REPUBLIC OF ESTONIA
MINISTRY OF ECONOMIC AFFAIRS
AND COMMUNICATIONS

CYBERSECURITY STRATEGY 2024–2030 'CYBER-CONSCIOUS ESTONIA'

TABLE OF CONTENTS

INTRODUCTION

Estonia is an open and democratic society with one of the highest levels of digitalisation of public services in the world. For several decades now, people in Estonia have grown accustomed to the convenience of online access to public services, the protection of data entrusted to the state, and the modernisation and personalisation of services developed by both the state and the private sector. Estonia's long experience, rapid technological development and the flexibility of a small country offer excellent opportunities for this. At the same time, the more digitalised a state, economy and society become, the more challenging it is to ensure cybersecurity. The vision of the strategy 'Cyber-conscious Estonia' is to create an Estonian society where the reliability and resilience of digital services remain unchanged, even in a significantly deteriorated security situation and in the context of very rapid global technological development. Only this way can we maintain the high level of trust that Estonian citizens have in both the digital state and the digital services of the private sector intertwined with it.

In updating this strategy, the new EU cybersecurity directive (NIS 2 Directive)[1] guidelines regarding national strategy documents[2] and the national strategy 'Estonia 2035' have been considered. Sectoral cybersecurity aspects and development objectives are described in the National Defence Development Plan[3], the Internal Security Development Plan[4] and other sectoral development plans (research and development, education, foreign policy), and are not duplicated in this document.

The country's central development strategy 'Estonia 2035' states: 'We will ensure that the cyber risks of the digital society are well-managed, and that Estonian cyberspace is highly reliable.'[5] The foundations of the state's security policy further highlight: 'In the digital space, we need to plan cyber and information security across all information systems, organisations and processes.'[6]

Within the framework of the development plan 'Estonia's Digital Agenda 2030'[7], this cybersecurity strategy, the fourth in a row, 'Cyber-conscious Estonia', can be regarded as a White Paper in the field of cybersecurity.[8] As a horizontal strategy, its objective is to make agreements between the actors involved in ensuring Estonia's cybersecurity – the public sector (both civilian and military defence), providers of services that are vital and essential for the functioning of society, companies operating in the sector, universities and other research institutions – and to create the conditions for implementing a comprehensive, systemic and inclusive cyber policy.

This strategic document sets objectives for 2024–2030 in four key areas: managing the development of national cybersecurity, enhancing society's cyber resilience, strengthening cyber-shield (including incident monitoring and prevention), and shaping a secure cyber environment in Estonia and globally.

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

2 https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32022L2555&qid=1706103351118, Article 7(1).

3 National Defence Development Plan 2022–2031, https://www.riigikantselei.ee/media/1451/download.

4 Internal Security Development Plan 2020–2030, https://www.siseministeerium.ee/media/748/download.

5 Development Strategy Estonia 2035, https://valitsus.ee/media/4022/download, p 27.

6 Foundations of Estonian Security Policy, https://www.riigiteataja.ee/aktilisa/3280/2202/3001/julgeolekupoliitika_2023.pdf, p 6.

7 The currently valid version, which is subject to updates, can be accessed here: https://www.mkm.ee/media/6791/download.

8 Within the framework of 'Estonia's Digital Agenda 2030', three additional white papers are either being drafted or have already been completed: the white paper on data and artificial intelligence, the white paper on the personalised state, and the white paper on e-ID.

1 STRATEGIC CONTEXT

As cyberspace is inherently global, worldwide threats, trends, and opportunities are also reflected in Estonia. Compared to the previous strategic period[9], the overall level of cyber and security threats worldwide has clearly increased, which has, in turn, influenced the vigilance of society. This has been driven by growing dependence on digital solutions and advancements in technology, including artificial intelligence and quantum technology. Attackers' objectives have become more diverse: alongside cybercriminals seeking financial gain, politically motivated attackers now play a more prominent role in cyberspace. Among the latter there are technically advanced threat actor groups[10] associated with state governments as well as volunteers organised via social media, known as hacktivists.

1.1 STATE ACTIVITY IN CYBERSPACE

For Estonia and the entire Western world, Russia's war of aggression against Ukraine has significantly heightened the cyber threat. This has shown that, in addition to supporting kinetic warfare through cyberattacks on the opponent's vital infrastructure, cyberattacks are also more broadly used as part of hybrid warfare. Cyberattacks are used to gather intelligence and to 'punish' unfriendly states for their political decisions. The risk of supply chain attacks may also increase, in which a software component used in many products is compromised, providing simultaneous access to many organisations worldwide. Other active interstate conflicts, such as the Israel-Hamas war, also indirectly impact Estonia's cyberspace.

Although Estonia's security environment, including the cyber threat landscape, has so far been most directly influenced by Russia's actions, in the longer term, greater attention must also be paid to other authoritarian states active in cyberspace, such as Iran, North Korea and especially China.

China's activities in cyberspace are primarily focused on cyber intelligence, gathering information on political trends, intellectual property, and research outcomes in sectors of interest. Through its competitive technology sector, China systematically creates potential vulnerabilities that it can later exploit to its advantage and is therefore interested in the widespread export of its products.

The broader politicisation of internet governance and technology continues, with cyberattacks (including on technology supply chains) increasingly being used in interstate influence operations. As Russia's isolation from the global internet and supply chains used by the Western world deepens, it may be decreasingly constrained by fears of cyberattacks harming services or supply chains it relies on.

1.2 RANSOMWARE ATTACKS AND OTHER CYBERCRIME

Ransomware attacks have been in the spotlight for years as one of the most damaging manifestations of global cybercrime. It is a lucrative business model for criminals, with the global total of ransom payments increasing year by year. Since these attacks have also targeted vital services and critical infrastructure, preventing

9 The most recent Estonian cybersecurity strategy covered the period 2019–2022.

10 These are referred to using the acronym APT, derived from the English term advanced persistent threat.

and addressing ransomware is closely tied to the overall security of the state. In Estonia, an average of around a couple of dozen such attacks have been recorded over the last three years. Although, unlike in many other countries, our society has not yet been seriously affected by disruptive attacks, this possibility must also be considered in the new strategy period.

Estonian people are most affected daily by ordinary cybercrime, primarily investment fraud and bank account draining through phishing and scam calls. According to the Estonian Police and Border Guard Board in 2023, over €8.3 million was fraudulently obtained from private individuals in Estonia.[11] Systematic and holistic prevention involving all societal groups plays a crucial role in reducing the impact of cybercrime.

1.3 GLOBAL TRENDS IN TECHNOLOGY

Estonia's cybersecurity is also influenced by general technological trends: The increasingly widespread adoption of 5G technology, the broader implementation of artificial intelligence in both public and private sector services, the expansion of the Internet of Things (IoT), growing dependence on foreign service providers, including the processing of more data in cloud solutions, and, in the longer term, the increased accessibility of quantum computing.

Several technological trends will enable the creation of more effective cybersecurity solutions in the future, but this requires the existence of a strong cybersecurity sector, the development of new technologies and the cryptography competences. The rapid development of technology provides various growth opportunities for Estonian society and economy, provided we have sufficient know-how and an economic environment conducive to innovation.

The smarter the environment and technology around us become, the more vulnerable they are to cyberattacks. The rapid development of artificial intelligence creates new opportunities for providing services and saving resources, but these same solutions can also be exploited in cyberattacks.

The digitalisation of the economy, also known as the fourth industrial revolution, encompasses more sectors, including food production, medicine, defence, space and other industries, which in turn increases interdependence and increases the complexity of cyberspace and cyber risks. In some sectors, the practice of managing cyber risks is still rudimentary. Cybersecurity is a horizontal cornerstone in the digitalisation, management and development of services.

1.4 DEVELOPMENTS IN THE EUROPEAN UNION AND NATO, AND COOPERATION WITH LIKE-MINDED COUNTRIES

The advancement of technology, the spread of global cybercrime, and the evolving threat landscape driven by geopolitical tensions and competition have increased the need and desire for cooperation among like-minded countries. In the United Nations (UN), discussions are underway to create a new global framework for addressing cybersecurity issues, and Estonia, together with other like-minded countries, advocates for the enforcement of international law in cyberspace. The European Union member states have reached a fundamental political agreement on the world's first regulation of its kind concerning artificial intelligence and, in

11 Press release of the Police and Border Guard Board, 16 January 2024, https://www.politsei.ee/et/uudised/kurjategijad-petsid-eesti-inimestelt-vaelja-vaehemalt-8-3-miljonit-eurot-11725.

addition to the NIS Directive, adopted the Cyber Resilience Act in March 2024, which harmonises and strengthens the quality of digital products entering the European market. Since speed is one of the key words in successfully managing cyberattacks and incidents (e.g. in the case of high-impact supply chain attacks), new opportunities for operational and automated threat information sharing are being explored. One such possibility is the European Commission's initiative for regional centres, under which Estonia, together with other Nordic and Baltic countries, is considering ways to deepen cooperation. Since 2016, cooperation on cyber defence between the European Union (EU) and the North Atlantic Treaty Organization (NATO) has increased, and it is in Estonia's interest to further strengthen this cooperation.

The United States has taken a leading role globally in combating ransomware groups, promoting the zero-trust security concept, and popularising the secure development and validation of applications (security by design and default). The same approach has been adopted as the basis for information protection in NATO, enhancing NATO's ability to develop secure information exchange solutions. Contributing to this are, for example, DIANA, an innovation accelerator for defence startups based in Estonia, and the CR14 foundation, established by the Ministry of Defence, which engages in cybersecurity research and development, including cyber exercises and cyber ranges.

Like-minded countries also cooperate to increase broader recognition of the risks associated with technologies originating from authoritarian states.

2 MANAGING THE DEVELOPMENT OF NATIONAL CYBERSECURITY

To achieve cyber-conscious Estonia, it is essential to develop a national institutional structure and framework that meets current needs and considers the recent changes in the field of cybersecurity. The protection of the digital state, including electronic information, requires cross-sectoral cooperation and the shared use of capabilities. This, in turn, requires clearly defining the competences, roles, and authorities of the system participants, ensuring inclusive planning, and shaping a functional community. Both the public and private sectors have identified strategic overall management and coordination of cybersecurity as one of the main bottlenecks that needs to be developed.

Estonia's previous cyber strategy for 2019–2022 identified the lack of coherent strategic management in cybersecurity as one of the major challenges.[12] One solution proposed in the strategy was to create a comprehensive unit or centre that consolidates the competences of multiple institutions, with its exact scope to be determined through a comprehensive interministerial cyber audit.[13]

Due to the changed security situation, the legal framework for cybersecurity, information protection and crisis management must be reviewed in the coming years to align with best practices and ensure the security of Estonia's state services and operations. During the revision of the Cybersecurity Act, the Ministry of Economic Affairs and Communications has proposed the opportunity to assess and prepare the necessary legal amendments to adopt best international practices, clarify the domestic governance arrangements, and the roles, rights, and obligations of the participants.

2.1 NATIONAL MANAGEMENT AND POLICY-MAKING

SITUATION

The field of cybersecurity in Estonia is managed and coordinated by the Ministry of Economic Affairs and Communications. Several institutions and individuals are involved in organising cybersecurity, including ministries, local government units, and providers of vital and socially important services, who shape and implement the strategy's priorities both independently and across organisations and areas of government.

The coordination of cybersecurity assurance, as well as the prevention and resolution of cyber incidents, is operated by the Information System Authority to the extent provided for in the Cybersecurity Act. The Consumer Protection and Technical Regulatory Authority acts as a certification authority for cybersecurity under Regulation (EU) 2019/881 of the European Parliament and of the Council[14]. Cyber diplomacy is part of the portfolio of the Ministry of Foreign Affairs. Cyber activities related to military defence and cooperation with NATO are in the area of government of the Ministry of Defence. The Ministry of the Interior is responsible for combating cybercrime. The Ministry of Economic Affairs and Communications, super-

12 CYBERSECURITY STRATEGY (mkm.ee), p. 12.

13 CYBERSECURITY STRATEGY (mkm.ee), p. 26.

14 Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32019R0881.

vising the area, harmonises cybersecurity policy objectives through the Cyber Security Council, involving all ministries. In addition, various cyber coordination units have been established, the most important of which is the Cyberpolicy Board, which includes representatives from state authorities, the private sector and research institutions. The other participants in Estonia's cybersecurity ecosystem are listed in Annex 1 to this strategy.

The Government of the Republic receives the most important cybersecurity issues each week as part of a cybersecurity briefing, as well as in response to major domestic incidents. Periodic overviews of the cybersecurity situation are provided to the Secretaries General and government members attending the Security Cabinet meetings. The cybersecurity community (information security managers, vital infrastructure owners and service providers) is also informed about threat assessments and the situation in cyberspace[15], and sector-specific newsletters[16] are distributed. Due to the decentralised management model, central policy-making is more challenging, and funding is more focused on individual institutions rather than on the national level.

Since 2018, the central legislation in the field of cybersecurity in Estonia has been the Cybersecurity Act, which, among other things, transposed the Directive (EU) 2016/1148 of the European Parliament and of the Council, NIS 1 Directive. In 2022, Directive (EU) 2022/2555 of the European Parliament and of the Council, NIS 2 Directive, was adopted, which significantly supplements the provisions of the previous directive and must also be transposed into Estonian law[17]. In addition, specific cybersecurity requirements for the financial sector have been established in the European Union.[18] In addition, based on NATO cybersecurity requirements, the cyber security defence requirements for classified information IT systems have been updated in the State Secrets and Classified Information of Foreign States Act.[19] In the process are the European Union regulations on cyber resilience, cyber solidarity, cybersecurity and data protection, NATO cloud security implementation directives, as well as certification schemes regulating the functioning of member states, which create the need to adapt Estonian legislation and determine baseline funding for fulfilling the obligations imposed on the state. In 2024, it was decided to begin updating the European Union's Cybersecurity Strategy (the last valid version from 2020), which involves reviewing existing roles, responsibilities, and forms of cooperation that may influence the development directions of this cybersecurity strategy.

The technological development impacts all aspects of the cyber threat landscape, which is why we must be able to adapt changes in a holistic approach and as a society in Estonia. The development of technology is no longer barely related to digital solutions, but to everyday life in general. Estonia is a fully digital state. In other words, cybersecurity as a concept is no longer only necessary for protecting technologies, but for the functioning of society and securing its future resilience.

STRENGTHS AND WEAKNESSES

Since several activities in the field of cybersecurity are the responsibility of different ministries, it is important to align the objectives when planning the strategy and policies.

15 See https://www.ria.ee/kuberturvalisus/kuberruumi-analuus-ja-ennetus/olukord-kuberruumis, https://www.mkm.ee/digiriik-ja-uhenduvus/kuberturvalisus/riigi-kuberturvalisuse-tagamine.

16 See https://www.mkm.ee/digiriik-ja-uhenduvus/kuberturvalisus/riigi-kuberturvalisuse-tagamine.

17 The deadline for transposition is October 2024.

18 Regulation (EU) No 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, https://op.europa.eu/et/publication-detail/-/publication/8ebf4cce-305c-11ee-9e98-01aa75ed71a1/language-et.

19 State Secrets and Classified Information of Foreign States Act – Riigi Teataja

So far, it has not been analysed whether it is reasonable to consolidate the functions performed by different institutions into a single institution. The trend towards the creation of such consolidated cybersecurity agencies has been adopted in recent years both in the European Union (e.g. Czech Republic, Netherlands, France, Belgium, Lithuania, Latvia) and in many like-minded countries (e.g. the United Kingdom, Singapore), but the scope of the institutions' responsibilities and their placement within government administration vary from country to country (in some countries, under the Ministry of Defence, and in others, directly under the Prime Minister).

