislative requirements and achieve the improvement that the legislator intended, organisations need to carry out a thorough operational analysis. This analysis may be complex and extensive, particularly for organisations that are responsible for widely divergent operations and therefore must conform to various regulatory frameworks and requirements.

Complex regulation

Increased regulation in the area of cybersecurity places new demands on organisations' ability to manage cyber-related operational risks. Systematic efforts to address cybersecurity risks usually strengthens an organisation's operation and can even result in long-term savings. At the same time, burdensome regulation can also entail costs for private individuals, public actors and private companies alike. Various regulatory frameworks at both national and international level may include overlapping requirements that are difficult to navigate and create prioritisation challenges. This is especially the case for actors like small and medium-sized enterprises with limited resources. National cybersecurity efforts are also divided into various partially overlapping areas of responsibility, which means that different central government agencies are responsible for supervision, regulations and guidance according to various regulatory frameworks. This risks making it more difficult for private companies and other organisations to follow the rules.

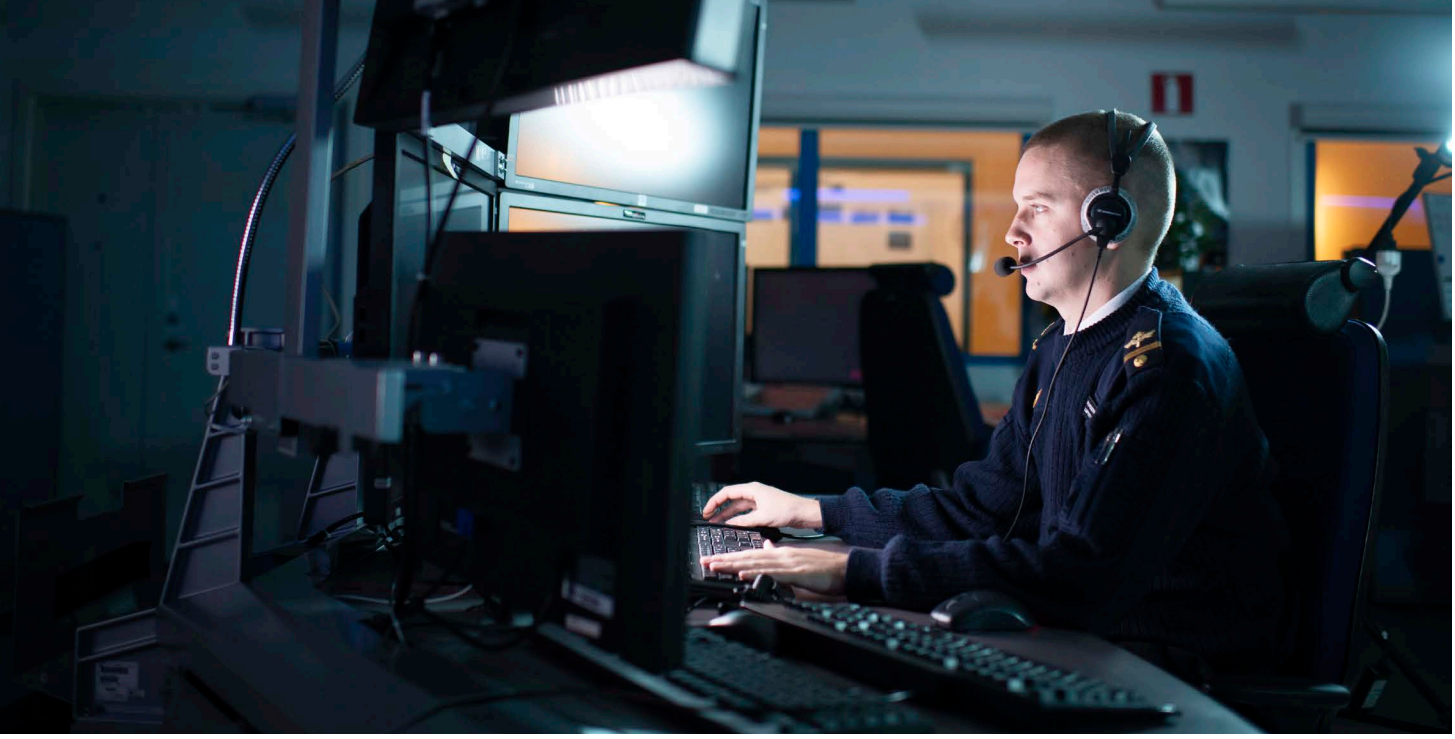
Skills shortages

Skills supply has long been a challenge in the area of cybersecurity. In addition to the lack of general cybersecurity skills, there is a lack of both cybersecurity experts and staff with relevant training and professional experience in related fields such as protective security and security within operational technology (OT security). This deficiency, which is global, affects the public and private sectors alike. In addition, general knowledge about cybersecurity is often limited among managers, lawyers, purchasers and IT developers, which are groups that do not often work with these issues. Technological developments and digital transformation contribute to a steadily increasing need for research, expertise and skills in cybersecurity. Shortcomings in general cybersecurity expertise within organisations can also result in clear requirements not being placed on the IT systems that are important for the operation. Moreover, increased and evolving regulatory frameworks for cybersecurity and protective security, and the resumption of Total Defence Planning entail new skills needs for both entities and supervisory authorities.

Swedish cybersecurity research is competitive, with leading research being conducted at several Swedish universities. While cybersecurity research is dominated by a few areas, research on other important cybersecurity issues is only conducted to a limited extent and often lacks an interdisciplinary perspective. Moreover, coordination within cybersecurity research in Sweden has often been lacking.

Curious children.

Photo: Emelie Asplund/Image Bank Sweden



Air combat commander.

Photo: Besav Mahmod/Swedish Armed Forces

Inadequate incident management

Suitable working methods for incident and continuity management are lacking in many organisations, and few conduct exercises in order to practice these capabilities. Inadequate incident management is a serious risk for organisations, particularly during times of increased cyber threats. Weak processes increase organisations' vulnerability when cybersecurity incidents occur. Deficient incident management can also increase risks of loss of sensitive information, loss of the capability to provide critical services, financial loss and undermined confidence in an entity.

Cybersecurity incidents covered by incident reporting requirements must also be shared with competent authorities, but underreporting, leading to hidden statistics, has long been a reality at national and international level. This affects the possibility of gaining an operational overview and warning other organisations, which risks exacerbating an existing crisis. It also reduces possibilities of drawing lessons and focusing on preventative work.

Hidden statistics in reported cyber offences also impair law enforcement agencies' preventive efforts, operational responses, and investigations regarding cybersecurity incidents. By extension, this affects the possibility of prosecuting those who carry out criminal offences. Nevertheless, there is no obligation to report a cyber offence to the police. This necessitates expedient information sharing between the government agencies that receive incident reports and law enforcement authorities in order to increase the possibility of following up offences and securing evidence.

Insufficient information sharing between the private and public sectors

Organisations are dependent on each other to prevent, identify, and manage vulnerabilities, threats and cybersecurity incidents. Private and public organisations have access to different information flows. For example, expert and supervisory authorities receive incident and vulnerability reports,

whereas private organisations possess the majority of society's cyber resources and are thus central to national cybersecurity capability. Information sharing and cooperation between and within the private and public sectors require established channels of communication and appropriate processes, as well as trust between actors. These processes need to be based on and account for private actors' commercial interests and secrecy for business and operational circumstances. Underdeveloped and inadequate cooperation between the private and public sectors, at national and international level, is a vulnerability.

Vulnerable supply chains, dependencies and products

Incidents in digital supply chains, such as supplier system failures , can have consequences beyond the organisation that was initially affected and can cause disruption to essential public functions. Today's complex interdependencies also make it difficult to map out vulnerabilities in digital supply chains and complicate accountability.

Poor supplier cybersecurity practices risks affecting the security of customer organisations. As many organisations are dependent on externally supplied IT operating services, organisations that fail to account for this fact in their risk analyses become vulnerable if a supplier fails to deliver their service. In such cases, organisations run the risk of lacking alternative solutions. This can entail serious risks if many organisations are dependent on the same service or system.[1] Such oligopolistic or monopolistic market structures also reduce customer flexibility and options, such as the possibility of using alternative services during ongoing incidents. Dependencies of digital product and service deliveries from organisations based in third countries may be both inappropriate and constitute a vulnerability that can be exploited as a means of political coercion.

Unsecure digital products with low cybersecurity pose a risk for both national and international supply chains. Uncertainty and risks also emerge frequently with hardware and software updates. Remedying this has been identified as a necessity at EU level, and is a focus of the Cyber Resilience Act, which aims to increase producer and supplier responsibility for cybersecurity and to place products with digital elements on the single market with fewer vulnerabilities.[2] Development and widespread application of international security standards in the area of technology and cybersecurity can also contribute to more robust supply chains. However, geopolitical competition is increasingly influencing the development of international standards.

---

1 Unknown deficiencies at suppliers that provide IT support to many organisations and/or inadequate requirements placed on such risk leading to major disruptions in both the private and public sectors in Sweden. The consequence of license fees being increased, or services discontinued, also runs the risk of having a major impact.

2 The single market's vulnerability to poor cybersecurity is also a focus of the certification framework established under the Cybersecurity Act. The possibility of demonstrating that cybersecurity requirements have been met through certification is regulated in various bodies of EU legislation, including the NIS 2 Directive, the Cyber Resilience Act, the Artificial Intelligence Act, and the revised eIDAS Regulation.

Challenges related to the development of digital infrastructure and services

Sweden's digital infrastructure is developing continuously. New generations of mobile networks are being rolled out, and space is turning out to be an additional infrastructure domain for mobile data communication. The need for trusted and secure digital infrastructure and services is gaining in importance and scope. This creates many new opportunities, but also places major demands on both procurement capability and well-developed management of vulnerabilities and dependencies for both private and public alternatives.

Challenges with the connectivity of devices and infrastructure

Processes within critical infrastructure[1] that were previously manual or mechanical have become increasingly digitalised. This trend has been enhanced by the growth of new so called IoT devices, which are permanently connected and can be used for purposes such as process controlling and monitoring. The systems used within critical infrastructure have technical conditions that differentiate them from traditional IT systems and make protecting them complicated. OT security efforts are thus a challenge, particularly in light of the scarcity of expertise in this area.

IoT devices with poor security can pose significant cybersecurity risks and can trigger cybersecurity incidents if they are connected to other IT infrastructure within organisations. IoT consumer products with poor security can also pose risks to private individuals. Such products can be used in bot networks and exploited by threat actors for DDoS attacks against other organisations.

Technological development

The development of technologies of strategic importance creates opportunities for Sweden. Technological development can affect society's security. For example, AI functions can be used to make cybersecurity more effective. At the same time, AI can be used to carry out cyberattacks and disinformation campaigns with wider dissemination. Cybersecurity incidents in AI systems also bring greater consequences as society's dependence on such systems increases.

Development of quantum technology and powerful quantum computers make certain cryptographic algorithms all the more vulnerable to cryptanalysis. Through measures such as cyberattacks, interception and other intelligence gathering, qualified threat actors can gain access to encrypted data that they store with the aim of decrypting it when future quantum technology has been developed.

1 Critical infrastructure comprises services and their provision within, inter alia, the financial, transport, energy and electronic communications sectors. It can also include IT infrastructure that is used widely within central government and municipal administration. However, this list should by no means be considered exhaustive or as a legal definition. Critical infrastructure comprises a vast array of activities, many of which are covered by the Protective Security Act, the NIS 2 Directive, or other sector-specific EU legislation containing equivalent cybersecurity requirements, such as the Digital Operational Resilience Act.

Max IV Laboratory in Lund.

Photo: Per Pixel Petersson/Image Bank Sweden

The government's approach

The National Cybersecurity Strategy is based on three pillars that set out the direction of Sweden's cybersecurity efforts.

The pillars comprise several targets with accompanying key performance indicators. The targets focus on several key areas to drive change and address the threats and vulnerabilities described in the Cybersecurity landscape section of this document. The targets extend to and include 2029. There is an introduction to respective targets that describes each target and its context. Subsequently, Desired state 2030 presents the Government's vision of Sweden's position, and of the necessary changes occurred, within respective targets at the end of the Strategy period. Given the long-term efforts to develop the NCSC, in which it will serve as the hub for national cybersecurity efforts, the Government envisions a crucial role for the NCSC in several of the target areas and their follow-up.

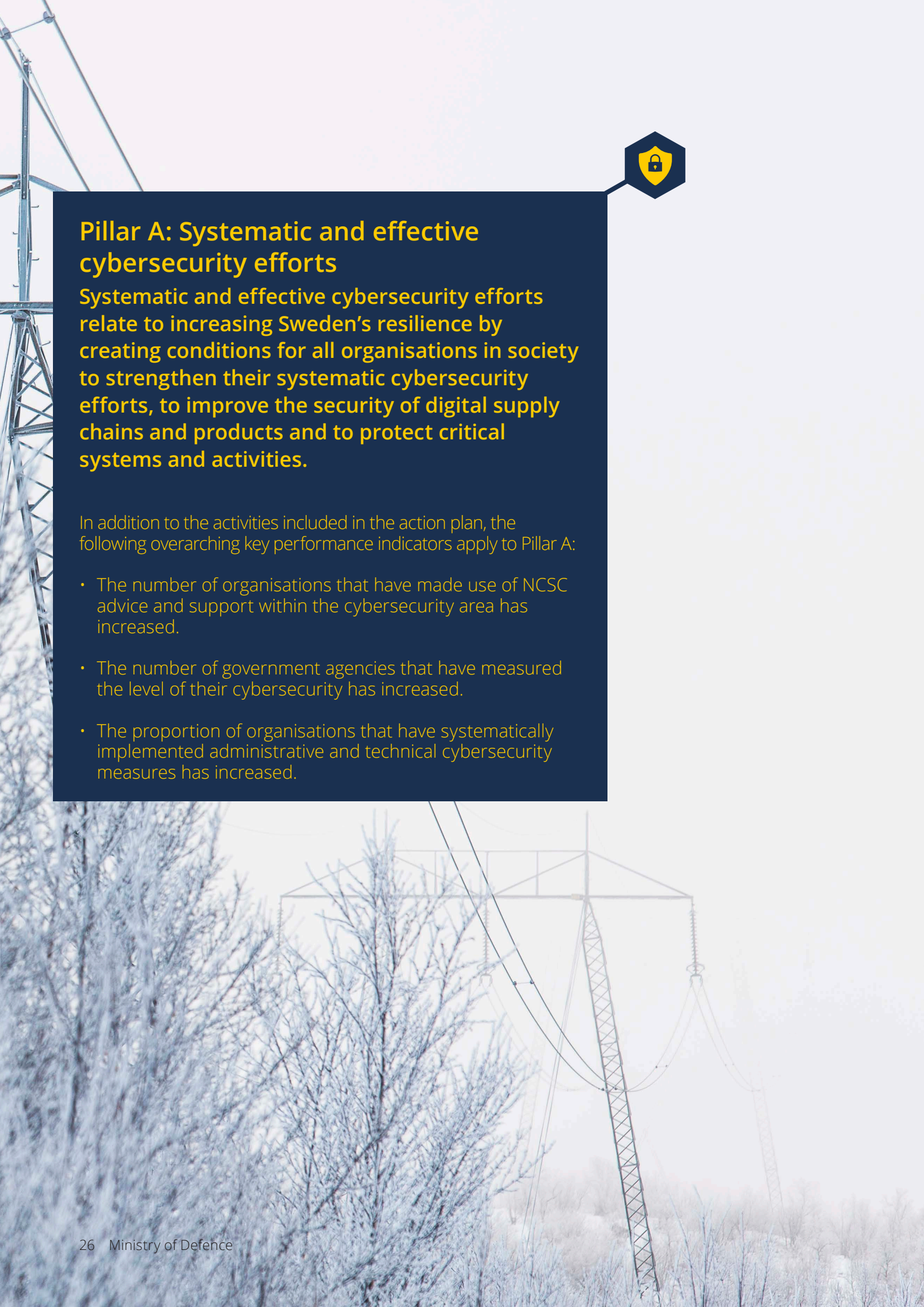
The Strategy's pillars and targets are accompanied by an action plan (Annex 1[1]), which includes a number of activities that align with the Government's approach and the requirements in the NIS 2 Directive. The action plan will be regularly updated, and activities assigned to incrementally achieve target fulfilment.

1 Only available in Swedish.

Pillar A: Systematic and effective cybersecurity efforts

Pillar B: Advanced knowledge and skills development in cybersecurity

Pillar C: Capability to prevent and manage cybersecurity incidents



Pillar A: Systematic and effective cybersecurity efforts

Systematic and effective cybersecurity efforts relate to increasing Sweden's resilience by creating conditions for all organisations in society to strengthen their systematic cybersecurity efforts, to improve the security of digital supply chains and products and to protect critical systems and activities.