The Cybersecurity Act establishes the primary legislative basis for cybersecurity and follows a risk-based approach. A risk-based approach must also be introduced in the related legislation. This enables the flexible implementation of measures that best ensure the achievement of the objective. New technologies and the evolving threat landscape create the need to reassess the flexibility and proportionality of regulations, the balance of rights and obligations, and the scope of the subjects involved. There are inconsistencies and ambiguities in the current legislation as regards the requirements and obligations of the target group. As several European Union, NATO and other international legislation have been introduced in a short period, their correct and consistent implementation, as well as that of national legislation, requires special attention and unified coordination. Under the Electronic Communications Act the minimising of supply chain risks has been taken up. To align other sectors, the objectives must be more closely linked to the state's cybersecurity goals.

In 2024, the number of topics related to the standardisation of the cyber domain (e.g. certification schemes based on the NIS 2 Directive and the EU Cybersecurity Act, the Cyber Resilience Act, the Cybersecurity Strategy) will have increased due to EU legislation, which will require a broader coordination of domestic activities (i.e. creating capabilities, planning resources, and involving relevant stakeholders, partners, and, depending on the situation, other market participants). Estonia's international leadership in launching the cybersecurity cost model initiative has been insufficient, and there are gaps in coordination towards the European Union, within the country, and in cybersecurity cooperation among member states.

THE OBJECTIVES WE WANT TO ACHIEVE DURING THE STRATEGY PERIOD

- The field of cybersecurity is centrally and strongly managed and coordinated, all important parties are involved in policy making, it is regularly visible at the level of the Government of the Republic and the needs of internal security, data protection, national defence and the economy are considered.
- Cybersecurity obligations imposed on different target groups are proportional and purposeful, considering the activities of these groups and the impact of the related cybersecurity threat on society.
- National coordination and cooperation between experts in the field have been enhanced.
- To obtain a central and up-to-date risk overview of developments in the field of cybersecurity, the Cyber Security Council has observed the implementation of the cybersecurity strategy and monitored and updated trends of development.
- European Union and NATO directives have been transposed into Estonian law. Clarity of definitions, a balance between the requirements of national defence, freedom to conduct business and cybersecurity, technology neutrality, risk-basis, including minimisation of supply chain risks, and user-centricity are ensured in legislation. Sufficient time has also been provided for implementing the associated requirements.

ACTIVITIES NEEDED TO ACHIEVE THESE OBJECTIVES

- When developing the legal framework and making decisions that affect cybersecurity, it is necessary to take into account international trends, the prevailing threat landscape, the security situation, and other changes related to cybersecurity, information security, and data protection.
- It is necessary to analyse the creation of an institution or centre that consolidates cybersecurity competences, which would improve coordination at the national level and collaboration among sector experts, and to make a decision based on the analysis by 2027 at the latest.
- The Cyber Security Council must regularly update and monitor progress towards the objectives and activities of this strategy.
- Together with partner institutions, the transposition of the NIS 2 Directive needs to be evaluated, the existing legislation on cybersecurity and data protection (State Secrets and Classified Information of Foreign States Act, the Public Information Act, the Electronic Communications Act, etc) should be harmonised. The Cybersecurity Act should also be updated, during which the circle of obliged persons and the proportionality of obligations and supervisory measures are assessed and organised, reducing supply chain and other relevant risks, for example by creating legal possibilities for the enforcement of measures that can be used to prevent incidents more promptly than before.

METRICS

- According to the EU Cybersecurity Index (EU CSI)[20] developed by the European Union Agency for Cybersecurity (ENISA), Estonia's performance is above the Union's average in all measurable areas.
- Estonia continues to rank among the top ten countries according to the International Telecommunication Union (ITU) global cybersecurity index, ranking 3rd in 2020 (assessed every four years).
- Annual review of the implementation of the objectives of the Cybersecurity Strategy at the Cyber Security Council. – Yes/No.
- Competences and national coordination for cybersecurity have been analysed and a decision has been made. – Yes/No.
- The revision of the Cybersecurity Act has been carried out and the target group implementing the law has been regulated. – Yes/No.
- Estonia has transposed European and NATO directives on cybersecurity. – Yes/No.

2.2 FUNDING OF CYBERSECURITY

SITUATION

At the time the previous strategy was completed, Estonia's cybersecurity organisation was clearly underfunded and project based. From 2020 to 2024, the volume of the state's digital society development plan increased from 52.6 million euros to 149 million euros, with the cybersecurity portion growing from 3.9 million euros (7.4%) to 16.1 million euros (10.8%).[21]

Due to the changed security situation, ministries, the institutions in their area of government and constitutional institutions can use funds from the Government of the Republic's reserve for unforeseen expenditures and to increase the level of cybersecurity in the financing of activities

20 EU Cybersecurity Index, https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/eu-cybersecurity-index.
21 The data comes from the State Budget Acts for the years 2020 to 2024.

approved by the Ministry of Economic Affairs and Communications.[22]

The funding of cybersecurity in Estonia's private sector remains insufficient, and companies often realise only after a cybersecurity incident occurs that they should have invested in cybersecurity earlier. For smaller and medium-sized enterprises to invest more in their cybersecurity, the Information System Authority, in cooperation with the Estonian Business and Innovation Agency, has been offering support for mapping and developing cybersecurity levels as part of a pilot project since March 2023. One important requirement of the support measure is the applicant's own contribution. In this way, the private sector is also encouraged to contribute to cybersecurity, while simultaneously promoting the cybersecurity services market. The creation, development, and continuation of such measures helps increase cybersecurity funding in the private sector, but the mentioned pilot project will end in September 2024.

The enhancement of cybersecurity competence also takes place on a project basis. Since 2022, the Information System Authority has been fulfilling the role of Estonia's National Coordination Centre (NCC-EE) within the European Cybersecurity Competence Centre network, promoting the development of the cybersecurity industry, technology, and science. One of the centre's objectives is to bring international research grants and investments to Estonian cybersecurity companies. To this end, the NCC-EE has been financed on a project basis through European Union resources, as well as through the resources of the Research and Development, and Innovation and Entrepreneurship (RDIE) development plan. Similarly, youth cybersecurity education, talent policy, and further training have also been funded on a project basis, often only when the leaders are able to secure co-financing from a ministry's budget for a European Union project.

Funds have been requested from the targeted reserve to compensate for the costs associated with the transposition of European Union directives for the entities under the Cybersecurity Act and the relevant institutions of the relevant areas of government whose tasks are changing.

STRENGTHS AND WEAKNESSES

Instead of the current largely project-based funding model, it is necessary to secure permanent funding for the operation and further development of existing national cybersecurity services, and to find additional resources to develop new demand-based services and to meet the obligations of the state under new EU legislation[23].

Public sector spending on cybersecurity varies widely, and it is difficult to develop a common methodology for assessing the adequacy of the spending amount. It is important to raise awareness in the public sector of the critical need to contribute funding for cybersecurity in the IT budget. This knowledge is also needed by the private sector – both by those who are legally obliged to address cybersecurity and by those who do so out of market necessity.

A country can shape cybersecurity policy by leading by example and acting as a major customer. Supports and funding applications for digitisation must also take into account the cost of cybersecurity components. IT procurements and cooperation agreements must include, among other things, cybersecurity requirements based on the security situation to maintain or improve the security level of the services. Risk assessment should also be implemented, attention be paid to attacks against supply chains, and compliance with contractual requirements must be monitored, security-tested and verified.

22 The procedure for the allocation of the funds from the reserve fund of the Government of the Republic and the use of the allocated funds, https://www.riigiteataja.ee/akt/112022019004.

23 See chapter "2.1 National management and policy-making" on page 7.

THE OBJECTIVES WE WANT TO ACHIEVE DURING THE STRATEGY PERIOD

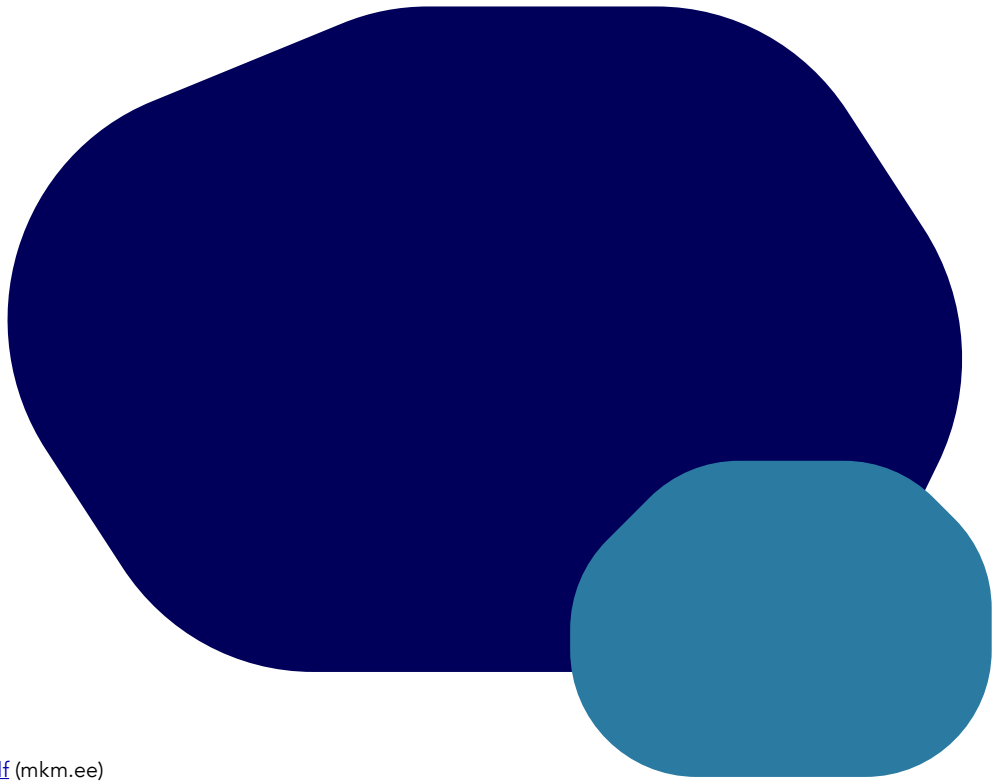
+ Ensure the adequacy of budgetary resources for the secure operation and development of services.
+ The funding for the state's basic cybersecurity services is consistently ensured at the agreed level, allowing for long-term planning.

ACTIVITIES NEEDED TO ACHIEVE THESE OBJECTIVES

+ Analyse the implementation of the cost model in Estonia as commissioned by the Ministry of Economic Affairs and Communications, including the baseline and target levels to achieve the objectives[24].
+ Analyse the appropriate size of the target level of the national cybersecurity component that public sector bodies should plan for in their ICT budgets.
+ Develop a long-term plan for the cybersector's RDIE that also takes into account the objectives of the cybersecurity strategy.

METRICS

+ The financing of basic cybersecurity services is provided from the state budget. - Yes/No.



24 Küberturbe kulumudel_v2.0.pdf (mkm.ee)

3 ENHANCING SOCIETAL RESILIENCE

The protection of Estonian society, individuals, institutions, businesses, and way of life from cyber threats is more successful the more widely and thoughtfully it is addressed. When considering cybersecurity threats, risks, and measures, both existing and potential future technological threats must be taken into account. Cybersecurity is important in every technology sector, from consumer electronics to space technologies. Development of the cybersecurity field must take into account national capabilities, the monitoring of information security development and maturity assessments, which in turn provide support for supranational crisis management and ensuring national security. Different target groups require different approaches, and limited resources also play a role.

3.1 UP-TO-DATE THREAT LANDSCAPE

SITUATION

The continued readiness to protect Estonia's digital state and society, and the way of life our people have become accustomed to in recent decades, depends largely on how aware the state is of what is happening in cyberspace. This includes an understanding of real and potential threats, technological developments and trends in international relations. Currently, the Information System Authority sees only the tip of the iceberg regarding incidents occurring outside the state network and the obligates entities under the Cybersecurity Act, which is why situational awareness must be improved. This would help to notify the widest possible range of users about emerging threats more quickly and accurately than before, as well as to develop precise practical guidelines for the protection of their network and information systems.

For example, attacks against healthcare institutions are becoming increasingly common, as cybercriminals primarily target organisations whose systems have a critical impact and contain extensive and sensitive data. One of the central objectives set out in the European Union's Digital Decade Policy programme for 2030 is ensuring that citizens of the Union have full access to their digital health records, prioritising healthcare services.

STRENGTHS AND WEAKNESSES

The central analyser of the national cybersecurity threat landscape and the entity responsible for informing government agencies, businesses and the public, is the Information System Authority. Issues related to the cybersecurity threat landscape reach the government level less frequently than the current geopolitical and security situation would suggest. Although cooperation with government agencies and the private sector is close, the Information System Authority, as the central cybersecurity agency, lacks a comprehensive sectoral and nationwide cybersecurity threat overview that would significantly expand the scope of threat awareness.

THE OBJECTIVES WE WANT TO ACHIEVE DURING THE STRATEGY PERIOD

+ To prevent, detect and counter cyber threats as quickly as possible, the Information System Authority creates a comprehensive threat landscape of the Estonian cyberspace, which will enable to provide better preventive support to different groups of society.
+ Thanks to a more comprehensive threat landscape and action guidelines, the

Government of the Republic of Estonia, the Riigikogu, ministries, public authorities, companies, and regular users are more aware of the situation in cyberspace thanks to a more comprehensive threat landscape and action guidelines, have been guided on implementing protective measures, and institutions understand better why and how to protect their information from cyber threats.

ACTIVITIES NEEDED TO ACHIEVE THESE OBJECTIVES

+ The Ministry of Economic Affairs and Communications and Information System Authority must agree with ISPs on how it would be most practical to create a cyberthreat landscape in an anonymous form, taking into account the fundamental rights of individuals and the freedom to conduct business.

METRICS

+ The relevant rights and obligations of institutions and undertakings contributing to the creation of a national threat landscape have been agreed upon. – Yes/No.
+ A nationwide cyber threat landscape reaches the target groups in a more complete form than before. – Yes/No.

3.2 COMPREHENSIVE PREVENTION

SITUATION

In order to cope with the continuous evolution and growth of cyber threats, all members of society need to be aware of them and be able to prevent potential incidents. It is unlikely to achieve complete success, as it is not possible to simultaneously elevate the entire population to a new level. Educating the population is effective through targeted campaigns. Young people are an important target group, and by influencing their behaviour as early as possible, we can prevent issues from escalating in the future.

Contributing to cyber-aware behaviour among different stakeholders, including businesses and public sector employees and key players, as well as the wider population, is essential to ensuring the security of society. One effective measure is the annual cybersecurity test, which serves as a reminder of best practices and the fundamentals of secure behaviour. In 2023, when the Information System Authority launched its cybersecurity test, over 15,000 people completed it, which can be considered a good result. The private sector also offers opportunities to test and enhance cybersecurity knowledge. It is essential for organisations to ensure that employees are aware of information security rules.

The risk-aware behaviour of all parties is shaped through comprehensive prevention to reduce the impact of cybercrime and cyber incidents. The use of social advertising and the involvement of influencers has increased the visibility of cybersecurity. As a combined result of all these measures, by September 2023, less than 10% of people in Estonia had not taken any steps to ensure their personal security or privacy in cyberspace.[25]

STRENGTHS AND WEAKNESSES

Awareness of cybersecurity among key public and private sector parties is still insufficient and needs to be promoted and improved in society at large to prevent cyber incidents and cybercrime. Cybersecurity is not perceived as a personal responsibility or a risk to the main activity of an organisation, but is often treated as a complex technical issue that needs to be dealt with by someone else.

25 Statistics Estonia's survey 'Information technology in households in 2023'. The Information System Authority commissions this survey, and its results are not publicly available on the Statistics Estonia website.

The awareness of small and medium-sized enterprises (SMEs) about threats in cyberspace is low, and SMEs also fail to make sufficient investments in improving cybersecurity or mitigating potential supply chain risks.[26]

The increase in cyber threats and the rapid expansion of the Internet of Things (IoT) is increasing the responsibility of all actors in cyberspace to ensure cybersecurity. Best practices in cyber hygiene are still not sufficiently implemented, nor are the opportunities for misuse of devices adequately minimised.

THE OBJECTIVES WE WANT TO ACHIEVE DURING THE STRATEGY PERIOD

- As a result of comprehensive prevention, Estonian society is cyber-aware. All those active in cyberspace have the necessary knowledge to deal with threats and prevent incidents.
- The level of cyber hygiene among the population has increased, and the number of residents who have taken no steps to ensure their personal security or privacy in cyberspace has decreased.
- The number of cybercrimes in Estonia has decreased as a result of comprehensive prevention and cooperation between Information System Authority and Police and Border Guard Board.
- The awareness of key individuals in the public and private sectors, including SMEs, has increased regarding the importance of cybersecurity in ensuring the main activities of the organisation.
- Cybersecurity awareness tests are widely used among employees of state agencies, providers of vital services, and businesses to assess and enhance their cybersecurity knowledge.

ACTIVITIES NEEDED TO ACHIEVE THESE OBJECTIVES

- In cooperation with the Ministry of Education and Research, it is necessary to develop skills in digital and cyber security in all age groups.
- It is necessary to assess the trends in cybercrime based on impact, develop corresponding technological capabilities and skills accordingly, and implement other measures to protect society and raise awareness.
- Society needs to be aware of the prevailing cyber threats and the responsibility of each individual in reducing them. Share advice on mitigating risks.
- In cooperation with the private sector, it is necessary to develop and implement measures to improve the cyber awareness of SMEs.
- To gain access to devices centrally managed by the public sector, the user must first pass a cyber test.

METRICS

- Avoiding e-services due to security risk. – Less than 10% (source Statistics Estonia).
- More than 90% of the population have taken the necessary measures to ensure their personal security or privacy.[27]
- The number of cybercrimes is decreasing.

26 Statistics Estonia's survey 'Information technology in enterprises in 2022'. These data are not collected at the request of the Information System Authority and are publicly available on the Statistics Estonia website. A survey 'Cybersecurity In Enterprises' conducted by Kantar Emor in 2022 and commissioned by the Information System Authority. The survey is not publicly available.

27 Statistics Estonia's survey 'Information technology in households'. The Information System Authority commissions this survey every year, and its results are not publicly available on the Statistics Estonia website.

3.3 IMPLEMENTATION OF THE INFORMATION SECURITY STANDARD

SITUATION

In 2022, requirements for systems that are essential for the functioning of society entered into force, an integral part of which is the implementation of information security standards – the Estonian Information Security Standard (E-ITS) and ISO/IEC 27001. The E-ITS is an information security system in the Estonian language created by the Information System Authority and is in compliance with the Estonian legal framework and the international standard ISO/EC 27001. The E-ITS entered into force in December 2022 and most obligated entities have started to implement it. The Information System Authority collects feedback and suggestions from implementers on how to update and improve the standard.

STRENGTHS AND WEAKNESSES

The large number of E-ITS measures create a considerable administrative burden for organisations, especially when implementing information security for the first time. The modular nature of the standard allows it to be adopted by organisations of any size. At the same time, the lack of employees with information security skills can pose a problem for smaller organisations, potentially hindering the implementation of a comprehensive management system. As a result, implementers have highlighted in their feedback the expectation for the development of solutions that would facilitate the adoption of E-ITS, particularly in smaller organisations. Automated solutions will also be needed in the future to simplify the implementation and monitoring of such measures.

As a result of the implementation of the Information Security Standard, the institution will have a comprehensive overview of its cybersecurity situation and risks. At the same time, experience has shown that not all those who are supposed to implement the Information Security Standard are aware of it, and there are those who implement measures primarily on a formal basis, without looking into the substantive risks. Another issue is that supply chain organisations are not interested in being integrated into the systemic implementation of information security and there are few tools to influence them.

The E-ITS is a standard that considers the conditions inherent in Estonia, but as it is not yet internationally recognised, organisations may need an internationally recognised ISO/IEC 27001 certificate. It is necessary to find ways to better align E-ITS with ISO/IEC 27001.

THE OBJECTIVES WE WANT TO ACHIEVE DURING THE STRATEGY PERIOD

+ Organisations and their leaders are aware of their information security obligations and consciously implement security measures based on a risk-based approach, and require the same from their supply chain.
+ E-ITS is updated annually in cooperation with the community. This is a community standard in accordance with Estonian legislation, which takes into account new threats and technological developments.
+ Organisations that need to prove the implementation of the information security management system at an international level can also do so by implementing E-ITS and passing an E-ITS audit.

ACTIVITIES NEEDED TO ACHIEVE THESE OBJECTIVES

+ There is a need to reinforce the positive image of E-ITS through sector-specific advocates.

+ It is necessary to expand the provision of information security standard training by also involving the private sector.
+ It is necessary to develop solutions to automate the implementation of E-ITS measures to facilitate the implementation of E-ITS in smaller institutions and organisations.
+ Opportunities must be created for organisations to measure the implementation and performance of E-ITS and, based on the measurement results, to assess the effectiveness of the implementation of E-ITS across different types of institutions.
+ The development of cyber threats and technology must be analysed, and protective measures must be streamlined when updating E-ITS.
+ Based on the analysis, a compliance mechanism between E-ITS and the ISO/IEC 27001 certification must be established and international recognition of E-ITS must be applied for.

METRICS

+ The E-ITS has been updated every year according to the threat landscape, taking into account best international practices – Yes/No.
+ As a result of the implementation of the E-ITS, there will be at least 50% fewer institutions with significant information security deficiencies by 2027. The assessment will be based on the Information System Authority's supervision procedure.

3.4 SECURE BASIC ARCHITECTURE AND MODERN SECURITY PRINCIPLES

SITUATION

As the amount of data and information systems that need to be protected continues to grow, but the overall threat landscape tends to deteriorate, the general trend in modern information security is to prevent security incidents from reaching the end-user as much as possible. In the event of an incident, the damage caused should be minimised and manageable as much as possible. From the perspective of the state, this means paying more attention to security aspects during the development and lifecycle of services, as well as standing up for government institutions to follow modern security principles and use state-of-the-art security solutions.

All developments must be based on the security-by-design principle, where security is taken into account from the earliest stages of service or product development. For example, in software development, security aspects are introduced at the design stage, rather than at a later stage or after the software has been introduced. With this approach, security is integrated throughout the entire software lifecycle – from requirements definition to design, development, testing and market launch. By doing so, it is possible to significantly reduce security risks, improve the overall quality of the software, and reduce the costs associated with addressing security vulnerabilities after the product's market launch.

In turn, rapid technological advances and the expansion of the Internet of Things (IoT) are creating new cyber threats. The arrival of quantum computers poses a potential threat to current cryptographic algorithms, as these computers can solve complex computations much faster than conventional computers.

This could pose a threat to widespread digital security methods in the future, which is why it is important to develop cryptographic solutions that are resistant to quantum computing in order to ensure the permanent security of data.

STRENGTHS AND WEAKNESSES

In Estonia's digital state with a history of a couple of decades, both the public and private sectors currently utilise numerous outdated systems, known as legacy software (estimated at 40% of public e-services). Legacy software is an information system, technology or software that is still operational but no longer meets modern information security and data protection requirements. Often, the owners of such services also lack a complete overview of their architecture, dependencies and main vulnerabilities due to the absence of necessary documentation. The systems are being kept operational, but they are not sustainable in the long term. Even services being developed today can become legacy software within a few years if their lifecycle and the need for updates are not comprehensively considered from the very beginning.

In addition to legacy software, a lot of digital waste has accumulated in public sector information systems over time. This includes unnecessary files, applications no longer in use, outdated devices, and similar items, the retention of which unnecessarily consumes significant data storage and may also pose security risks. While in some areas of government digital cleanup days are already organised on a regular basis, this practice should be extended (e.g. as part of a nationwide digital cleanup day[28] initiated by the private sector).

To mitigate future threats, Estonia participates in international projects and we are involved in quantum computing and sensor technology research groups. To ensure the continuity of Estonia's digital state, the security solutions in use must be reliable and up to date, which is why the assessment of security measures implemented requires a scientific approach and the creation of a centre of competence in cryptography. In the framework of cybersecurity, it is important to assess the compliance of security solutions used in systems, including cryptography and its implementation, with requirements arising from both Estonian and international legislation. Estonia lacks independent capability in this area. As a country, we rely on other countries' assessments, which consumes time and entails financial costs. The Estonian state is taking the first steps in this area, so that as a country we would have the elementary independent capability to assess communication security solutions by 2026.

With the development of cloud technologies and the increasing proliferation of supply chain risks and rise in hybrid workplaces, network security principles are also in need of a new approach. The classic approach to network security is to focus on securing against external threats, but because of the trends just mentioned, the boundary between 'internal' and 'external' in the definition of network security has become blurred and both are being protected. As a result, several countries (e.g. the USA, Japan, Germany and France) are increasingly moving towards the so-called zero-trust security model. According to this model, no one is trusted by default, and accessing any resource requires verifying the identity of each user and ensuring their right to use the resource. Such an approach is supported by the fact that data is increasingly moved to various cloud solutions, where the application of security measures is distributed between the service provider and the service user.

The topic of internet protocol is also associated with secure underlying architecture. Essentially, the Internet Protocol (IP) is a technical solution that enables data exchange on the internet, based on Internet Protocol addresses, or IP addresses. The Internet Protocol IPv4, in use since the early

28 Wikipedia article Digikoristuspäev (Digital Cleanup Day), https://et.wikipedia.org/wiki/Digikoristusp%C3%A4ev.

1980s, is becoming obsolete, one indication of which, is that there are no longer enough unique IP addresses. As a result, multiple devices use the same address, which is, however, unacceptable from an information security perspective. The solution is the adoption of the next-generation Internet Protocol, IPv6, which the private sector in Estonia is already gradually doing (e.g., Telia). Many countries, including India, the USA, and China, are moving towards IPv6-only services. Estonia also needs to present its IPv6 ambition at national level, as it is necessary to maintain our competitiveness and security.

THE OBJECTIVES WE WANT TO ACHIEVE DURING THE STRATEGY PERIOD

- By the end of the strategy period, the dependence of the state's critical databases and services on legacy has been reduced by at least half.
- Public sector institutions systematically reduce digital waste.
- In the public and private sectors, a lifecycle-based development and security policy is implemented as part of each stage of technology development, ensuring that security requirements are continuously taken into account until the application is removed from use.
- The public sector has established clear information security requirements and minimum IT service management requirements (centralised management, centrally regulated use of public cloud services, etc), the updating of which is regularly monitored by the Cyber Security Council.
- Be prepared for the arrival of new technologies (including quantum computing), taking into account technological trends.
- Increase national knowledge in cryptography and competence in the implementation of cloud services.
- National information is maintained with approved/certified quantum-resistant communications security (including cryptographic) solutions.
- Estonia has the necessary capability and interest for developing quantum software to be part of the European quantum ecosystem.
- Throughout the entire strategy period, central government agencies are moving towards a zero-trust security architecture.
- The capability to prevent security incidents in digital services is continuously updated through the implementation of the IPv6 internet protocol. Outdated technologies will be removed from use.

ACTIVITIES NEEDED TO ACHIEVE THESE OBJECTIVES

- In making funding requests and decisions, the reduction of legacy must be prioritised.
- Public sector institutions must set targets to reduce digital waste and participate in annual digital cleanup days.
- When developing new state digital services and updating existing ones, the principles of security by design and the implementation of non-functional requirements must be followed. This means that security risks are taken into account in the design and development of services at each stage and the life cycle of the service or product is planned comprehensively, in line with the E-ITS measures.
- It is necessary to establish scientific centres of competence for the implementation of cloud technologies and cryptographic solutions to ensure the quantum-resistance of data.
- A methodology for the assessment of data and communication security solutions containing cryptography is agreed and approved nationally and its implementation is addressed.

- It is necessary to investigate technological trends and future technologies, including artificial intelligence and quantum technologies, share best practices, and develop measures for their implementation.
- Gradually, the zero-trust security principle must be implemented.
- During the strategy period, the compatibility of the state's most widely used digital services with the new generation internet protocol IPv6 must be assessed, and a roadmap for implementing IPv6 in the public sector must be created.

METRICS

- By 2030, the dependence of public services on legacy for services consumed through the public network will have decreased to 20%.
- Minimum requirements for the organisation of IT services are established. – Yes/No.
- A foundation has been laid in the country for centres of competence in cryptography and cloud services. – Yes/No.
- Research and development studies and analyses have been carried out and the results can be implemented. – Yes/No.
- By 2030, an advanced level has been reached according to the maturity model of the zero-trust architecture (level Advanced in the maturity model used by CISA[29]).
- By 2030, at least 80% of publicly consumed state e-services will be on the IPv6 network.

3.5 ENHANCING THE CRISIS RESILIENCE OF VITAL SERVICES

SITUATION

Several recent crises have proven that vital infrastructure and services are an important target for the conflict parties. The conflict that intensified in the Middle East in 2023 directly affected Estonia for the first time through an attack on industrial automation. Russia's war in Ukraine has left no doubt that a potential adversary could deliberately damage our vital infrastructure if necessary. Industrial automation has gained momentum in recent years, but operators often lack sufficient knowledge of cyber threats and cybersecurity. So far, the discussion has been rather theoretical, but now there is also a practical example and experience of the necessity of maintaining manual control as an alternative, planning for the transition to manual control, and rehearsing in exercises, among other things.

Attacks on infrastructure and systems essential for the functioning of the state are not only the result of conflicts, but they also occur at other times. An attack can be carried out by a hostile state or a criminal group. In all cases, the attacker is trying to create situations with the greatest possible adverse impact. Anticipating such situations and establishing adequate cyber security defence is generally more effective when cybersecurity is monitored at the management level within the organisation and cyber risks are considered as part of business risks. There are also large providers of vital services where there is no cybersecurity manager, or where this function is performed by an infrastructure manager.

In the provision of vital services in today's security situation, it is no longer enough to ensure standard continuity, we must also be prepared

29 Further reading at https://www.cisa.gov/zero-trust-maturity-model.

for national defence scenarios.[30] Estonia has so far been able to respond adequately to cyber incidents and crises. Lessons have been learned and preventive steps have been taken. Crisis exercises usually also include a cybersecurity aspect and in crisis planning the importance of the functioning of ICT solutions and the protection of information assets has been taken into consideration.