In addition to the activities included in the action plan, the following overarching key performance indicators apply to Pillar A:

- The number of organisations that have made use of NCSC advice and support within the cybersecurity area has increased.
- The number of government agencies that have measured the level of their cybersecurity has increased.
- The proportion of organisations that have systematically implemented administrative and technical cybersecurity measures has increased.

Target 1: Increased cybersecurity efforts among private and public organisations

A robust society needs effective IT systems, with comprehensive cybersecurity efforts creating the necessary conditions to address peacetime crises and ultimately war. In a digitalised society, therefore, all organisations need to make appropriate, systematic security efforts, including the implementation of cybersecurity measures. Management bodies have ultimate responsibility for their respective organisations' operations and thus their cybersecurity. The NIS 2 Directive requires that management bodies approve cybersecurity risk management measures, monitor their implementation and follow training. This constitutes a firm foundation for cybersecurity efforts, but these must in turn be based on a fundamental understanding of how organisations' operations can be impacted by cyber incidents.

Desired state 2030

Organisations that provide essential public services conduct detailed operational analyses to identify which cybersecurity capacities are necessary to guarantee the provision of their services. Through active participation in EU cooperation on NIS 2 requirements, relevant government agencies have produced guidance and support adapted to national needs. Together with applicable standards, relevant government agency guidance helps organisations to adapt to NIS 2 requirements and thereby implement proportionate security measures. NIS 2 requirements also influence organisations that are not subject to the Directive, especially those with vital societal functions and who are already covered by regulations that set out extensive requirements but lack an all-hazards approach. Sector-specific cybersecurity legislation, such as the Digital Operational Resilience Act (DORA), are applied and extend resilience requirements to include additional actors. Basic cyber hygiene is an integral component of all essential public services and an increased level of cybersecurity maturity in all essential public service sectors is achieved. Public actors and companies, irrespective of size, actively work with business continuity planning as a core aspect of their preparedness.

All organisations take responsibility for and protect their information and the network and information systems used for their activities or to provide services have the necessary conditions to do so. Access to information, functions and capacities is also maintained. Protection is scaled according to the security needs of both the activity and the information, as well as regulatory requirements, and is backed by well-developed support and guidance from government agencies tasked with providing such support. Organisations have plans in place for operations that must be maintained in the event of disruption or incidents. Public-private cooperation has developed in several sectors and reflects private actors' increasingly central role in national security. Relevant government agencies offer training to management bodies of essential public services and contingency planning organisations.

A common and dimensioned level of national cybersecurity based on regulatory requirements, established security levels and products and technical solutions based on nationally specified requirements has been implemented for strategically important operations in the public and private sectors.

Power lines in winter frost

Photo: Tomas Arlemo/Svenska kraftnät

Target 2: Strengthened cybersecurity in central and local government administrations' information management

The ability of the public sector to ensure a high level of cybersecurity is crucial to maintaining strong confidence in public institutions. At the same time, organisational conditions and resources available to government agencies, municipalities, and regions to conduct adequate cybersecurity efforts differ. Russia's full-scale invasion of Ukraine has also raised the question of the central government's ability to maintain essential services and critical infrastructure, as well as protecting important basic data at times of crisis and ultimately war.

Desired state 2030

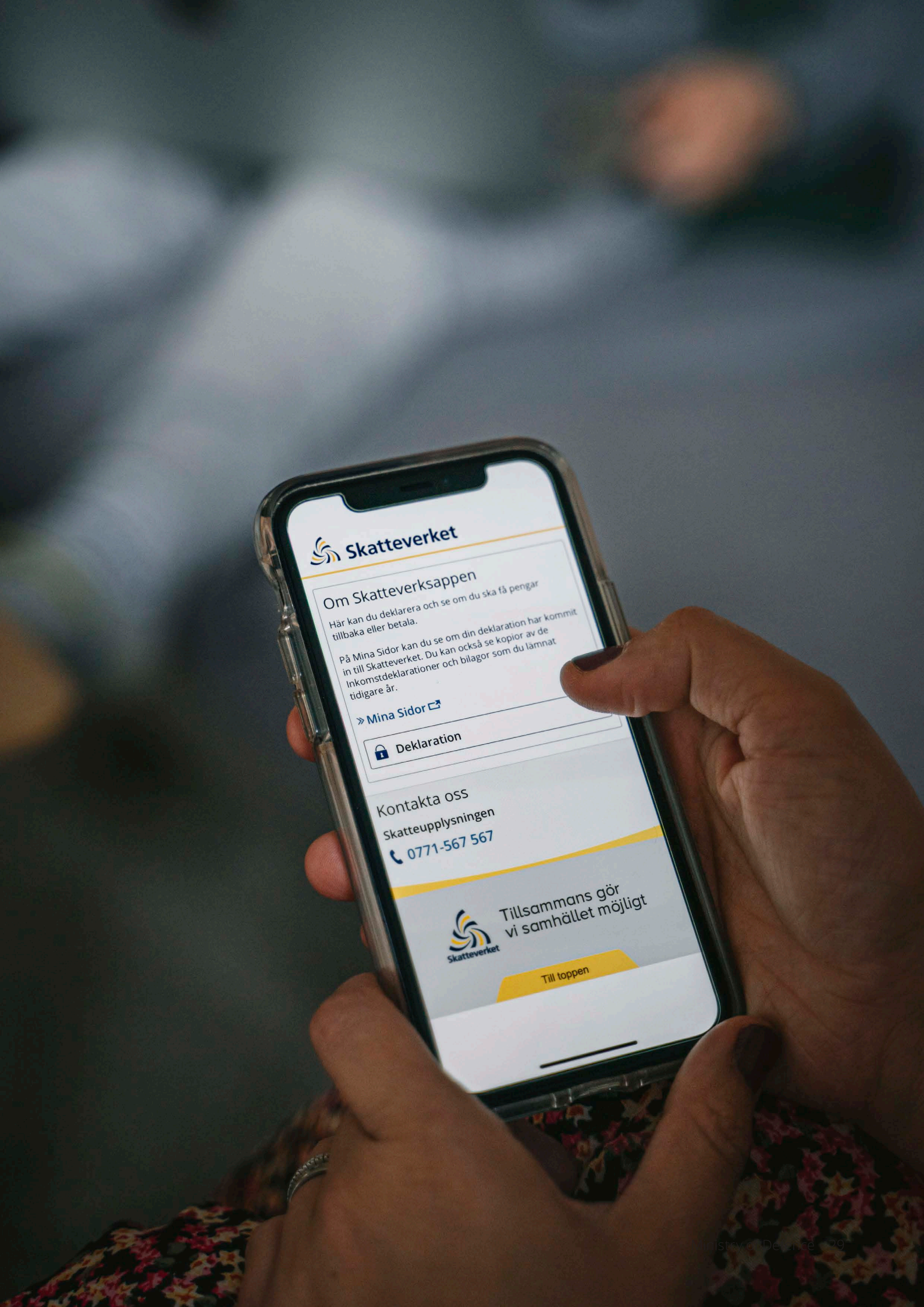
Relevant government agencies' tools for measuring organisations' level of cybersecurity are improving and achieving greater impact through supporting other organisations in mapping internal cybersecurity efforts. Related advice on which steps organisations should take, based on the results of measurements of their cybersecurity levels, has been further developed and has achieved greater impact. Requirements in national regulations implementing the NIS 2 Directive in Swedish law have established a firm foundation on which to improve cybersecurity in public administration, which is also apparent in the cybersecurity capability of actors in national assessments of civil preparedness. Consistent security requirements and security levels in the public sector promote cybersecurity across all actors and a common level of robust cybersecurity.

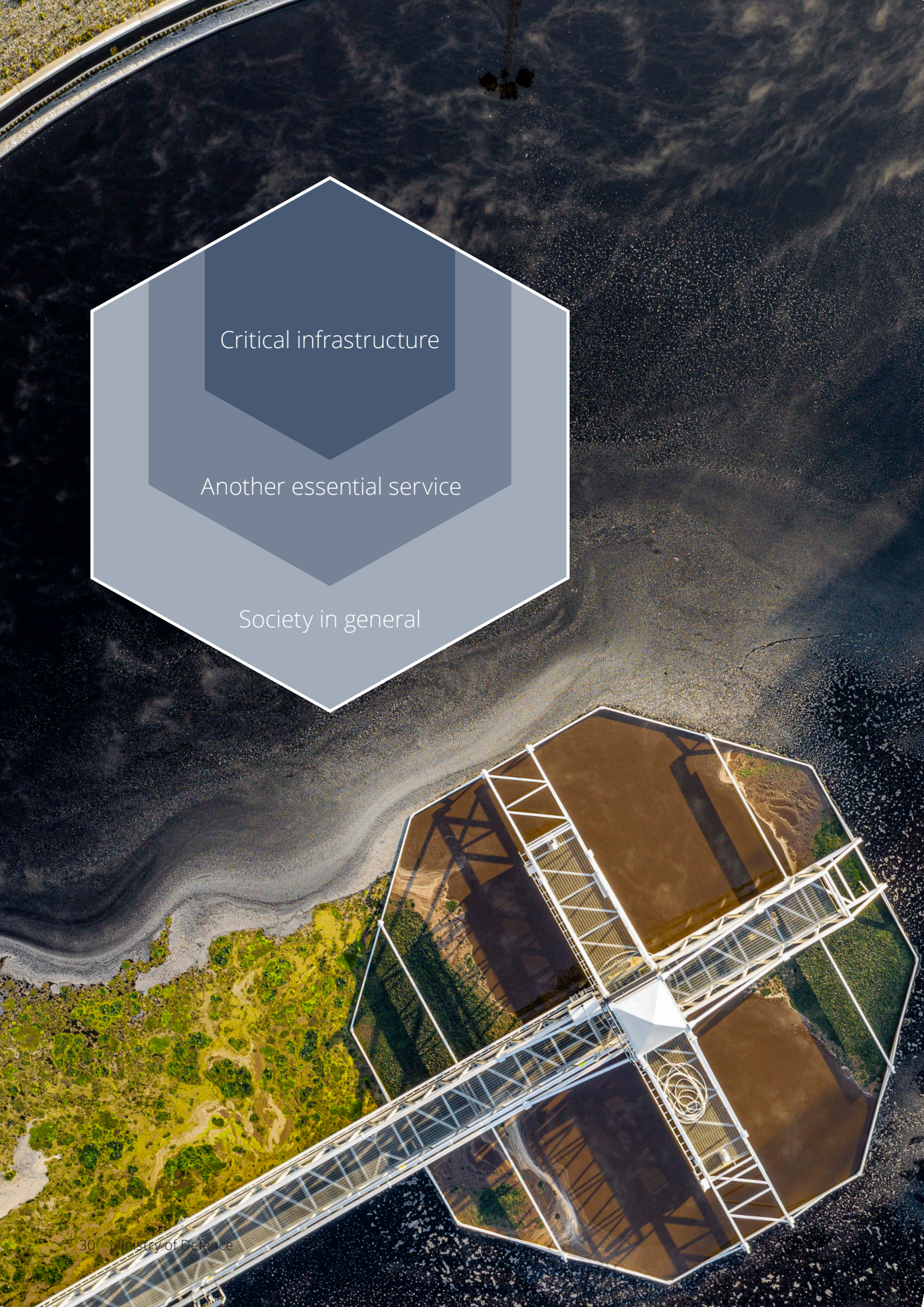
Government agencies provide coordinated, secure and, as far as is possible, cost-efficient alternatives for shared digital infrastructure and services. This has helped actors lacking in cybersecurity capabilities and contributed to ensuring societal functions can be safeguarded throughout the entire conflict spectrum. Framework agreements are in place with cybersecurity requirements that protect confidentiality, integrity and availability. Procurement with appropriate criteria results in contracts that include robust security requirements that lead to effective services, secure information management and innovation in the field of security. On the whole, this strengthens society's confidence that the right information is always available to the right party.

Government agencies' national initiatives relating to technical support are cost-efficient and meet the needs of target groups. More collective technical security solutions are offered centrally. They support cybersecurity particularly among small organisations in government agency sectors and in municipalities and regions where information that is relevant to essential public services and socio-economically important activities is found. Municipalities and regions have identified and implemented several effective common methods to increase their collective cybersecurity.

Digital essential services.

Photo: Liselotte van der Meijs/Image Bank Sweden


Skatteverket
Om Skatteverksappen
Här kan du deklarera och se om du ska få pengar tillbaka eller betala.
På Mina Sidor kan du se om din deklaration har kommit in till Skatteverket. Du kan också se kopior av de inkomstdeklarationer och bilagor som du lämnat tidigare år.
» Mina Sidor
Deklaration
Kontakta oss
Skatteupplysningen
0771-567 567
Skatteverket
Tillsammans gör vi samhället möjligt
Till toppen


Critical infrastructure
Another essential service
Society in general

Target 3: Strengthened cybersecurity efforts in critical infrastructure

Safeguarding critical infrastructure is necessary for the security and stability of society. Many of the services and functions that constitute critical infrastructure are provided by private organisations. Therefore, cybersecurity efforts of critical infrastructure operators need, among other things, to be based on organisations' individual operational circumstances as well as their particular vulnerabilities and the specific threats directed towards the organisation in question. Society's dependence on these organisations makes their cybersecurity efforts vital. Enhanced cybersecurity efforts also make it harder for threat actors to direct cyberattacks against critical infrastructure as part of hybrid activities intended to affect Sweden.

Desired state 2030

Operators' protection of critical infrastructure, including security efforts within OT, are dimensioned with respect to their importance to society and the antagonistic threats they face. Security monitoring of IT and OT systems within critical infrastructure is stimulated. Government agencies with responsibility for sectors under the NIS 2 Directive and other relevant government agencies utilise NCSC's advice and support within cybersecurity to adapt guidance and other policy documents for respective sectors. Operators' efforts to implement security measures are thereby strengthened, which, together with their management of vulnerabilities, results in improved resilience. Government agencies develop support for protection of critical infrastructure. NIS 2 entities and organisations with specific responsibilities for civil preparedness benefit from the support and training offered within security for critical infrastructure. Cooperation and information sharing between government agencies and critical systems operators have developed and contribute to linking sectors together, given that sectors often have clear overlaps and mutual dependencies. Exercise and test activities, enabled through, for example, cyber range environments, continue to be developed and extensively utilised. Sector-specific cooperation forums continue to play a key role in terms of collaboration, training and information sharing, and greater cooperation takes place between government agencies and the private sector.

Waste water treatment plant.

Photo: Per Pixel Petersson/Image Bank Sweden

Target 4: More robust digital supply chains and reduced dependency

Managing digital supply chains, cloud services, and dependencies is a top priority for the Government's cybersecurity efforts. To strengthen Sweden's cybersecurity, mono-dependencies and critical third-country dependencies need to be identified and addressed, and supply chains need to become more robust.

Desired state 2030

Sweden has high ambitions for national and international efforts related to digital supply chain security, especially at EU level. Government agencies provide private and public organisations with guidance in terms of reviewing supply chains and outsourcing. Organisations review and evaluate the security of their supply chains and set out appropriate cybersecurity requirements in supplier contracts. Even organisations that are not subject to the NIS 2 Directive evaluate dependencies and risks in their supply chains and ensure that they have the necessary contingency plans in place.

The Cyber Resilience Act's provisions on cybersecurity in products that include digital elements result in increased security in supply chains. Swedish companies that adhere to secure development practices for software and firmware as well as security by design are more competitive and contribute to providing the market with products with fewer security vulnerabilities. Demand for secure products has increased among organisations in Sweden, driven by stricter and improved requirements from the public sector in terms of the function of services and products. Sweden maintains continued influence through international standardisation and contributes to well-adapted international standards that promote secure supply chains. Relevant government agencies, in cooperation with the private sector, strive to ensure that new standards and European cybersecurity certification schemes are developed transparently and that Sweden's needs and priorities have impact. Organisations utilise cybersecurity-certified IT services and products based on their own risk assessments.

Ambulance staff.

Photo: Helena Wahlman/Image Bank Sweden

Target 5: Simplified regulatory compliance and enhanced functional supervision

The regulatory framework in the cybersecurity field will continuously expand. Due to growing system integration, in which rising numbers of actors become mutually dependent, additional regulation and stricter cybersecurity requirements for increasing numbers of actors can be expected. To increase society's cybersecurity, it is therefore important to simplify organisations' application of complex rules as much as possible, and to strengthen and coordinate the activities of supervisory authorities. Simplified regulatory compliance can also strengthen companies' competitiveness.

Desired state 2030

With the support of implemented national measures, Sweden is a leading Member State in the development of new international regulatory frameworks within cybersecurity that incorporate proportionate and harmonised rules. Government agencies' active participation in the exchange of experience at EU level contributes to harmonised NIS 2 requirements among Member States. NIS 2 requirements have been included in harmonised regulatory frameworks between sectors and have created conditions for effective regulatory compliance. Government agencies are well-coordinated in terms of existing regulations with the aim of ensuring that regulations, general advice and guidance are harmonised and follow a consistent logic, structure and terminology to the furthest extent possible. NCSC's advice and support on cybersecurity issues complement sectoral agencies' work on provisions. Continuous and improved supervisory activities strengthen cybersecurity regulatory compliance. Government agencies with central roles have the appropriate powers and mandate.