One of the biggest innovations in recent years is the creation of the Information System Authority's cybersecurity reserve in autumn 2022. While during the ID-card crisis in December 2017, the Information System Authority managed to involve competent experts from both the public and the private sector on an ad hoc basis, a cybersecurity reserve system, unique in the world so far, has now been created and tested.[31]

STRENGTHS AND WEAKNESSES

Centralised monitoring will enable the identification of vulnerable devices and systems in Estonian cyberspace. However, no effective solution has yet been found for contacting problematic owners and persuading them to rectify the situation without delay.

Cybersecurity requirements are imposed nationally on a very wide range of public organisations, vital service providers and private companies. The information security requirements and the minimum requirements for the organisation of IT services are not based on uniform principles and the level of cybersecurity of society is not assessed on the basis of comparable criteria across providers of vital services, critical infrastructure and the subjects of the Cybersecurity Act. Many strict cyber defence requirements are imposed on businesses and public institutions whose services have a small impact on the functioning of society or the dependence of which on cyber components is small. This fragments already limited resources and does not allow focusing on filling more urgent gaps.

The management of institutions and organisations has a poor understanding of cyber threats and adequate protection, senior executives do not feel a high enough level of responsibility for cybersecurity and often view it as an inevitable cost of doing business.

The threat awareness of industrial automation operators in providers of vital services is inadequate, both regarding actors with a national background and criminals carrying out ransomware attacks. In addition to improving operators' awareness, a central monitoring capability needs to be developed, in particular for monitoring industrial automation networks and equipment.

The changes to national crisis management do not adequately and in a balanced way reflect the cyber risks associated with vital infrastructure. General measures to ensure continuity of service must be balanced with cybersecurity measures. Investments in the cybersecurity component have no added value if the perimeter is not secure or the electricity supply is unstable. There is also no point in investing in the physical protection of infrastructure if the vulnerabilities identified in the threat warnings cannot be overcome quickly enough and with the measures prescribed. Existing national crisis management governance models do not reflect clear priorities for ensuring continuity of services in times of peace and crisis, cross-dependencies between services or other crisis management requirements (environment, connectivity, escalation, etc).

The cybersecurity reserve was established very quickly and the process has started very successfully. But this does not mean that everything has been completed, on the contrary – a comprehensive concept has not yet been written down or agreed. The exercises have revealed a number

30 National Defence Development Plan 2022–2031, https://www.riigikantselei.ee/media/1451/download.
31 See https://www.ria.ee/uudised/suur-kuberoppus-pani-proovile-riigi-kuberreservi.

of shortcomings, the organisation of the reserve needs to be improved and some procedures clarified. Attention needs to be paid to resolving cyber incidents in the context of other crises and to the involvement and integration of the cybersecurity reserve with other areas of crisis management.

THE OBJECTIVES WE WANT TO ACHIEVE DURING THE STRATEGY PERIOD

- The monitoring of security vulnerabilities in vital services has been enhanced, and a direct notification system for the owners of critical network and information systems has been established.
- Vital infrastructures and services are equipped with security measures based on national security aspects, enabling them to withstand both current and future threats.
- The streamlined crisis management model takes into account national capabilities, interdependencies between services, priorities, and escalation options to ensure national (cyber)security. The operational continuity of essential digital services must be ensured, both in peacetime and during crises.
- The cybersecurity reserve concept is implemented, and the operation and involvement of the cybersecurity reserve in crisis management are seamless.

ACTIVITIES NEEDED TO ACHIEVE THESE OBJECTIVES

- It is necessary to study options on how to identify the owners of critical network and information systems (based on security vulnerabilities) and how to notify them directly.
- Owners of critical network and information systems must be obliged to eliminate the security vulnerabilities of network and information systems mentioned in the threat notices by appropriate measures. It is necessary to establish a central monitoring capability to observe industrial automation networks and equipment.
- Agree on the methodology and criteria on the basis of which cybersecurity requirements are differentiated, taking into account the impact of the service on the functioning of society.[32]
- The legal framework for crisis management must be streamlined, ensuring that crisis measures in the cyber domain are proportional to other measures.
- Based on national capabilities and scenarios, specify the continuity requirements for ensuring the crisis resilience of vital and digital services and begin their implementation.
- In preparing for crisis situations, solutions independent of the cybersecurity component must be envisaged.
- In organising the continuity of providers of vital services the possibility of a large-scale cyberattack needs to be taken into account.
- In order to ensure operational continuity, manual control must be retained as an alternative for critical systems, including industrial automation.
- It is necessary to test the crisis resilience of digital services and the functioning and involvement of the cybersecurity reserve to determine the limits of national capabilities, resource qualifications, and skill levels.

32 See sub-chapter "2.1 National management and policy-making" on page 7

METRICS

- The national crisis management model has been regulated. – Yes/No.
- The cyber incident has not caused any long-term disruption to vital services.
- The operation of all critical information systems has been restored within 24 hours after the incident.
- A cybersecurity reserve concept has been created – Yes/No.

4 STRONG CYBER-SHIELD – MONITORING AND PREVENTING INCIDENTS

A more cyber-aware Estonia is based on the principle that every person in cyberspace behaves consciously and responsibly, and every owner of an information system is responsible for its security. The National Cyber Security Centre contributes to this by raising awareness of threats in cyberspace and providing up-to-date technical measures to protect public digital services.

SITUATION

Security incidents in Estonian cyberspace are monitored and recorded by the CERT-EE Department of the Cyber Security Centre of the Information System Authority, which also helps to resolve public sector incidents. As far as possible, CERT-EE also helps to resolve cyber incidents outside the public sector, especially during active waves of attacks. In most cases, assistance is limited to standard recommendations to businesses, institutions and individuals.

Estonia is unique in that the state provides a central data communications service to public authorities and local government units. This is called the state network. In case of an increased threat, CERT-EE can implement additional protection measures for the national network. Effective monitoring of the national network is also ensured. CERT-EE sees only part of what is happening in the rest of the Estonian IP space: the threat landscape is put together using various technical tools and is based on the reports received by the incident register. Unlike in the national network, CERT-EE cannot implement additional protective measures in the rest of Estonia's IP space when the threat level increases.

STRENGTHS AND WEAKNESSES

Due to the transposition of the NIS 2 Directive, the number of institutions targeted in the Cybersecurity Act will increase, and will have to comply with stricter cybersecurity requirements. This has created an expectation in society that, in addition to adopting legislation, the state will take on a greater role in ensuring cyber security. In 2022, the first steps were taken on this path. In particular, CERT-EE started to provide the public sector with an additional technical layer of protection against denial-of-service attacks, the volume of which has multiplied due to Russia's war of aggression in Ukraine. The overall endurance of the national network to different types of cyberattacks has also been enhanced.

The Information System Authority's capability to act as a central authority against cyber threats is not bad, but the changed security situation and the deteriorating threat landscape mean that it needs to be strengthened during the strategy period. CERT-EE's ability to inform Estonian businesses and institutions about critical security vulnerabilities and to provide specific recommendations for their elimination must improve. In order to prevent public sector incidents, in addition to maintaining a high level of general cyber hygiene, there is an increasing need to address specific threats, such as the prevention of targeted phishing. Estonia, like many other countries, should also use the help of the international community of ethical hackers to test public services against security vulnerabilities.

THE OBJECTIVES WE WANT TO ACHIEVE DURING THE STRATEGY PERIOD

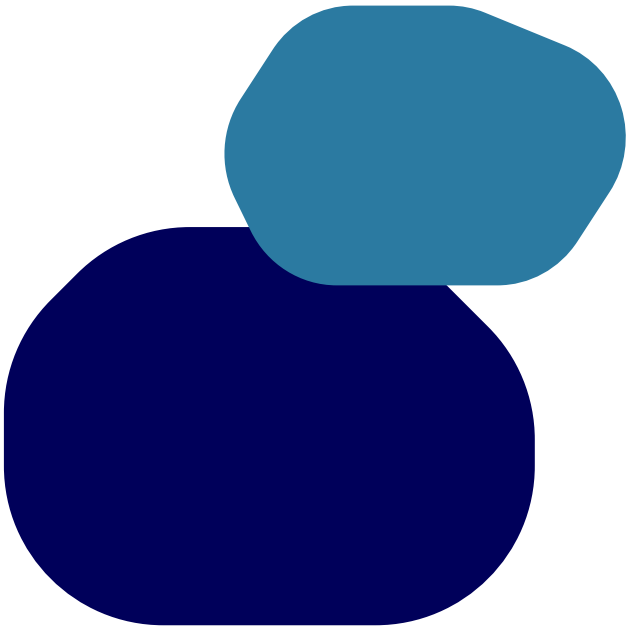
- The target group for CERT's protective measures is clearly prioritised.
- The nationwide Information Security Monitoring Centre (SOC) has been established and is operational, and in contact with strategic partners.
- The likelihood of successful cyberattacks against Estonian companies has decreased thanks to better sectoral visibility, automated monitoring and threat notification. Protective measures to mitigate threats are developed and provided by the local cybersecurity sector.
- The state provides support to prevent cyber threats originating from hostile countries (including basic penetration tests).
- Information about critical-impact security vulnerabilities and instructions for eliminating them reach vital infrastructure, Estonian companies, and individuals in a timely manner.

ACTIVITIES NEEDED TO ACHIEVE THESE OBJECTIVES

- It is necessary to implement an additional layer of protection, a national cyber-shield, for the prioritised target group (e.g. vital services and infrastructure).
- It is necessary to analyse the target group of the state network from the perspective of national defence and security.
- Optimal centralised information security services must be provided to the public sector, such as protection against denial-of-service attacks and centrally managed devices in government agencies.
- Cooperation with the private sector is necessary in the area of threat intelligence sharing.
- A well-functioning nationwide direct notification and follow-up system for critical-impact security vulnerabilities must be established.
- The cyber threat awareness of information security managers and public sector employees of vital infrastructures must be continuously improved, taking into account the hardware and software in use in Estonia.
- It is necessary to extend preventative vulnerability scanning in a cost-effective way to key public services.

METRICS

- Information exchange with strategic partners has improved and is automated. – Yes/No.
- Target level for 2030: After receiving a notification about a critical-impact security vulnerability from CERT-EE, at least 80% of recipients (companies and institutions) implement a security update before follow-up inspection.



5 SHAPING A SECURE CYBER ENVIRONMENT IN ESTONIA AND GLOBALLY

Although Estonia is small in terms of population and territory, by acting purposefully, we can steer the cyber environment in a desirable direction not only domestically but also on a much broader scale. In addition to participating in EU legislative and political processes and shaping strategic courses we must also try to promote the same trends globally, through UN processes and well-targeted development cooperation.

Considering the pressures of introducing digitalisation and automation facing Estonian businesses, it is reasonable to address the importance of cybersecurity in all national measures to enable digitalisation and automation. There are still companies in Estonia that see cybersecurity and related issues as a technical issue that only IT specialists must deal with. They may not fully understand the importance of cybersecurity, or they may consider it irrelevant to their business operation. Both the public sector and cybersecurity organisations need to continue their efforts to explain the reality of cyber threats, the nature of control measures and the mechanisms for their implementation.

5.1 INTERNATIONAL CYBERSECURITY COOPERATION

SITUATION

Estonia's outstanding reputation as a digital state has opened many different doors for cybersecurity cooperation with other countries. Major digital development and cybersecurity events such as the Tallinn Digital Summit, the e-Governance Academy (eGA) annual conference, the CyCON conference show that Estonia continues to be a global hub for cybersecurity. Several delegations are visiting Estonia and Estonian representatives are expected to play an active, if not a leading role, in international organisations on cybersecurity issues. Demand for Estonia's experience and resources continues to outstrip the capacity to deliver. The cybersecurity cooperation with our closest allies (the United States, the United Kingdom, France, Germany and the Nordic-Baltic region) and international organisations (the EU, NATO, the UN, OSCE, etc), which is a priority for Estonia's foreign and security policy, has provided a good framework for launching an international coalition to assist Ukraine, such as the Tallinn Mechanism and the IT Coalition.

The increasingly tense geopolitical situation and the major role of cyberattacks in international conflicts (especially in Russia's military aggression against Ukraine) have clearly demonstrated that Estonia's previous policy of being an active provider of cybersecurity information and sharing its experience has strengthened important partnerships for Estonia. Alongside the exchange of information and experience, there are growing expectations for Estonia's involvement in international policy making (especially in the context of new technologies). International attributions of cyberattacks are also on the rise due to the heightened geopolitical situation. Estonia has participated in almost all the major attribution coalitions, but has not yet initiated any attribution statements itself.

In the context of Russia's aggression against Ukraine, Estonia continues to be recognised as one of the most active sherers of cyber threat intelligence, which has resulted in the

prevention of planned attacks against EU and NATO member states. We will continue to take a proactive approach and share cyber threat intelligence with like-minded countries and partners. Estonia's support to Ukraine during cyber conflicts strengthens our image as a reliable partner and shows that we can stand out positively among other small countries. Russia's aggression against Ukraine has proven that today, ensuring resilience in a physical armed conflict also requires ensuring resilience in a digital society. The lessons of the war in Ukraine are very important for Estonia's security. They will give Estonia, as one of the most digitally advanced countries in the world, together with Ukraine an opportunity to draw global attention to cybersecurity issues and through this to introduce solutions created in Estonia.

The provision of cybersecurity assistance has also reached a whole new level. Notably, with Estonia's active participation, the Tallinn Mechanism[33] and the IT Coalition were established in 2023 to coordinate international assistance in the civilian and defence sectors respectively. The Tallinn Mechanism is the main aid channel for all major donors. This is a good basis for creating new synergies between bilateral support provided by Estonia and multilateral support coordinated by Estonia.

Estonia has contributed to the development of the Caribbean region and the promotion of cybersecurity there. In 2019, the EU CyberNet project[34] was launched under the Information System Authority to coordinate EU cybersecurity development cooperation and has been a success. The Latin America and Caribbean Cyber Competence Centre (LAC4) has been established in the Dominican Republic to support international cooperation between countries in the region and the European Union. In addition to the first project grant, follow-on funding is guaranteed until 2026. In the region, Estonia is a digital state and a cybersecurity advocate, representing European values, and is part of a coalition balancing the influence of China and Russia. Estonia is also planning further activities related to developing cybersecurity capabilities in Africa and Southeast Asia that would create further synergies with ICT development cooperation projects.

Within the framework of the EU CyberNet project and under the guidance of the Information System Authority, an EU cyber development cooperation network has been established involving over 500 experts and 150 organisations. Such wide-ranging involvement is the basis for the success of development cooperation and the network has great potential to support future projects.

We will continue to actively contribute to keeping the European Union's internal market secure with an optimal administrative burden.

STRENGTHS AND WEAKNESSES

Estonia's cybersecurity cooperation with other countries has so far been mainly through bilateral initiatives or participation in the work of international organisations, which is distributed unevenly across different sectors and institutions. What is lacking is a systematic and coordinated approach and a holistic overview of cooperation opportunities and mechanisms.

We will continue to participate in international formats to exchange information and experience. Such cooperation is the basis for building better relations and trust to make a joint contribution to deterring cyberattacks and identifying the perpetrators. It is also important for Estonia to develop its own technical and analytical capabilities, so that in addition to supporting attribution statements by our allies, we are also able to initiate such statements ourselves. Otherwise, there is a risk that Estonia will lose the confidence

33 Tallinn mechanism, https://www.vm.ee/rahvusvaheline-oigus-ja-kuberdiplomaatia/digi-ja-kuberdiplomaatia/tallinna-mehhanism.
34 EU CyberNet, https://www.eucybernet.eu/.

to participate in such cooperation formats. Estonia does not see the need for a new cybersecurity convention, but we support the implementation of agreed cybersecurity provisions and standards and cyber governance measures.