Target 6: Strengthened support for small and medium-sized enterprises' cybersecurity efforts

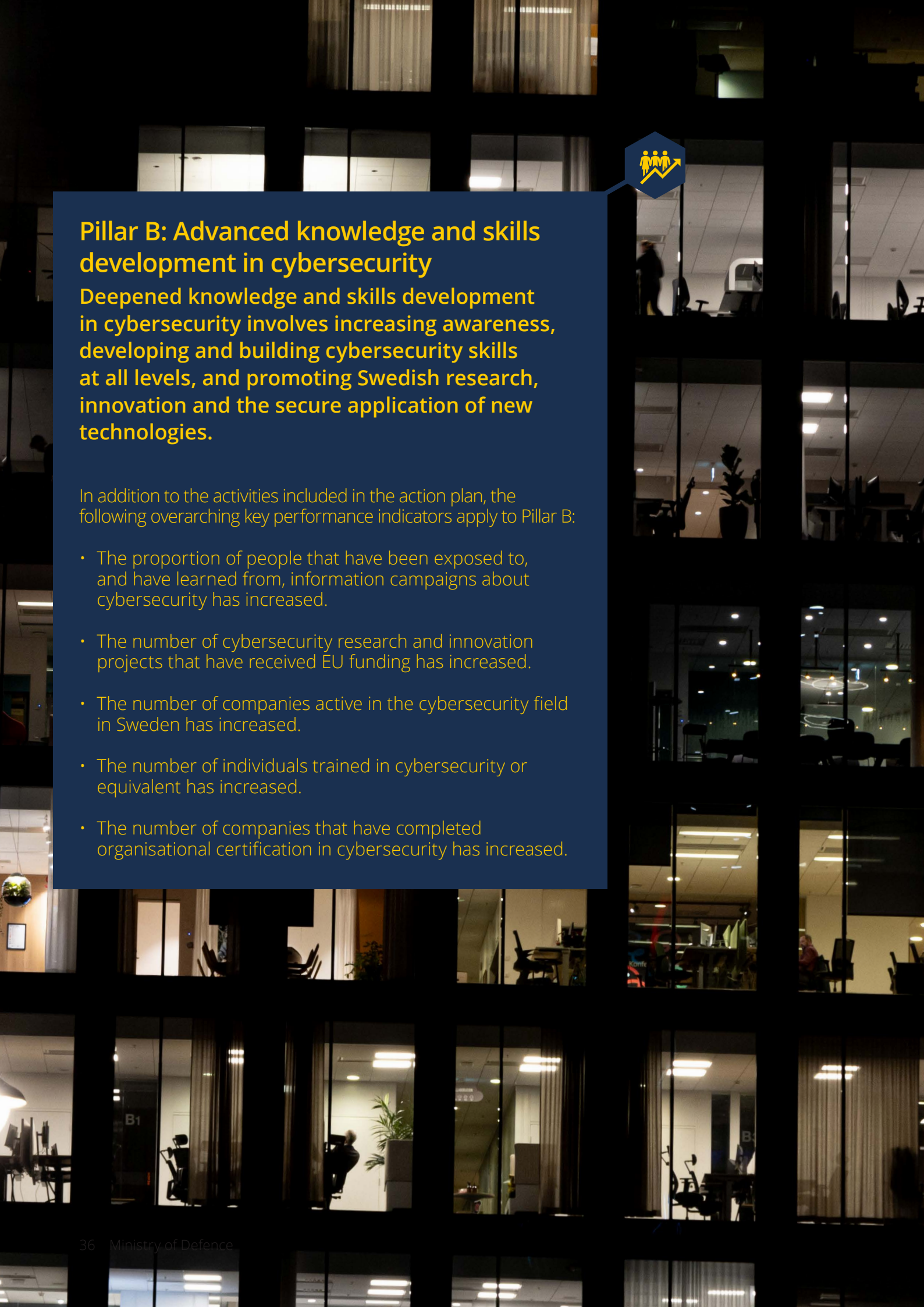
The private sector accounts for considerable economic value through innovation, production and essential public services. The majority of Swedish companies are small and medium-sized enterprises and constitute a substantial proportion of this economic value; they are also generally more vulnerable to cybersecurity risks than larger companies. When such companies experience cybersecurity incidents, substantial productivity losses, disruption to essential services and economic impacts can occur. Certain small and medium-sized enterprises maintain apt cybersecurity practices, and a significant segment of such companies is active in the cybersecurity field, but factors such as limited cybersecurity awareness and scarce resources make the majority of these companies vulnerable. They also run greater risk of being unable to recover from serious cybersecurity incidents. Small and medium-sized enterprises' resilience and protection of commercial secrets are therefore a vital part of safeguarding Sweden's overall competitiveness and resilience.

Desired state 2030

Government agencies offer extensive support and guidance that help small and medium-sized enterprises, including those that are not subject to Swedish regulations implementing the NIS 2 Directive into Swedish law. Government agencies' cooperation with industry and stakeholder organisations is stimulated and utilised to counteract digital crime and increase cybersecurity. Tech companies take responsibility for offering secure services, which indirectly strengthens small and medium-sized enterprises' cybersecurity through more secure IT services. Small and medium-sized enterprises make use of support offered by organisations such as regional chambers of commerce and industry and stakeholder organisations. In addition, these actors review opportunities to utilise common technical security solutions that reduce small and medium-sized enterprises' need to manage key areas to make their operations cyber-secure with their own resources and competencies. To strengthen their cybersecurity capacity, small and medium-sized enterprises utilise the opportunity to apply for funding from the European Cybersecurity Competence Centre via the National Cybersecurity Coordination Centre (NCC-SE).

Lindholmen Science Park.

Photo: Lindholmen Science Park



Pillar B: Advanced knowledge and skills development in cybersecurity

Deepened knowledge and skills development in cybersecurity involves increasing awareness, developing and building cybersecurity skills at all levels, and promoting Swedish research, innovation and the secure application of new technologies.

In addition to the activities included in the action plan, the following overarching key performance indicators apply to Pillar B:

- The proportion of people that have been exposed to, and have learned from, information campaigns about cybersecurity has increased.
- The number of cybersecurity research and innovation projects that have received EU funding has increased.
- The number of companies active in the cybersecurity field in Sweden has increased.
- The number of individuals trained in cybersecurity or equivalent has increased.
- The number of companies that have completed organisational certification in cybersecurity has increased.

Target 7: Increased cybersecurity awareness and cyber hygiene in society

An increasing exposure to digital threats and risks necessitates good cyber hygiene and a cognisant security culture throughout society. Cyber hygiene refers to basic measures to protect oneself and others online. Safer internet usage by individuals contributes to strengthening Sweden's cybersecurity by reducing vulnerability to fraud and cyberattacks. Achieving behavioural change among the public requires continuous efforts from various private, public and non-profit organisations.

Desired state 2030

Citizens are well-informed about the importance of good cyber hygiene and are better equipped to manage and address cybersecurity risks. Measures are taken to provide individuals with better opportunities to achieve good cyber hygiene based on their circumstances and needs. Employers also ensure that processes and routines promote secure practices and cybersecurity awareness. Government agencies regularly produce information and training campaigns with the aim of raising awareness and promote behavioural changes in society. Government agencies, non-profit organisations and companies collaborate on cybersecurity information and training initiatives for the public. These initiatives take into account differences in exposure to cybersecurity risks and differences in the basic conditions for good cyber hygiene. Efforts to increase cybersecurity awareness go hand in hand with efforts to combat hybrid activities, such as support for media and information literacy, countering disinformation campaigns and Sweden's participation in international efforts to strengthen norms and regulations to protect the free flow of digital information. Exposing and holding accountable state cyberthreat actors, including in foreign and security policy, also contribute to cybersecurity awareness.

Offices.

Photo: Niklas Forsström/Government Offices

Target 8: Strengthened skills supply, education and continuous training in cybersecurity

Cybersecurity skills are becoming increasingly important, and demand has long exceeded supply. The education system plays a central role in meeting society's needs by providing basic knowledge in the subject, sparking and stimulating interest, and ultimately improving the cybersecurity skills supply. In addition, cybersecurity skills among employers and employees need to be strengthened to meet current and future cybersecurity needs. Existing skill sets must be developed and new labour attracted.

Desired state 2030

More applicable knowledge of cybersecurity is integrated into the curriculum in primary schools, adapted primary schools, special schools and Sami schools. Students in upper secondary schools, adapted upper secondary schools and municipal adult education are given the opportunity to understand the importance of societal cybersecurity and acquire practical cybersecurity skills. Private and public organisations continue to contribute with interactive training packages and modules that can be used for education and continuing professional development in cybersecurity. Colleges, universities and vocational schools consider whether and how cybersecurity should be incorporated into their curricula. Cybersecurity thus becomes increasingly integrated across all subject areas.

Basic curriculum in areas that lay the groundwork for cybersecurity, such as mathematics, computer science and cryptology, remain popular. Interactive games and competitions aimed at young people to stimulate and spark interest in practical cybersecurity are widely available.

Cybercampus Sweden serves as a hub for cybersecurity education and contributes to enhanced skills provision of cybersecurity experts in the public and private sectors. Organisations such as educational institutions, other government agencies and vocational education providers have signed declarations of intent to join Cybercampus within the scope of its operations.

Government agencies continue to work to spark interest in cybersecurity careers. Relevant government agencies, municipalities and regions, as well as other organisations, engage in active industry collaboration on skills provision in the cybersecurity area and disseminate knowledge regarding employers' current and future skills needs. New target groups are being considered to a greater extent for roles in which the lack of previous experience or education in the field can be compensated for through intensive and internal training. Lifelong learning and career changes are encouraged, with support such as transition study grants or similar. Employers provide good quality, continuous training for employees working in cybersecurity, as well as skills development for other staff, managers and leadership regarding cybersecurity. Government agencies and private organisations offer trainee programmes in cybersecurity through public-private partnerships. In addition, organisations are inspired by and evaluate how successful initiatives in other countries related to knowledge and experience exchanges can be adapted to a Swedish context.

University education

Photo: Magnus Liam Karlsson/Image Bank Sweden


VGGOPAENQXFDFWNY
BZMMRTXHJFVAEKEA
MVOALPXWARRBZYPU
HDNELNWEFSSJOEDI
SIAWQGECXMMKDAFA
GADWYBACKASXWOMA
NRBFZBIAGELMVDCC
RHJJBZKAAGHRCEPN
BECEERYMEGQLMFQL
LTYVBCKLACRIESDR
IOHEHAPJLWKVOHDA
TJWHILEKECHFLBMZ
CURWAMANFUIMCLJX
FDUEMBLDDJRAWNTR
HVAFAJYRMFBSUTEK
FANTOMENFBRCOBTM
TASITEVTMQKDAKTA
HJBAJENTNTHHVYRP
YYTTRAQLAGARYIPC
TBMOYRCIFTMTBGRY
OXWBVCGDDHFENDTM
BHREANNMARKANVKA
ZVARPQRBVGGMYTRA

Target 9: Strengthened research and innovation in the cybersecurity field

Sweden is home to many world-leading tech companies, including an expansive cybersecurity industry comprising many innovative small and medium-sized enterprises that develop and offer competitive cybersecurity solutions. The tradition of close collaboration between central government, educational institutions and industry also exists within cybersecurity. Cybersecurity research is conducted at several universities and colleges, which are funded by both central government and private research financiers. Sweden has well-established research groups in certain areas of cybersecurity, but the field is fragmented. A key factor is ensuring that organisations and companies have favourable conditions for innovation, research, and investment within the cybersecurity field in Sweden. Opportunities and funding from sources such as EU programmes and funds need to be better utilised.

Desired state 2030

Sweden's research- and technology-intensive cybersecurity sector remains at the forefront and compete on a global market. The Government's substantial investment in research and innovation for emerging, disruptive and strategic technologies set out in Government Bill 2024/25:60, Research and innovation for the future, curiosity and benefit, has also created favourable conditions for enhanced cybersecurity research.

Initiatives such as Cybercampus Sweden have enhanced research and innovation in cybersecurity, contributing to a secure, digitalised and resilient Sweden. Development of entities such as Cybercampus, Cybernode and the NCC-SE continues through effective cooperation with and between educational institutions and the private sector. This contributes to greater coordination of cybersecurity research and innovation, as well as favourable conditions for entrepreneurship in the field. Research and innovation in the cyber field also have an interdisciplinary approach, thereby benefiting the whole of society as technical expertise becomes increasingly interlinked with other fields. Research results in the field lead to greater innovation and commercialisation. Government agencies actively contribute to the development and commercialisation of cybersecurity innovation through measures such as innovation-driven procurement and by supporting organisations in accessing cybersecurity funding opportunities within the EU. There is a sufficiently high level of national co-financing to ensure Swedish actors' active and long-term participation in funds and programmes in fields such as cybersecurity. Sweden influences the content of work programmes at an early stage ahead of upcoming calls for expressions of interest. International cooperation on cybersecurity research and innovation has increased within the EU and NATO as well as bilaterally with like-minded countries.

Target 10: Enhanced capability to manage the risks and opportunities of emerging technologies

Advances in emerging, disruptive and strategically important technologies are rapid. AI and quantum technology are examples of areas where significant advances have been made with relevance to cybersecurity. Greater capability to manage emerging technologies improves national security and competitiveness. To address the risks and opportunities of emerging technologies, relevant organisations need to prioritise these efforts, and high-quality innovation and research in technological areas are crucial.

Advances in quantum technology, especially quantum computing, affect cryptographic technologies, which is an essential security interest and an area in which Sweden has traditionally been at the forefront. Organisations have the necessary conditions to protect classified information through access to approved cryptographic systems that are already quantum-safe, but additional steps are needed to maintain and develop the ability to make information that is not classified safe against quantum threats.

Technological advances in general, and perhaps especially in AI, are beneficial in many respects. However, they also place additional demands in terms of cybersecurity efforts and continuous development of regulatory frameworks to address opportunities and challenges. The development and implementation of secure and ethical AI systems is becoming increasingly important.