Bilateral actions in support of Ukraine's defence are a clear reason why EU and NATO member states have trusted Estonia to coordinate resources and support. In the military field, Estonia is the lead country of the IT Coalition[35], and in the civilian field, the initiator of the Tallinn Mechanism. Successful activity in Ukraine is the basis for similar aid mechanisms in other crisis-stricken countries, offering Estonia opportunities for further engagement in both development cooperation and business diplomacy.

In Latin America and Africa, Estonia is leading the way on digital and cyber issues. In addition to Estonia's own financial contribution, we have also leveraged our activities through projects funded externally. The management of development cooperation projects such as those funded by the European Union will continue to be important to Estonia.

Developing services and cybersecurity competence in third countries could motivate Estonian cyber companies and ICT sector leaders to expand. We have created opportunities to export e-government services, but so far the take-up of such opportunities has been rather modest.

THE OBJECTIVES WE WANT TO ACHIEVE DURING THE STRATEGY PERIOD

- Estonia is a respectable and strong partner in the international arena.
- Estonia is guaranteed comprehensive international support and partner countries are ready to respond to cyberattacks against Estonia.
- Together with the main member states of the European Union and NATO, the readiness to respond has been put to the test during exercises.
- Estonia remains an important partner for Ukraine and supports the development of cyber defence.
- Exports of Estonian ICT companies have been strongly promoted in foreign markets.
- Estonia's activities to develop a secure digital society in Latin America and Africa support target countries' capacity to prevent and counter cyberattacks and suppress international cybercrime.
- The EU CyberNet is the European Union's effectively-operating cybersecurity development cooperation network with a long-term mandate.

ACTIVITIES NEEDED TO ACHIEVE THESE OBJECTIVES

- For priority countries, the focus must be on practical cooperation: regular exchange of threat landscapes, joint exercises and sharing of best practices, technologies and knowledge in the field of cybersecurity, including enhancing the cybersecurity of vital infrastructure and involving the private sector.
- Upon planning and developing Estonia's defence measures, it is necessary to take into account the threat assessments for high-risk countries in the cyber domain, as well as Ukraine's experience and lessons learned in connection with the Russian war of aggression.
- It is necessary to improve Estonia's technical and analytical capability to initiate attribution statements.

35 See more at https://www.kaitseministeerium.ee/et/uudised/eesti-luksemburg-ja-ukraina-kaivitasid-ramsteinis-ukraina-toetamiseks-it-koalitsiooni.

- The Ministry of Economic Affairs and Communications and the Ministry of Foreign Affairs must ensure national coordination of international cyber activities and participation in cyber cooperation between Member States.
- Estonia supports the development of cybersecurity in Ukraine, involving, where possible, Estonian ICT companies.
- Development of the EU CyberNet network will continue, and its long-term funding will be secured.

METRICS

- At least one cyber exercise has been carried out with all priority countries during the strategy period.
- Estonia has initiated at least one international public attribution in relation to cyber attacks.
- Increase in the number of countries joining the Tallinn Mechanism over the strategy period.
- Consistent growth of the total budget of the Tallinn Mechanism in the period from 2024 to 2027.
- 0.1% of the development cooperation activities budget is allocated to cybersecurity.
- Ten per cent (10%) of ICT development support is targeted at cybersecurity.

5.2 COMMUNITY AND SUCCESSION

SITUATION

The strength of Estonia's cybersecurity over the years has been the community mindset that everyone has to take responsibility for their own cybersecurity, but together we can do more. Estonia's small size is also our strength: community members know each other and sit side by side at conferences and in the 'sauna', even if their employers are competitors. This strength needs to be maintained and developed, as automation and machine-to-machine interaction alone will not enable the state to ensure the cybersecurity of citizens and society.

In implementing the strategy and more broadly ensuring cybersecurity in society, it is important to share knowledge within the country with think tanks, universities, research institutions and private sector partners. The state will use the capability of think tanks as strategic partners to develop Estonia's sectoral expertise and international cooperation.

The Information System Authority, state IT houses, ministries, universities, private companies, as well as foundations and non-profit organisations have been organising regular and well-known events for the community for years. The sustainability of private sector community events is largely driven by free market principles and participation fees, whereas sustainable community events organised by the state have a symbolic impact.

STRENGTHS AND WEAKNESSES

The Estonian cybersecurity community is a diverse and colourful bunch. Individuals and companies who may not be aware of the community-based approach should continue to be involved. This means that special attention should be paid to those who have been less represented in the community – it is a question of gender balance, regional differences and linguistic representation. Estonia is never alone in cyberspace, we are supported by a global cyber community, including European partners and contributors from further afield. Estonia's cyber community is the stronger the more diverse and open we are in our communication.

There is a shortage of cybersecurity specialists in Estonia, Europe and the rest of the world.

Therefore, special attention needs to be given to community development through educational initiatives in cooperation with partners. Awareness of cyber hygiene is only a starting point – here too, more cooperation with schools should also be undertaken, so that children learn to recognise threats lurking in cyberspace already in primary school. From basic school onwards, special attention needs to be given to sciences, career opportunities in computer sciences and the field of cybersecurity. Vocational and higher education usually responds to societal changes quite quickly, but in the field of cybersecurity we see the need for faster intervention. To build comprehensive cyber security defence and maintain the current level, it is important to ensure a steady influx of young people with specific cybersecurity skills and systematically expand educational opportunities in fields that might initially seem too complex to them, such as cryptograph and quantum computing y based on advanced mathematics. There is a need to increase the number of students in higher education who are knowledgeable about the cornerstone of cybersecurity – security solutions, including cryptography. It is also important to reach a situation where cyber hygiene and cybersecurity are an integral part of the curricula at all education levels in the coming years.

Cybersecurity as a career model has been a very male-centric field. Therefore, in order to widen the pool of professionals, new ways should be sought, alongside existing initiatives[36], to attract girls' interest in the field, especially at an age when they are starting to make career choices. The inclusion of women in lifelong learning through retraining programmes could also be one of the possible fast solutions to the labour shortage in the field of cybersecurity.

So far, Estonia has relied on solutions provided by private companies and domestic know-how to ensure cybersecurity. Innovation arises in the private sector, relying on investments and research institutions. Often, however, innovation remains on the shelf, as unlike an offensive state, Estonia (and Europe) may lack sufficient platforms to help innovative solutions reach the testing phase or even the market. More experimentation is needed, along with regular and targeted investment in education and research (including the development of future cybersecurity specialists), state guarantees or support, and the courage of private enterprises. In doing so, it is reasonable to follow the objectives set out in the Estonian Research and Development, Innovation and Entrepreneurship (RDIE) Strategy 2021–2035[37]. In addition, the state needs to focus on developing domestic expertise and raising awareness in the field of research and development to address the cybersecurity challenges of new technologies in the long term.

36 The organisations CyberTomorrow and Women in IT.

37 Estonian Research and Development, Innovation and Entrepreneurship (RDIE) Strategy 2021–2035 | Ministry of Education and Research (hm.ee)

THE OBJECTIVES WE WANT TO ACHIEVE DURING THE STRATEGY PERIOD

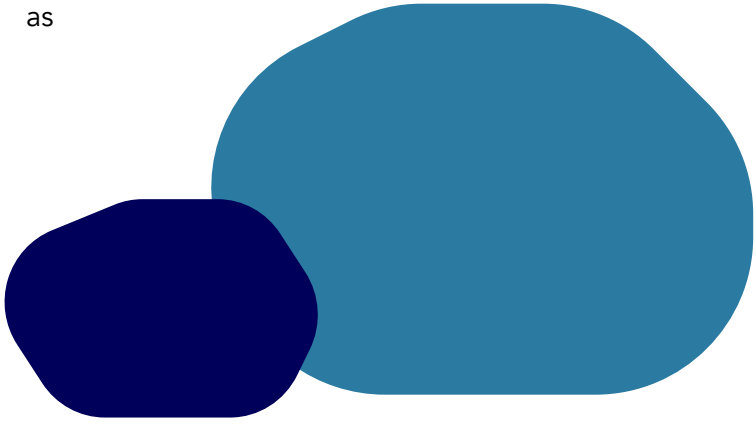
- Estonia's cyber community is open and diverse.
- The Estonian education system supports the development of the next generation of competent cybersecurity professionals.
- Cyber hygiene and cybersecurity are integrated into the curricula at all school levels.
- Local knowledge of future technologies is growing significantly based on the national objectives of the cybersecurity sector (set out in the RDIE Strategy 2021–2035) and an environment promoting innovation and entrepreneurship.

ACTIVITIES NEEDED TO ACHIEVE THESE OBJECTIVES

- It is necessary to encourage rotation between different public authorities and structures to promote the spread of the necessary competences and good practices and to generate new knowledge.
- The state must contribute to privately initiated community events.
- It is necessary to support the promotion of career choices in the fields of natural sciences, computer science, and cybersecurity, including among girls and women, by involving community members as influencers.
- In cooperation with the Ministry of Education and Research it is necessary to develop digital and cyber skills at all education levels.
- The Ministry of Economic Affairs and Communications, in cooperation with the Ministry of Education and Research, must prepare proposals on how to complement the curricula with topics of cyber hygiene and security.
- It is necessary to develop cybersecurity micro degree programmes.
- It is necessary to establish a framework for the development of domestic know-how through research and development funding and to set strategic priorities in the field of research.
- Local cybersecurity companies need to be strengthened through community-based activities and centrally shared threat intelligence.

METRICS

- Cybersecurity education has been included in education levels.
- Cyber hygiene and cybersecurity are integrated into the curricula at all school levels. – Yes/No.
- At least two Estonian higher education institutions offer cybersecurity micro degree programmes.



SUMMARY

Estonia's National Cybersecurity Strategy 2024–2030 'Cyber-conscious Estonia', has been renewed at a time when the global security situation has deteriorated significantly compared to what we are used to. Consequently, compared to the previous cybersecurity strategy in place for 2019–2022, the focus is primarily on strengthening security and safety. However, the development of cybersecurity has been addressed as comprehensively as possible, covering cybersecurity aspects from developing core security solutions and ensuring the functioning of vital services to broad prevention and ensuring adequate succession. In each of these areas, specific objectives have been set, the actions needed to achieve these objectives have been identified, and metrics have been provided to monitor the achievement of the objectives and the actions to be taken. The adoption of the strategy is followed by the preparation of the implementation plan.

Compared to the previous strategy, the objective to harmonise existing national defence, cybersecurity and data protection legislation, and to ensure adequate budgetary resources for basic national cybersecurity services at a level that allows for long-term planning, can be seen as a leap forward in ambition for this document. Based on national security and cyber threat landscape, we will prioritise enhancing the monitoring of vital services, increasing the level of continuity, future-proofing and crisis-proofing. We will achieve these objectives by setting minimum requirements for the organisation of information security and IT services, strengthening cybershield, developing and testing cybersecurity reserve and implementing the results of risk assessments on future technologies.

National cybersecurity management must address the target group's needs and prevent incidents and crises in enhancing the security of digital services. For the first time, a clear target has been set for the development of cybersecurity skills across all age groups in Estonia. An objective is set to improve centrally provided protection services, enhance cooperation with the private sector and continue to work on cyber hygiene and security in a more targeted and comprehensive way. The need, which has been set over time, to introduce a degree of differentiation in the requirements imposed on the target group of the Cybersecurity Act, considering the real impact of the services they provide on the functioning of society, has also been noted.

In addition, a more comprehensive cyber space threat landscape will be developed in partnership with internet service providers to enable faster threat prevention and mitigation. As did the previous cybersecurity strategy, it also stipulates that a comprehensive analysis of the national cybersecurity architecture must be carried out and decisions taken by 2027 at the latest. We must decisively move away from highly vulnerable legacy software and the increasing digital waste that is damaging the environment. Of course, daily efforts must also be made to ensure that cyber environment in Estonia is created in the European Union as well as in other like-minded countries around the world.

As this guidance document promises to clearly strengthen cyberspace safety and security by the end of the strategy period, the next strategy can focus more on those objectives that are not set for the public sector, but for example on supporting the private sector and start-ups to raise their cybersecurity level. The strategy is updated at least every two years, depending on the cyber threat landscape and the national security situation.

ANNEX 1. LIST OF INSTITUTIONS AND STAKEHOLDERS TO BE INVOLVED IN THE IMPLEMENTATION OF THE STRATEGY

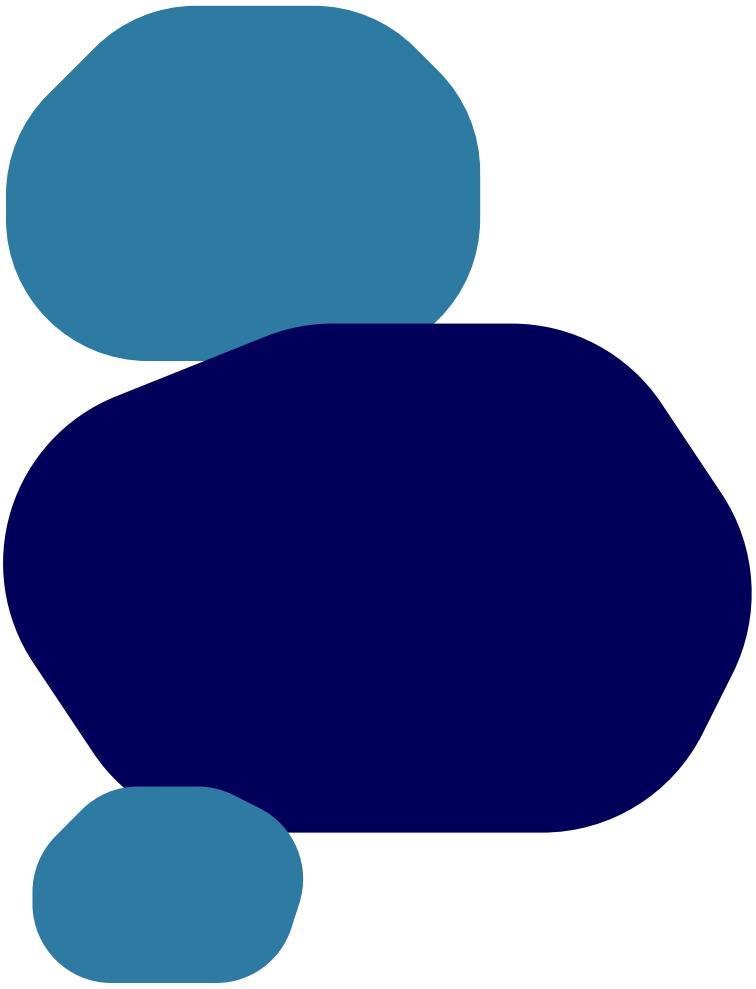
- The **Government Office** ensures that cybersecurity is integrated into national defence planning documents, plays a leading role in the development of crisis management policy and coordinates the activities of the relevant government agencies.
- The **Security Committee of the Government of the Republic** shapes the positions regarding security, national defence and crisis management policy in matters within the competence of the Government and coordinates the activities of the executive authorities in the planning, development and organisation of national defence and crisis management.
- The **Cybersecurity Council** operates under the Security Committee of the Government of the Republic and develops a coordinated position on cybersecurity issues between institutions and ensures monitoring of the implementation of the activities agreed in the cybersecurity strategy at least twice a year. The members of the Cybersecurity Council are all ministries, the Government Office and the Prosecutor's Office, as well as the Information System Authority, the Data Protection Inspectorate, the Police and Border Guard Board, the Estonian Internal Security Service, the Estonian Foreign Intelligence Service and the Consumer Protection and Technical Regulatory Authority. The perspective on national defence is represented alongside the Defence Forces, by the Defence League as a voluntary, militarily organised national defence organisation that organises military exercises.
- The main task of the CERT-EE Department of the **Ministry of Economic Affairs and Communications** is to manage, organise and coordinate the ensuring of nationwide cybersecurity, both nationally and internationally, to develop development plans and monitor their implementation and performance, to lead initiatives, to nurture the community and to shape legislation in the field of cybersecurity. Cybersecurity is also linked to the ministry's tasks in the development, support and organisation of digital society and digital development, economic and business activities, research and development, innovation, cross-border public services and other such services.
- The **Information System Authority** performs a wide range of tasks in the field of the state information system and cybersecurity, and is also the central cyber authority of the state within the meaning of the EU directive on security of network and information systems (the NIS directive). One part of the Information System Authority is the National Cyber Security Centre, which develops and advises on the implementation of information security measures, manages the cybersecurity of vital infrastructure and performs crisis management tasks in the event of large-scale cyber incidents, as well as monitoring cyber threats and risks, preventing critical cyber incidents and analysing developments in Estonian and international cyberspace. In addition, the Information System Authority provides services to communications service providers to secure the internet backbone system through RTIX, an internet exchange

point that interconnects Estonian internet networks and ensures inter-network traffic even when connections to other countries are disrupted. The Information System Authority also acts as a coordinating unit for industry, technology and research in the field of cybersecurity in Estonia and implements EU capacity building projects.