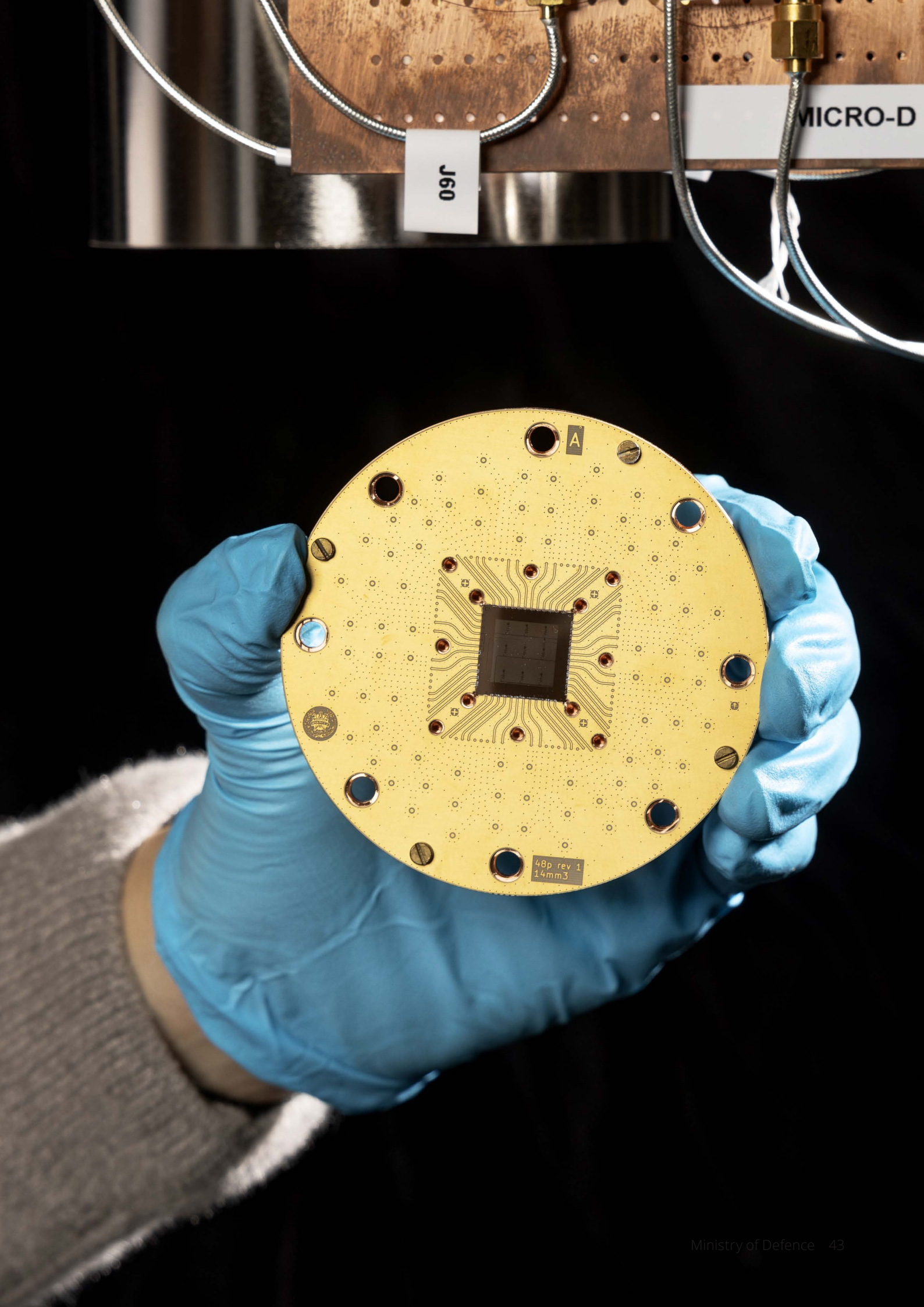
Desired state 2030

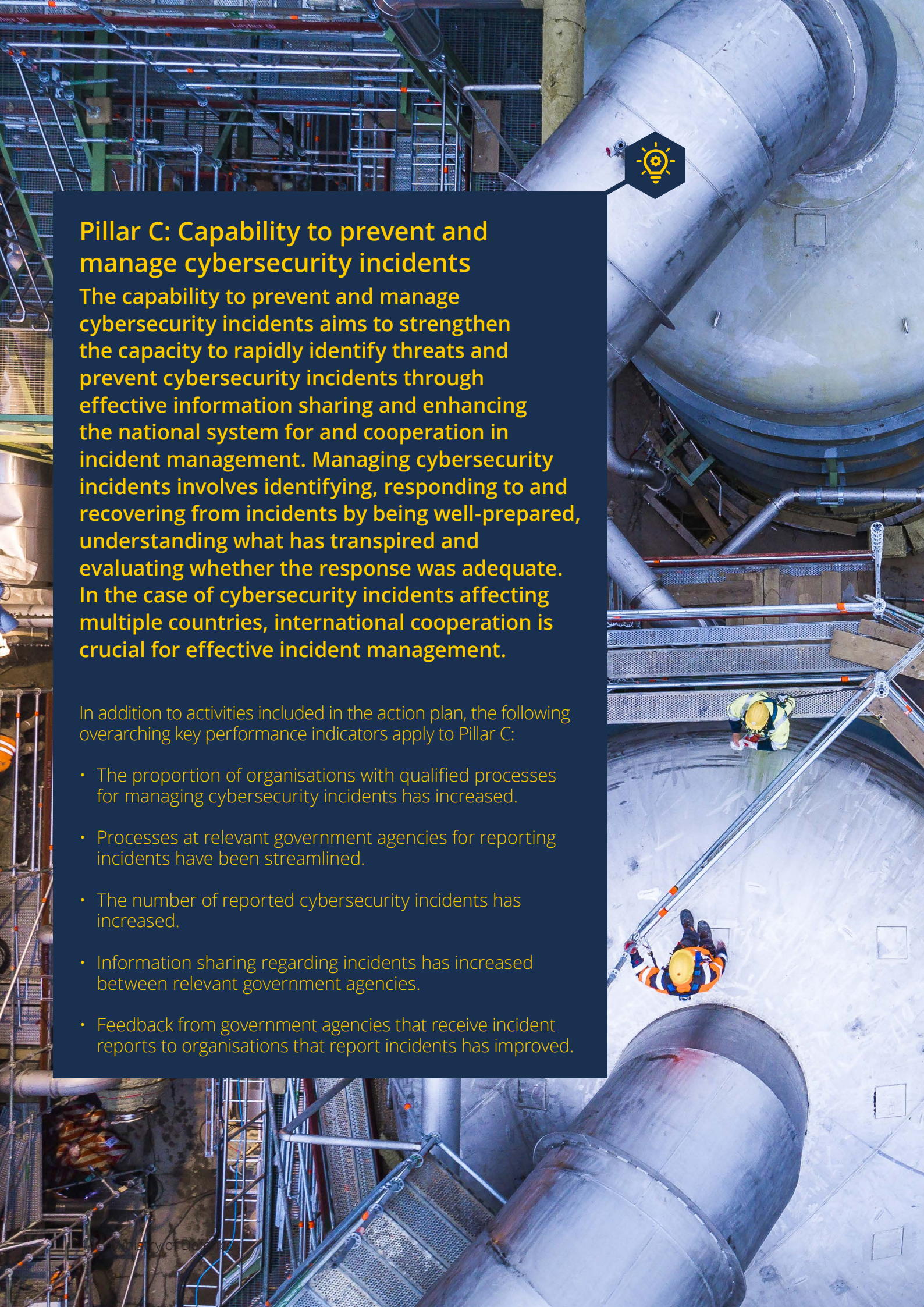
Developments in AI are leveraged to achieve significant positive impacts in the cybersecurity area. Sweden has good access to AI expertise and is represented in the international contexts where developments are taking place and is thereby able to identify and manage risks associated with AI, as well as taking advantage of the opportunities that AI offers in terms of cybersecurity.

Government agencies maintain a high degree of expertise, self-sufficiency and national autonomy when it comes to communications security for classified information (COMSEC). Based on the assumption that cryptographically relevant quantum computers may be in use from the early 2030s, quantum-safe cryptographic functions are developed and implemented in line with the coordination and standardisation needs resulting from Sweden's EU and NATO memberships. Quantum-safe cryptographic solutions are also prioritised for information that is sensitive but not classified, such as certain commercial secrets and personal data. Relevant government agencies strive to ensure that critical encryption technologies and products continue to be developed in Sweden and are adapted for national as well as EU and NATO needs. The Swedish cryptographic sector and new Swedish companies in this field have opportunities to develop in Sweden and supply an international market. Government agencies continue to support work on cryptographic protection within the EU and developing an active contribution to NATO's capabilities in this area, including by creating conditions for Swedish cryptographic products to be used within the Alliance. The Government's substantial investment in research and innovation for emerging, disruptive and strategic technologies as outlined in Government Bill 2024/25:60 has increased the long-term skills provision in various technological areas, which is crucial for Swedish competitiveness, societal development and cybersecurity.

A quantum computer chip.

Photo: Sofia Sabel/Image Bank Sweden


J60
MICRO-D
A
48p rev 1
14mm3



Pillar C: Capability to prevent and manage cybersecurity incidents

The capability to prevent and manage cybersecurity incidents aims to strengthen the capacity to rapidly identify threats and prevent cybersecurity incidents through effective information sharing and enhancing the national system for and cooperation in incident management. Managing cybersecurity incidents involves identifying, responding to and recovering from incidents by being well-prepared, understanding what has transpired and evaluating whether the response was adequate. In the case of cybersecurity incidents affecting multiple countries, international cooperation is crucial for effective incident management.

In addition to activities included in the action plan, the following overarching key performance indicators apply to Pillar C:

- The proportion of organisations with qualified processes for managing cybersecurity incidents has increased.
- Processes at relevant government agencies for reporting incidents have been streamlined.
- The number of reported cybersecurity incidents has increased.
- Information sharing regarding incidents has increased between relevant government agencies.
- Feedback from government agencies that receive incident reports to organisations that report incidents has improved.

Target 11: More effective and secure national and international information sharing

Continually mapping, identifying and assessing cyber threats across the spectrum often requires extensive cooperation between government agencies, both national and international, particularly in established forms of cooperation within the EU and NATO. Cooperation with the private sector and non-profit organisations also provides important contributions. Organisations' various information flows can contain information that is important both for the organisation itself and to others regarding cybersecurity incidents, vulnerabilities and threats. Effective cooperation with a high degree of trust between actors thus forms the foundations for information sharing and warnings regarding relevant threats and vulnerabilities, as well as investigating and attributing attacks.

Desired state 2030

The requirements of the NIS 2 Directive and the Cyber Resilience Act contribute to increased information sharing regarding vulnerabilities discovered in products and services. The NCSC has well-established methods for international and public-private cooperation. Positive examples of public-private partnerships have been further developed. Platforms for sharing security-related information are established both within and between the public and private sectors, which enables increased sharing and analysis of real-time information at technical and operational levels. Through enhanced analysis of such information, organisations are encouraged to implement and share suggestions of relevant security-enhancing measures. These efforts also contribute to improved and relevant situational awareness reports from the NCSC, which benefits various target groups and improves cooperation between relevant government agencies regarding matters of attribution. Information sharing is conducted in accordance with legislation and established processes for the benefit of all involved parties and strengthens, among other things, the ability to identify, manage, and investigate incidents and attacks.