- The **Consumer Protection and Technical Regulatory Authority** is the national cybersecurity certification authority that manages the use of radio frequencies for data communications and connectivity, including in a national crisis situation (in times of increased defence readiness, state of emergency and state of war).
- The **Estonian Information and Communication Technology Centre** (Estonian IT Centre) is an agency managed by the Ministry of Economic Affairs and Communications and provides computer workstation and basic server infrastructure services in the country. The Estonian IT Centre provides services to around 25,000 public sector jobs.
- The **State Infocommunication Foundation** (RIKS) is a non-profit foundation under the Ministry of Economic Affairs and Communications, which provides communications services and special purpose and operational communications for state authorities and other state-funded institutions. In addition, RIKS provides operational radiocommunication services and maritime communication and telephone services for data centres and the state. In 2022, RIKS started to develop a satellite communications solution in Estonia to ensure the delivery of the country's essential services.
- The **Ministry of the Interior** ensures the implementation of the Internal Security Development Plan and related programmes and contributes to the creation of cross-sectoral cooperation and coordination mechanisms, as well as a unified situational awareness landscape.
- The **Information Technology and Development Centre of the Ministry of the Interior** (SMIT) ensures the management and development of information systems related to internal security. SMIT creates and manages the information systems needed for internal security, which are intended for use primarily by the Police and Border Guard Board, the Rescue Board, the Emergency Response Centre, the Estonian Academy of Security Sciences and the Ministry of the Interior, but also, for example, by the Ministry of Finance, the Ministry of Defence, the Ministry of Justice and the Estonian Transport Administration.
- The Police and Border Guard Board employs web police officers who monitor social media and work with youth safety organisations. Web police officers share information with the public about unsafe trends spreading online that can harm the well-being of young people and children.
- The **Cybercrime Office of the Central Criminal Police** is responsible for the detection, prevention and prosecution of cybercrimes.
- The competence of the **Estonian Internal Security Service** is to collect and process information on activities aimed at violently altering the constitutional order and territorial integrity of the state and to prevent and suppress intelligence activities against the state.
- The **Ministry of Defence**, in cooperation with the Estonian Defence Forces, the Defence League and the Foreign Intelligence Service, contributes to cyber security primarily through the implementation of activities related to military defence.

- The main tasks of the **Cyber Command of the Defence Forces** are the conduct of operations in cyberspace within the area of responsibility of the Ministry of Defence for the organisation of command support, the management and coordination of the development of cyber and command support capabilities, and the organisation of cyberweapon training.
- The **Cyber Defence Unit of the Defence League** (KKÜ) is a voluntary organised association created to protect Estonian cyberspace. Its membership includes professionals in key positions in cyber defence, patriotic people with IT skills, including young people, who are ready to contribute to the cyber defence of the country. The KKÜ works closely with the Information System Authority within the framework of the cybersecurity reserve.
- The **Estonian Foreign Intelligence Service** organises electronic information security, or cyber protection of classified IT systems, and monitors compliance with the requirements established for this purpose. The Service contributes significantly to the development of Estonia's national defence and security policy by gathering intelligence on external security threats to Estonia. The intelligence gathered by the Service provides the necessary early warning in the event of events that threaten us, thus forming the front line of Estonia's national defence.
- The **CR14 Foundation** is a state-owned company established by the Ministry of Defence, based on more than a decade of experience in the field of cybersecurity exercises, testing, validation and experimentation. To the extent agreed with the Ministry of Defence, CR14 also represents Estonia in its relations with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).
- The role of the **Ministry of Education and Research** in cyber literacy is certainly growing, as one of the development needs highlighted is that cybersecurity in the education system should be addressed as part of the development of digital literacy at all levels of education. The Education and Youth Board, operating within the area of government of the Ministry, manages the digital competence and digital security environment https://digipadevus.ee/.
- The **Ministry of Justice** is shaping a safe society through legal and crime policy. In the area of cybersecurity management, the role of the Ministry of Justice is to ensure that the legislation on public information and the keeping of databases and processing of data is up to date.
- The **Data Protection Inspectorate** is a government agency operating in the area of government of the Ministry of Justice, standing for good protection of personal data and access to public information, and is a shaper and supervisor of secure data processing in the digital world.
- The **Centre of Registers and Information Systems** is an agency operating under the Ministry of Justice that develops and manages important registers and information systems, such as the e-business register, e-notary, e-land register, court information system, criminal records database, e-file and the electronic Riigi Teataja.
- The **Ministry of Finance** is responsible for policy-making in related areas related to cybersecurity (eg legislation on virtual currency trading) and will ensure the involvement of the financial sector. The Ministry of Finance is involved in all policy areas through the budget processes.

- The **Financial Supervision Authority** establishes rules and legislation specifically related to the financial sector, exercises supervision, promotes information exchange and works with international partners to harmonise cybersecurity measures in the financial sector.
- **Eesti Pank** cooperates closely with the Financial Supervision Authority, also coordinating its activities with the European Central Bank, with the eurozone-wide guidelines prescribed there influencing the cybersecurity requirements and standards of Estonian financial institutions.
- The **IT Centre of the Ministry of Finance** provides IT services to the Ministry of Finance, the Financial Intelligence Unit, the Estonian Tax and Customs Board, Statistics Estonia, the State Shared Service Centre and the Estonian Information and Communication Technology Centre. In addition, it's portfolio includes external websites of various government agencies, for which host and management services are provided on a cloud-based government web-portal platform.
- The **Ministry of Foreign Affairs** is the leader of Estonia's digital and cyber diplomacy and the shaper of foreign policy. The Ministry coordinates Estonia's international activities in the field of cybersecurity and is in charge of coordinating development cooperation.



ANNEX 2. ACTION PLAN OF THE CYBERSECURITY STRATEGY

Priority (1 – priority, Cyber Security Council monitoring, 2 – important, 3 – basic hygiene); Responsible party (BOLD – main responsible party)

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
1. MANAGING THE DEVELOPMENT OF NATIONAL CYBERSECURITY				
1.1. NATIONAL MANAGEMENT AND POLICY-MAKING				
When developing the legal framework and making decisions that affect cybersecurity, it is necessary to take into account international trends, the prevailing threat landscape, the security situation, and other changes related to cybersecurity, information security, and data protection.	National cybersecurity is centrally and strongly managed and coordinated, all important parties are involved in policy making, it is regularly visible at the level of the Government of the Republic and the needs of internal security, data protection, national defence and the economy are considered.	**Ministry of Economic Affairs and Communications** in cooperation with other ministries	31.12.2025, continuous	3
+ International and national legislative cooperation approaches and positions are agreed upon and coordinated with the parties.		**Ministry of Economic Affairs and Communications** in cooperation with other ministries	31.12.2025	3
Together with partner institutions, the transposition of the NIS 2 Directive must be assessed, the existing legislation on cybersecurity and data protection (State Secrets and Classified Information of Foreign States Act, the Public Information Act, the Electronic Communications Act, etc) must be harmonised.	European Union and NATO directives have been transposed into Estonian law. Clarity of definitions, a balance between the requirements of national defence, freedom to conduct business and cybersecurity, technology neutrality, risk-basis, including minimisation of supply chain risks, and user-centricity are ensured in legislation. Sufficient time has also been provided for implementing the associated requirements.	**Ministry of Economic Affairs and Communications** in cooperation with other ministries	31.12.2025	3
+ Update the Cybersecurity Act, during which the circle of obliged persons and the proportionality of obligations and supervisory measures are assessed and organised, reducing supply chain and other relevant risks, for example by creating legal possibilities for the enforcement of measures that can be used to prevent incidents more promptly than before.	Cybersecurity obligations imposed on different target groups are proportional and purposeful, taking into account the activities of these groups and the impact of the related cybersecurity threat on society.	**Ministry of Economic Affairs and Communications**	31.12.2025	1
+ Harmonise the definitions and cybersecurity requirements in the Public Information Act, Electronic Communications Act, State Secrets and Classified Information of Foreign States Act and Cybersecurity Act into a single whole.		**Ministry of Justice, Ministry of Defence, Ministry of the Interior, Ministry of Economic Affairs and Communications**	31.12.2025	1

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
+ Assess the timely transposition of the EU General Data Protection Regulation and NATO information security regulations into Estonian legislation in cooperation with partner institutions.		**Ministry of Defence** in cooperation with other ministries (Ministry of Economic Affairs and Communications, Ministry of Justice)	31.12.2025	2
The establishment of a body or centre consolidating cybersecurity competences must be analysed and a decision based on that analysis must be made no later than 2027. The tasks and capabilities of subordinate institutions under ministries must be analysed from international (EU, NATO) and national legal aspects to enhance coordination in the field and cooperation between experts in the field. Proposals for the action plan are included in the implementation plans for the target groups.	National coordination and cooperation between experts in the field have been enhanced.	**Ministry of Economic Affairs and Communications** in cooperation with other ministries (Ministry of the Interior, Ministry of Defence) **Comment:** *Cybersecurity competences must, inter alia, be analysed in the context of both public and classified information.*	31.12.2027	1
The Cyber Security Council must regularly update and monitor progress towards the objectives of this strategy.	To obtain a central and up-to-date risk overview of developments in the field of cybersecurity, the Cyber Security Council has observed the implementation of the cybersecurity strategy and monitored and updated trends of development.	**Ministry of Economic Affairs and Communications** in cooperation with other ministries	31.12.2025, once per year	2
+ The implementation plan is updated/ supplemented in the fourth quarter of each year.	The implementation plan has been supplemented, prioritised, and responsible parties have been assigned.	**Ministry of Economic Affairs and Communications** in cooperation with other ministries	31.12.2025	1
+ The implementation plan of the cybersecurity strategy is taken into account when preparing the work plans of institutions.	The activities have been included in the work plans of the responsible institutions.	All ministries	31.12.2025	1
+ At the beginning of the new year, the priority activities and responsible parties requiring monitoring by the Cyber Security Council for the upcoming year are approved, and an overview of the previous year's results is provided.	The implementation plan has been monitored.	**Ministry of Economic Affairs and Communications** in cooperation with other ministries	31.12.2025	1
+ Updating the cybersecurity strategy.	The cybersecurity strategy is updated every two years.	**Ministry of Economic Affairs and Communications** in cooperation with other ministries	31.12.2026	1

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
1.2. FUNDING OF CYBERSECURITY				
Analyse the implementation of the cost model in Estonia as commissioned by the Ministry of Economic Affairs and Communications, including potential activities, metrics, target levels to achieve the objectives. A supranationally agreed cybersecurity cost model and action plan for ensuring funding have been established.	Ensure the adequacy of budgetary resources (in the form of base funding) for the secure operation and development of services. The funding of basic cybersecurity services is provided from the state budget.	**Ministry of Economic Affairs and Communications**	31.12.2025	1
+ According to the agreed model and target level, cybersecurity needs to ensure sustainability have been submitted to the SBS.	The financing of the state's basic cybersecurity services is ensured at a level that allows for long-term planning. The ICT budget includes the expenditure for the cybersecurity component. The funding for the state's basic cybersecurity services is consistently ensured at the agreed level, allowing for long-term planning.	All ministries	31.12.2026	3
Negotiate and agree with the responsible parties of the Ministry of Economic Affairs and Communications and the Ministry of Education and Research in charge of the RDIE Strategy on the long-term support for improving cybersecurity in enterprises and educational institutions through the RDIE Strategy, based on the objectives of the Cybersecurity Strategy 2024–2030 'A more cyber-conscious Estonia'.	The RDIE Strategy includes a measure to support the improvement of cybersecurity in enterprises and educational institutions with a sustainable budget. **Comment:** *The long-term plan of the RDIE should be based on the RDIE roadmap 'Digital solutions across all areas of life'. Supporting the Information System Authority in applying for Digital Europe support measures.*	**Ministry of Economic Affairs and Communications (area of economy and innovation), Ministry of Education and Research**, Ministry of Finance	31.12.2025	2
+ Supporting the Information System Authority in applying for Digital Europe support measures at the launch of Phase II of the Cybersecurity Level Mapping and Development Grant.	Estonia's contribution to launching the Phase II of the Cybersecurity Level Mapping and Development Grant has been guaranteed. The support measure for mapping and developing the cybersecurity level of SMEs has been continued. **Comment:** *The Information System Authority, in cooperation with the Ministry of Economic Affairs and Communications and the Estonian Business and Innovation Agency, is applying for the continuation of the support measure under the Digital Europe programme.*	Ministry of Economic Affairs and Communications, **Information System Authority**, Estonian Business and Innovation Agency	31.12.2025	3
Development of the conditions for granting and using the Government ICT reserve funds (TAT directive), assessment methodology, and updating of the application form.		**Ministry of Economic Affairs and Communications**	31.12.2025	3

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
Support measure for the transposition of NIS2 for subjects of the Cybersecurity Act: development of conditions for granting and using support (TAT regulation), launch of call-based funding (development of assessment methodology, application form, notification of applicants, organisation of information days in cooperation with the 2nd level intermediate bodies, etc).		**Ministry of Economic Affairs and Communications**	31.12.2025	3
Analyse existing support schemes and development plans to identify more effective ways to support the development of sustainable cybersecurity.		**Ministry of Economic Affairs and Communications**	31.12.2026	1
Definition of cybersecurity support areas (analysis of where the market functions effectively and where state support is needed). Minimum and maximum requirements for support of areas (analysis in the perspective of 2025 to 2035).	The analysis has been completed. The main support areas (state intervention areas) for the 2025–2035 period have been defined. The minimum need for state support has been determined by areas and target groups.	**Ministry of Economic Affairs and Communications**	31.12.2025	1
		Comment: *The analysis serves as input for mapping the needs and planning the funding period for the 2028+ Structural Funds funding period.*		
2. ENHANCING SOCIETAL RESILIENCE				
2.1 UP-TO-DATE THREAT LANDSCAPE				
The Ministry of Economic Affairs and Communications and Information System Authority must agree with ISPs on how it would be most practical to create a cyber-threat landscape in an anonymous form, taking into account the fundamental rights of individuals and the freedom to conduct business.	In order to prevent, detect and counter cyber threats as quickly as possible, the Information System Authority creates a comprehensive threat landscape of the Estonian cyberspace, which will enable to provide better preventive support to different groups of society. The relevant rights and obligations of institutions and undertakings contributing to the creation of a nationwide threat landscape have been agreed upon.	**Ministry of Economic Affairs and Communications, Information System Authority**	31.12.2026	1
		Comment: *See also 1.2 Cyber competency analysis.*		
+ More comprehensive public threat landscape (in collaboration with ISPs and the Police and Border Guard Board and Consumer Protection and Technical Regulatory Authority)	Institutions, companies, and regular users are more aware of the situation in cyberspace thanks to a more comprehensive threat landscape and action guidelines, have been guided on implementing protective measures, and institutions understand better why and how to protect their information from cyber threats. The nationwide cyber threat landscape reaches target groups in a more comprehensive form than before.	**Information System Authority**, Police and Border Guard Board, Consumer Protection and Technical Regulatory Authority, Estonian Foreign Intelligence Service, Estonian Internal Security Service	31.12.2026	2
		Comment: *The public threat landscape within the area of responsibility of the Estonian Foreign Intelligence Service and Estonian Internal Security Service.*		

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
+ Involvement of the Consumer Protection and Technical Regulatory Authority (TTJA) in the cyber threat landscape to create situational awareness of radio frequency interference and communications continuity.	The cyber threat landscape encompasses all sectors. The cooperation between the Consumer Protection and Technical Regulatory Authority and the Information System Authority has been agreed upon.	**Consumer Protection and Technical Regulatory Authority, Information System Authority**	31.12.2025	3
+ Sharing a more comprehensive threat landscape and protective measures with policymakers and the country's strategic leadership.	The Government of the Republic, the Riigikogu, ministries and state agencies are more aware of the situation in cyberspace thanks to a more comprehensive threat landscape. Governance and policymaking are based on the nationwide cyber threat landscape.	**Ministry of Economic Affairs and Communications, Information System Authority,** Ministry of the Interior, Estonian Internal Security Service, Ministry of Defence, Government Office	31.12.2025	3
Comment: *The nationwide cyber threat landscape is consolidated by the Ministry of Economic Affairs and Communications, which may also include classified information analysis based on input from other institutions. The Ministry of Economic Affairs and Communications sends the national cyber threat landscape to the Government Office.*				
2.2 COMPREHENSIVE PREVENTION				
In cooperation with the Ministry of Education and Research and the Ministry of Culture, there is a need to develop digital and cybersecurity (including cryptography) skills across all age groups.	As a result of comprehensive prevention, Estonian society is cyber-aware. All those active in cyberspace have the necessary knowledge to deal with threats and prevent incidents.	**Ministry of Economic Affairs and Communications,** Ministry of Education and Research, Ministry of Culture, Information System Authority	31.12.2027	2
Comment: *To achieve quantum-resistance, we need to significantly increase the number of cybersecurity and cryptography experts.*				
+ Regularly assess the effectiveness of training and educational programmes and adjust curricula according to the target group, technological developments, and taking into account the threat landscape and strategic changes.		Ministry of Economic Affairs and Communications, Ministry of Education and Research, Ministry of Culture, **Information System Authority**	31.12.2026, once per year	3
It is necessary to assess the trends in cybercrime based on impact, develop corresponding technological capabilities and skills accordingly, and implement other measures to protect society and raise awareness.	The number of cybercrimes in Estonia has decreased as a result of comprehensive prevention and cooperation between Information System Authority and Police and Border Guard Board.	**Ministry of the Interior,** Police and Border Guard Board	31.12.2025, once per year	1
+ Develop a metric for assessing trends in cybercrime.	A metric has been developed to assess cybercrime.	Ministry of the Interior, **Police and Border Guard Board**	31.12.2025	3

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
Society needs to be aware of the prevailing cyber threats and the responsibility of each individual in reducing them. Share advice on mitigating risks.	The level of cyber hygiene among the population has increased, and the number of residents who have taken no steps to ensure their personal security or privacy in cyberspace has decreased.	Ministry of Economic Affairs and Communications, **Information System Authority**	31.12.2025, continuous	3
+ Updating itvaatlik.ee according to the needs of the target group and the threat landscape.	itvaatlik.ee is a prevention portal where all the most important target groups – businesses, individuals, and the public sector – can easily find information on how to protect themselves in cyberspace. The usage statistics of itvaatlik.ee grow by at least 10% annually.	**Information System Authority**	31.12.2025	2
+ The analysis, statistics, and regular overviews of cyber incidents have been compiled and are accessible to the target group.		**Information System Authority**	31.12.2025, continuous	3
+ In cooperation with the private sector, it is necessary to develop and implement measures to improve the cyber awareness of SMEs.	The awareness of key individuals in the public and private sectors, including SMEs, has increased regarding the importance of cybersecurity in ensuring the main activities of the organisation.	**Information System Authority**	31.12.2025	3
To gain access to devices centrally managed by the public sector, the user must first pass a cyber test. The requirement for cyber tests is to be established in the form of minimum requirements.	Cybersecurity awareness tests are widely used among employees of state agencies, providers of vital services, and businesses to assess and enhance their cybersecurity knowledge. Those who complete the cyber tests are able to recognise cyber threats and behave securely in cyberspace while carrying out their core tasks. Cybersecurity Act subjects have established requirements within their organisations for passing the cyber test.	All ministries	31.12.2026	3
2.3 IMPLEMENTATION OF THE INFORMATION SECURITY STANDARD				
There is a need to reinforce the positive image of E-ITS through sector-specific advocates. Expand the provision of information security standard training by involving the private sector. The Information System Authority's department for Critical Information Infrastructure Protection organises sectoral information days, where E-ITS is introduced, among other topics.	Organisations and their leaders are aware of their information security obligations and consciously implement security measures based on a risk-based approach, and also require the same from their supply chain.	**Information System Authority**, Ministry of Economic Affairs and Communications in cooperation with other ministries	31.12.2025, continuous	3

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
+ Updating the E-ITS in accordance with international best practices, technological trends and the national threat landscape.	E-ITS is updated annually in cooperation with the community. This is a community standard in accordance with Estonian legislation, which takes into account new threats and technological developments.	**Information System Authority**	31.12.2025, once per year	3
+ Develop solution(s) to automate the implementation of E-ITS measures, to facilitate the implementation of E-ITS in less mature institutions and organisations. Opportunities must be created for organisations to measure the implementation and performance of E-ITS and, on the basis of the measurement results, to assess the effectiveness of the implementation of E-ITS across different types of institutions.	The implementation of E-ITS in institutions is facilitated, automated and a national risk assessment will be created to assess and compare different sectors. Support tools have been created to assist less mature subjects.	**Information System Authority**	31.12.2026	1
		Comment: *Automated self-assessment solutions must facilitate auditing and possible differentiation and can also be used to optimise supervision. See also section 2.5.*		
Investigate and, based on the analysis, create a compliance mechanism between E-ITS and the ISO/IEC 27001 certification, and apply for international recognition for E-ITS.	Organisations that need to prove the implementation of the information security management system at an international level can also do so by implementing E-ITS and passing an E-ITS audit.	**Ministry of Economic Affairs and Communications, Information System Authority, Consumer Protection and Technical Regulatory Authority, SK ID Solutions AS**	31.12.2026	2
Comment: *If the interaction between the State Secrets and Classified Information of Foreign States Act and Cybersecurity Act is enhanced (see sections 1.1 and 2.4), the application of the compliance mechanism and recognition in the field of state secrets should also be analysed.*				
2.4 SECURE BASIC ARCHITECTURE AND MODERN SECURITY PRINCIPLES				
In making funding requests and decisions, the reduction of legacy must be prioritised.	By the end of the strategy period, the dependence of the state's critical databases and services on legacy has been reduced by at least half. By 2030, the dependence of public services on legacy for services consumed through the public network will have decreased to 20%.	**Ministry of Economic Affairs and Communications**, Ministry of Finance	31.12.2025, continuous	3
		Comment: *Use the results of the E-ITS implementation/self-assessment tool for measurement.*		
Public sector institutions must set targets to reduce digital waste and participate in annual digital cleanup days.	Public sector institutions systematically reduce digital waste. The amount of data on disks and the proportion of legacy has been reduced, unnecessary or duplicate information has been deleted.	All ministries	31.12.2025, once per year	3

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
When developing new state digital services and updating existing ones, the principles of security by design and the implementation of non-functional requirements must be followed. This means that security risks are taken into account in the design and development of services at each stage and the life cycle of the service or product is planned comprehensively, in line with the E-ITS measures.	Training courses at the Digital State Academy support the implementation of E-ITS. The development of an E-ITS automation tool enables the creation of an implementation plan that ensures the minimum requirements for lifecycle development and security policies and IT service organisation. Lifecycle-based development and security policies are implemented in the public and private sectors.	**Information System Authority**, implementation: all ministries **Comment:** *The automated E-ITS tool generates sample documents according to the specific characteristics of the implementing organisation. Training sessions and workshops for the implementation of E-ITS continue at the Digital State Academy, covering also the topic of security by design.*	31.12.2025	3
Streamlining and updating the minimum requirements for information security and IT service management.	The public sector has established clear information security requirements and minimum IT service management requirements (centralised management, centrally regulated use of public cloud services, etc), the updating of which is regularly monitored by the Cyber Security Council.	**Ministry of Economic Affairs and Communications, Information System Authority** **Comment:** *See also section 1.1.*	31.12.2025	3
Gradually, the zero-trust security principle must be implemented, the approach of which must begin with the architecture of the application.	Throughout the entire strategy period, central government agencies are moving towards a zero-trust security architecture. By 2030, an advanced level (the Advanced level in the maturity model used by CISA) will be achieved according to the zero-trust architecture maturity model.	Ministry of Economic Affairs and Communications, all ministries, Information System Authority, Estonian IT Centre, other IT houses;	31.12.2028	2
+ Creating the concept of the zero-trust security principle and agreeing on the implementation principles. **Comment:** *The questions left unanswered are: Who will develop and what will the security architecture be? How and with what resources will the objective be achieved? Who and how will it be supervised? What obligations/activities are additionally involved?*	Clear principles and responsibilities for implementing the zero-trust security principle.	**Information System Authority**, Estonian IT Centre along with other IT houses.	31.12.2026	1
+ Implementation of the concept of the zero-trust security principle.	The level 'Initial' in the maturity model used by CISA.	All ministries, all IT houses;	31.12.2028	2
During the strategy period, the compatibility of the state's most widely used digital services with the new generation internet protocol IPv6 must be assessed, and a roadmap for implementing IPv6 in the public sector must be created. Compatibility must also be ensured in classified networks.	The capability to prevent security incidents in digital services is continuously updated through the implementation of the IPv6 internet protocol. Outdated technologies will be removed from use. By 2030, at least 80% of publicly consumed state e-services will be on the IPv6 network.	Ministry of Economic Affairs and Communications, **Information System Authority**, Ministry of Defence **Comment:** *Concept and roadmap*	31.12.2025	1

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
Establish scientific competence centres for the implementation of cloud technologies and cryptographic solutions to ensure the quantum-resistance of data.	In the state, the foundation for the establishment of scientific competence centres has been laid. Increase national knowledge in cryptography and competence in the implementation of cloud services.	**Ministry of Economic Affairs and Communications, Ministry of Defence, Ministry of Education and Research, State Infocommunication Foundation**	31.12.2027	2
+ Cloud services competence centre **Comment:** *Additional budget requirement*	Establishing and sharing competence in the implementation of cloud services.	**Ministry of Economic Affairs and Communications, Estonian IT Centre**	31.12.2026	1
+ Cryptography competence centre **Comment:** *The sustainable operation of the competence centre is ensured through the relevant ministry's budget. The exact format, location, and other details of the competence centre will be determined based on the analysis, which is expected to be completed in 2026 as part of the 'Cryptographic solutions assessment project'.*	In Estonia, the capability to develop and share cryptography competence is centrally consolidated. The competence centre is capable of assessing cryptographic security solutions and contributes to the adoption of quantum-resistant cryptography in the state.	**Ministry of Defence, Estonian Foreign Intelligence Service**, Ministry of Economic Affairs and Communications, Information System Authority, Consumer Protection and Technical Regulatory Authority, State Infocommunication Foundation	31.12.2027	2
+ Cryptographic solutions assessment project	A capability mapping has been created, along with proposals for developing Estonia's cryptography competencies.	Ministry of Defence, **Estonian Foreign Intelligence Service**	31.12.2026	1
A methodology for the assessment of data and communication security solutions containing cryptography is agreed and approved nationally and its implementation is addressed. **Comment:** *A comprehensive approach to the protection of public, internal, and classified information.*	National information is maintained with approved/certified quantum-resistant communications security (including cryptographic) solutions. The underlying architecture is based on quantum cryptographic solutions, the state has strong cryptographic knowledge, and there is a cryptography competence centre.	**Ministry of Defence, Estonian Foreign Intelligence Service**, Ministry of Economic Affairs and Communications, Information System Authority, Consumer Protection and Technical Regulatory Authority, State Infocommunication Foundation	31.12.2027	1

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
Investigate technological trends and future technologies, including artificial intelligence and quantum technologies, share best practices, and develop measures for their implementation.	Be prepared for the arrival of new technologies (including quantum computing), taking into account technological trends. Research and development studies and analyses have been carried out and the results can be implemented. (At least 2 studies per year) Estonia has the necessary capability and interest for developing quantum software to be part of the European quantum ecosystem.	**Ministry of Economic Affairs and Communications, Ministry of Defence** **Comment:** *Monitoring of extensive scientific research at the Cyber Security Council.*	31.12.2025, continuous	2
Implementation of the national cybersecurity certification authority.	Estonia has the capability to issue and supervise certificates that comply with the European cybersecurity certification regulation.	**Consumer Protection and Technical Regulatory Authority,** Estonian Accreditation Centre	31.12.2026	2
Implementation of cybersecurity requirements for radio equipment with internet capabilities and market supervision under RED DA.	Radio equipment with internet capabilities sold on the Estonian market complies with the essential cybersecurity requirements imposed on them.	**Consumer Protection and Technical Regulatory Authority**	31.12.2025	3
Analyse the possibilities to find the owner and operator for secure data communications (ATA).	A new operator will be found for interagency secure data communication (ATA). A new owner has been found for ATA, who will manage the ATA, including finding a new operator.	**Ministry of Defence, Ministry of the Interior,** Ministry of Economic Affairs and Communications **Comment:** *According to the 2022 explanatory memorandum of the Security Authorities Act, the task remains within the area of government of the Ministry of the Interior and the Ministry of Defence.*	31.12.2025	1
Opportunities and regulations have been created for processing restricted-level state secrets in the public cloud. **Comment:** *see also section 2.4, the row of centres of competence.*	The processing of restricted-level of state secrets in the public cloud is allowed, taking into account the NATO cloud security implementation directive.	**Ministry of Justice,** Ministry of Defence (Estonian Foreign Intelligence Service), Ministry of Economic Affairs and Communications, Ministry of the Interior (Estonian Internal Security Service), Estonian IT Centre	31.12.2027	1