Increased international cooperation in the cyber field contributes to valuable insights on themes such as information sharing methods which are adapted to the Swedish context. Public-private partnerships contribute to an enhanced capability to detect and resist cyberattacks, whether they are isolated incidents or part of hybrid activity.

Industry.

Photo: Per Pixel Petersson/Image Bank Sweden

Target 12: Strengthened public-private management of cybersecurity incidents

Effective coordination is of central importance during cybersecurity incidents. Insights and experiences must be reflected in the development of national incident management capabilities. The willingness to notify and report incidents needs to be encouraged, while challenges associated with overlapping reporting requirements need to be addressed. To effectively utilise the combined investigative and preventive resources in the cybersecurity area, government agencies' information sharing regarding incidents needs to be appropriate and purposeful. Sweden's ability to identify, manage and address cybersecurity incidents shall be strengthened.

Desired state 2030

Government agencies continuously develop the national operational capability for support and management of cybersecurity incidents. The NCSC develops and strengthens Sweden's overall capability to prevent, detect and manage hostile cyber threats and other IT-incidents. Public-private cooperation on cybersecurity incidents has developed and utilises incident management expertise from the private sector. Organisations in relevant sectors have the NCSC as a point of contact for the management of cybersecurity incidents.[1] Incident exercises are regularly conducted within and between organisations. National exercises continue to be conducted and developed. Government agencies have established joint incident reporting platforms that facilitate organisations in fulfilling their reporting obligations and receiving feedback and support, while also enhancing information sharing between relevant government agencies. Government agencies continuously communicate regarding capacity-enhancing measures related to the likelihood or consequences of incidents. Communication between recipient government agencies and affected organisations during and after cybersecurity incidents continue to evolve. Organisations' willingness to notify and report cybersecurity incidents increases.

Sweden has also actively participated in the coordinated management of large-scale cybersecurity incidents within the framework of cooperation procedures at EU level and has contributed to effective cross-border cooperation at the operational level between Member States.

1 However, this does not apply to, for example, security-threatening events under the Protective Security Ordinance.

Target 13: Enhanced capability to prevent and combat cybercrime

Cybercrime is continuously evolving and generating large criminal proceeds. This presents challenges for law enforcement agencies and creates a need for continuous development to address emerging challenges. The growing proportion of crime incorporating digital elements highlights the link between cybersecurity efforts and the fight against cybercrime, in which enhanced cybersecurity leads to fewer cyber offences. This underscores the importance of law enforcement agencies enhancing their capability to investigate and prosecute digital crimes.

The willingness to report incidents to law enforcement agencies also needs to increase. The number of cyberattacks on Swedish digital critical infrastructure, or individual persons, from abroad demonstrates the importance of Sweden participating in international collaborations aimed at combating ransomware attacks and data theft.

Desired state 2030

Law enforcement agencies' development of specialist functions for cybercrime has resulted in an improved ability to combat such crimes. Cooperation between the NCSC and law enforcement agencies' specialist functions has contributed to better situational awareness reports. Law enforcement agencies' ability to gather information in digital systems and from communication services has improved. In addition, legislation has developed through the EU's Regulation on European Production Orders and European Preservation Orders for electronic evidence. Efforts to combat the criminal economy has improved and the proceeds from cybercrime have decreased.

Government agencies' ability to recruit and retain digital crime-fighting expertise has improved and the knowledge about criminal actors' methods and the effectiveness of countermeasures has increased. The opportunities for operational cooperation offered by Eurojust and Europol have been strengthened and are utilised more extensively.

Relevant government agencies' support and advice regarding management and prevention of cybercrime has increased. Crime prevention partnerships between the non-profit sector, the private sector and government agencies has developed further. The hidden statistics for digital crime have decreased and the reporting rate is approaching levels similar to those of physical crime.

An enhanced capability to combat cybercrime has contributed to increased security for individuals and organisations in Sweden. Moreover, due to state threat actors' ability to use criminal groups as intermediaries for various forms of hybrid activities, Sweden's overall capability to counteract hybrid threats has been strengthened.

Telecommunications

Photo: MSB

Implementation and follow-up

The National Cybersecurity Strategy establishes a direction for the Government's efforts to address key issues related to Sweden's cybersecurity. The Strategy will be regularly evaluated, at least every five years, based on its key performance indicators, in accordance with the requirements under the NIS 2 Directive.

According to the attached action plan[1], the Strategy will be put into practice through initiatives such as specific government assignments and through steering of government agencies. Other government decisions may also be necessary to implement the Strategy in this respect. Developments in technology and the threat landscape mean that the cybersecurity field is changing and evolving rapidly, and therefore the Strategy needs to be implemented with a degree of flexibility. The content of the action plan will therefore be regularly updated. In addition, its content will be reviewed and evaluated as the Government sees fit. The appendix concerning organisations with roles and responsibilities within cybersecurity will also need to be updated, e.g. when national regulations implementing the NIS 2 Directive in Swedish law enter into force. The update will be carried out as the Government sees fit.

1 The action plan for 2025 is only available in Swedish.

Glossary

All-hazards approach: Applied in this strategy in the same way as the all-hazards approach in Recital 79 of the Preamble to the NIS 2 Directive.

Availability: An aspect of cybersecurity that means that information or information systems must be available when needed.

Confidentiality: An aspect of cybersecurity that means that only authorised individuals can access a given piece of information. However, questions related to the principle of public access, and public access to documents, fall outside this definition.

Cyberattack: An interaction between an attacker and a target, which: i) the attacker does not have the right to carry out against the target; ii) causes an exchange of information that results in an interaction, configuration, installation/saving, uninstallation/deletion or denial of service in one of the target's information systems; iii) results in at least one unwanted consequence for the target in terms of confidentiality, integrity or availability for the target or for others via the target; and iv) the attacker carries out with hostile intent.

Cybersecurity: Used in accordance with the NIS 2 Directive, which uses the definition found in the EU Cybersecurity Act, i.e. all activities that are necessary to protect network and information systems, users of these systems and others concerned about cyber threats.

Cybersecurity Act: The EU Cybersecurity Act regulates areas such as cybersecurity certification in the Single Market, which enables various cyber products and cyber services (e.g. cloud services) to be certified against a harmonised, quality-assured and common set of requirements. Such certification can be used in government agencies' requirements in conjunction with procurement, as requirements in supervisory and sectoral agencies' provisions, or to demonstrate compliance with various cybersecurity requirements.

Cyber range: Testbed and training facility for cybersecurity.

Cyber Resilience Act: Under the Cyber Resilience Act, certain critical products and services are subject to stricter security requirements (including assessment of conformity and third-party review according to the EU's New Legal Framework and the Cybersecurity Act's cybersecurity certification framework).

A helicopter over Swedish woodland.

Photo: Hampus Hagstedt/Swedish Armed Forces

Distributed denial of service (DDoS) attack: A method of attack that sends large amounts of data traffic or requests to a server or other network component with the aim of limiting its ability to process data and thereby blocking access for other, legitimate data traffic.

Digital supply chain: Services and infrastructure that supply or enable the supply of digital products used to establish, maintain, develop or restore an organisation's information management and information systems.

Integrity: An aspect of cybersecurity that means that information and information systems are correct or function as intended and have not been changed incorrectly.

IoT: Internet of Things relates to the use of connected devices in organisations.

Mono-dependency: Services or infrastructure which organisations are dependent on and for which alternatives are unavailable if the existing service or infrastructure were to cease.

Network and information systems: A network and information system as defined in Article 6.1 of the NIS 2 Directive.

NIS 2 Directive: Directive (EU) 2022/2555 of the European Parliament and the Council of 14 December 2022 on measures for a high common level of cybersecurity throughout the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

Ransomware: Malicious software that encrypts parts or all of an organisation's information stored on affected information systems and prevents access to that information. This type of malicious software is designed to attempt to extort an organisation or individual. Attacks can also be conducted with the aim of accessing specific information for purposes such as intelligence gathering.

Systematic cybersecurity: Preventive and continuous adaptation of protection based on needs and risks. This includes working methods based on a methodology for operational risk aimed at establishing, implementing, advancing, monitoring, reviewing, maintaining, and improving organisations' information security, i.e. protection of information assets that relate to confidentiality, integrity and availability.

Government Offices of Sweden
Ministry of Defence
Switchboard: +46 8-405 10 00
www.government.se