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
2.5 ENHANCING THE CRISIS RESILIENCE OF VITAL SERVICES				
It is necessary to analyse the possibilities for identifying the owners of critical network and information systems based on security vulnerabilities and informing them directly.	The monitoring of security vulnerabilities in vital services has been enhanced, and a direct notification system for the owners of critical network and information systems has been established. The cyber incident has not caused any long-term disruption to vital services.	Ministry of Economic Affairs and Communications, **Information System Authority**	31.12.2026	1
+ Owners of critical network and information systems must be obligated to eliminate the security vulnerabilities of the network and information systems specified in the threat notifications using the prescribed measures.	Vital infrastructures and services are equipped with security measures based on national security aspects, enabling them to withstand both current and future threats. The recommendations provided by the Information System Authority (RIA) for eliminating identified security vulnerabilities have been fulfilled without delay. The operation of all critical information systems has been restored within 24 hours after the incident.	**Ministry of Economic Affairs and Communications, Information System Authority** **Comment:** *The task is related to the creation of a transnational SoC.*	31.12.2025	2
+ Analysis of the creation of monitoring capability – budget and target group prioritisation. Establish a central monitoring capability for overseeing industrial automation networks and equipment.	Industrial automation devices are monitored, and their protection has been enhanced. A central monitoring system for industrial automation networks and equipment is in use, covering all prioritised vital and essential service providers.	Ministry of Economic Affairs and Communications, **Information System Authority**	31.12.2025	1
+ Agree on the methodology and criteria on the basis of which cybersecurity requirements are differentiated, taking into account the impact of the service on the functioning of society.	Smaller organisations have outsourced the services of an information security officer or hired an employee with information security skills. A solution has been developed to simplify the implementation and monitoring of measures through automation. Information security requirements and minimum requirements for IT service management have been established based on unified principles.	Ministry of Economic Affairs and Communications, **Information System Authority** **Comment:** *See also section 2.3.*	31.12.2025	1
The legal framework for crisis management must be streamlined, ensuring that crisis measures in the cyber domain are proportional to other measures.	The streamlined crisis management model takes into account national capabilities, interdependencies between services, priorities, and escalation options to ensure national (cyber)security.	**Government Office**, all ministries **Comment:** *The objective is for us all to have a shared threat landscape, situational awareness and action guidelines aligned with scenarios.*	31.12.2025	3

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
+ Gradually reduce insecure technologies and supply chain risks in the procurement of critical infrastructure. Establish requirements for the protection of critical infrastructure in the Public Procurement Act.	Exclusion of technology from high-risk countries to protect critical infrastructure. The Public Procurement Act has been amended and excludes the use of unreliable technology.	**Ministry of Finance**, all ministries	31.12.2025	1
+ Based on national capabilities and scenarios, specify the continuity requirements for ensuring the crisis resilience of vital and digital services and begin their implementation. In preparing for crisis situations, solutions independent of the cybersecurity component must be envisaged.	The operational continuity of essential digital services must be ensured, both in peacetime and during crises. Regulations have been established to ensure operational continuity during crises and to consider solutions independent of the cybersecurity component.	**Government Office**, all ministries **Comment:** *Crisis situations are considered to include worst-case scenarios (eg, armed conflict, hybrid conflicts, epidemics, disruption of external connections, large-scale cyberattacks, etc).*	31.12.2025	3
+ In order to ensure operational continuity, manual control must be retained as an alternative for critical systems, including industrial automation.	For new critical industrial automation systems, the option for manual control is ensured as an alternative where justified.	**Information System Authority**	31.12.2025	2
It is necessary to test the crisis resilience of digital services and the functioning and involvement of the cybersecurity reserve to determine the limits of national capabilities, resource qualifications, and skill levels.	A cybersecurity reserve concept and crisis involvement guidelines have been established, which are regularly tested (once per year) and updated. The cybersecurity reserve concept is implemented, and the operation and involvement of the cybersecurity reserve in crisis management are seamless.	**Information System Authority**	31.12.2025, continuous	1
+ A nationwide exercise is held annually to practise involving the cybersecurity reserve.		**Information System Authority**	31.12.2025, once per year	2
The state must have a well-functioning classified communications network, including for communication with foreign partners.	In times of crisis, the authorities concerned will be able to communicate with both national and foreign partners. Important national defence-related information reaches important target groups. **Comment:** *Also related to the ATA network, see also section 2.4. Government Office has responsibility as the national coordinator, and the Ministry of Economic Affairs and Communications as the organiser of state communications.*	**Government Office, Ministry of Defence, Ministry of Economic Affairs and Communications**	31.12.2027	3
3. STRONG CYBER-SHIELD				
Implement an additional layer of protection (CYBER-SHIELD) for the prioritised target group.	The target group for CERT's protective measures is clearly prioritised. Information exchange with strategic partners is more efficient and automated. The higher-priority target group is under additional protection.	**Information System Authority**	31.12.2027	1

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
+ It is necessary to analyse the target group of the state network from the perspective of national defence and security.	Based on the analysis, a decision will be made regarding why and to whom the state network service should be provided.	**Information System Authority** in cooperation with other ministries (Ministry of Economic Affairs and Communications, Ministry of Defence, Ministry of the Interior)	31.12.2027	1
+ It is necessary to implement an additional layer of protection, a national cyber-shield, for the prioritised target group (eg, vital services and infrastructure).	The nationwide Information Security Monitoring Centre (SOC) has been established and is operational, and in contact with strategic partners.	**Information System Authority**	31.12.2027	2
The cyber threat awareness of information security managers and public sector employees of vital infrastructures must be continuously improved, taking into account the hardware and software in use in Estonia. To protect vital infrastructure, monitoring and the creation of a situational overview must be enhanced, and awareness-raising training sessions and cyber tests must be provided. Resilience must be tested through exercises. In accordance with Article 11(3)(a) of the NIS2 Directive, the possibility to extend automated monitoring must be established, allowing all organisations in the target group to request automated monitoring upon application.	The likelihood of successful cyberattacks against Estonian companies has decreased thanks to better sectoral visibility, automated monitoring and threat notification. Protective measures to mitigate threats are developed and provided by the local cybersecurity sector.	**Information System Authority**	31.12.2026	3
A well-functioning nationwide direct notification and follow-up system for critical-impact security vulnerabilities must be established.	Information about critical-impact security vulnerabilities and instructions for eliminating them reach vital infrastructure, Estonian companies, and individuals in a timely manner. Target level for 2030: After receiving a notification about a critical-impact security vulnerability from CERT-EE, at least 80% of recipients (companies and institutions) implement a security update before follow-up inspection.	**Ministry of Economic Affairs and Communications, Information System Authority** **Comment:** *Ministry of Economic Affairs and Communications – regulatory amendments, Information System Authority – enhanced monitoring*	31.12.2030	1
Cooperation with the private sector is necessary in the area of threat intelligence sharing.	Important partners are linked to the national monitoring centre. Information exchange with strategic partners is efficient and automated.	**Information System Authority** **Comment:** *Information exchange between the public and private sectors has been enhanced.*	31.12.2027	2

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
Optimal centralised information security services must be provided to the public sector (the state), such as protection against denial-of-service attacks and centrally managed devices in government agencies.	The state provides support to prevent the realisation of cyber incidents and cyber threats (eg, threat assessments, basic penetration tests). The information security level of the public sector has improved.	**Information System Authority** **Comment:** *For centralised information security services, the target group is prioritised based on threat assessments.*	31.12.2027	3
+ The state provides support for protection against activities from hostile states and associated groups, as well as for preventing the realisation of cyber threats.	Protection against cyber threats from hostile countries has been enhanced.	**Information System Authority** together with other security agencies **Comment:** *Penetration testing is offered upon request based on risk assessment.*	31.12.2025, continuous	3
4. SHAPING A SECURE CYBER ENVIRONMENT IN ESTONIA AND GLOBALLY				
4.1 INTERNATIONAL CYBERSECURITY COOPERATION				
For priority countries, the focus must be on practical cooperation: regular exchange of threat landscapes, joint exercises and sharing of best practices, technologies and knowledge in the field of cybersecurity, including enhancing the cybersecurity of vital infrastructure and involving the private sector.	Estonia is a recognised and strong partner on the international stage. Together with the main member states of the European Union and NATO, the readiness to respond has been put to the test during exercises. At least one cyber exercise has been carried out with all priority countries during the strategy period. At least one international cyber exercise is organised annually in Estonia (eg, LockedShields/ CrossedSwordss). Cyber cooperation is enhanced following the exercise. Regular bilateral meetings are held with all priority countries.	Information System Authority and Ministry of Defence – exercises, Ministry of Economic Affairs and Communications, Information System Authority and Ministry of Foreign Affairs – international cooperation.	31.12.2025, an exercise at least once a year	3
Upon planning and developing Estonia's defence measures, it is necessary to take into account the threat assessments for high-risk countries in the cyber domain, as well as Ukraine's experience and lessons learned in connection with the Russian war of aggression.	Comprehensive international support for Estonia is ensured, and partner countries are prepared to respond to cyberattacks directed against Estonia. Clear agreements and plans are in place for handling attacks against Estonia and implementing assistance from partner countries, and these have been tested during exercises.	Information System Authority and Ministry of Defence – exercises, Ministry of Economic Affairs and Communications, Information System Authority and Ministry of Foreign Affairs – international cooperation.	31.12.2025, an exercise at least once a year	3
The Ministry of Economic Affairs and Communications, the Ministry of Defence and the Ministry of Foreign Affairs must ensure national coordination of international cyber activities and participation in cyber cooperation between Member States.	Targets and messages in international communication have been agreed upon and coordinated at a supranational level.	Ministry of Economic Affairs and Communications, Information System Authority, Ministry of Defence and Ministry of Foreign Affairs – international cooperation.	31.12.2025	3

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
Analyse and improve Estonia's technical and analytical capability to initiate attribution statements in cooperation with partners. **Comment:** *https://www.postimees.ee/8090985/video-fotod-ja-blogi-prokuratuur-kapo-ja-politsei-andsid-ulevaate-gru-kuberrunnakutest*	Estonia has an analysis and an action plan (with partners) for initiating cyber-attack attribution statements.	**Ministry of Foreign Affairs** in cooperation with other ministries (Ministry of Economic Affairs and Communications, Ministry of Defence, Ministry of the Interior), Information System Authority, Estonian Internal Security Service	31.12.2026	3
Estonia supports the development of cybersecurity in Ukraine, involving, where possible, Estonian ICT companies. Exports of Estonian ICT companies have been strongly promoted in foreign markets.	Estonia remains an important partner for Ukraine and supports the development of cyber defence. Consistent growth of the total budget of the Tallinn Mechanism and the participation of Estonian companies in the period from 2024 to 2027. Within the framework of the IT Coalition, the creation of a secure and resilient IT infrastructure and cyber defence capabilities have been developed for the Ministry of Defence and the Armed Forces of Ukraine of Ukraine to ensure the technological advantage of the Armed Forces of Ukraine on the battlefield.	**Ministry of Foreign Affairs**	31.12.2025	3
Estonia's activities to develop a secure digital society in Latin America and Africa support target countries' capacity to prevent and counter cyberattacks and suppress international cybercrime.	The development of a secure digital society has been supported within the framework of global development cooperation objectives. 0.1% of the development cooperation activities budget is allocated to cybersecurity.	**Information System Authority, Ministry of Foreign Affairs** **Comment:** *The cooperation is carried out in accordance with the Ministry of Foreign Affairs development cooperation priorities and existing initiatives.*	31.12.2025	3
+ The development of the EU CyberNet network will continue, and its long-term funding will be secured.	Estonia's ICT development cooperation activities have been substantiated and consistently leveraged by externally funded projects.	**Information System Authority, Ministry of Foreign Affairs**	31.12.2025	3
Comment: *EU CN is included in the strategy and brings funds and experience to Estonia's cyber development cooperation. The ICT development cooperation budget in Estonia is not controlled by the Information System Authority but by the Ministry of Foreign Affairs. The need and importance must be justified continuously using specific performance indicators.*				
Managing EU funding programmes and supporting research and development at the Governing Board of the ECCC (European Cybersecurity Competence Centre). The preparation and presentation of Estonia's positions, including the involvement of experts for this purpose. Active participation in the work of the Governing Board.	Estonia's interests in the Governing Board are protected and it is ensured that EU financial resources are directed to the most important cyber-related projects and initiatives.	**Ministry of Economic Affairs and Communications, Information System Authority**	31.12.2025	3

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
Supervision over ENISA Management Board regarding strategic management, budget, work programmes, staff and overall operations. Preparation of Estonia's positions and involvement of experts. Representation of positions and active participation in the work of the Management Board.	Estonia's interests are protected in the Management Board.	**Ministry of Economic Affairs and Communications, Information System Authority**	31.12.2025	3
In the ECCG working party, drafting and implementing EU cybersecurity certification schemes. Active participation in the ECCG and involvement of Estonian cybersecurity experts. **Comment:** *See also sections 1.1 and 2.4.*	Estonia's interests are protected in the drafting of EU cybersecurity certification schemes In cooperation with the national cybersecurity certification authorities of other countries, the issuance of EU certificates meeting uniform requirements within the EU is ensured. Estonia's input has been provided.	**Consumer Protection and Technical Regulatory Authority,** Information System Authority, Ministry of Economic Affairs and Communications, Ministry of Defence	31.12.2025	3
Supporting the implementation of the NIS2 Directive in the NIS Cooperation Group.	Instructions, recommendations and guidelines have been developed to ensure uniform and effective implementation of the requirements of the Directive in all Member States.	**Ministry of Economic Affairs and Communications, Information System Authority**	31.12.2025, continuous	3
Development of EU cyber policy (EU Cyber Strategy) and various EU cyber legislation) in the Horizontal Working Party on Cyber Issues (HWPCI) of the EU Council.	Estonia's interests are prepared in accordance with national law and represented and protected in the working party.	**Ministry of Economic Affairs and Communications, Information System Authority**	31.12.2025, continuous	3
4.2 COMMUNITY AND SUCCESSION				
Assess the possibilities for rotation between different agencies to promote competences and the dissemination of good practices.	Estonia's cyber community is sustainable, open and diverse.	Ministry of Economic Affairs and Communications in cooperation with other ministries	31.12.2026	3
The state must contribute to privately initiated community events.	Local cybersecurity companies are supported through community events. Each year, 10 to 12 community events are held, with participation increasing by 10% annually.	Ministry of Economic Affairs and Communications, **Information System Authority**	31.12.2025	3
Analyse and support the promotion of career choices in the fields of natural sciences, computer science, and cybersecurity, including among girls and women, by involving community members as influencers.	The Estonian education system supports the development of the next generation of competent cybersecurity professionals. Cyber hygiene and cybersecurity topics are integrated at all school levels as part of mandatory subjects in the national curriculum.	Ministry of Economic Affairs and Communications and Ministry of Education and Research in cooperation with other ministries	31.12.2025, continuous	2
		Comment: *Consider the creation of a so-called state order to support/ensure the transition of individuals into areas deemed important from the state's perspective.*		

ACTIVITY	OUTCOME	RESPONSIBLE PARTY	DUE DATE	PRIORITY
In cooperation with the Ministry of Education and Research and the Ministry of Culture, it is necessary to develop digital and cyber skills at all education levels.	Cyber hygiene and cybersecurity are integrated into the curricula at all school levels and other national training activities aimed at increasing digital competence.	Ministry of Economic Affairs and Communications, Ministry of Culture and Ministry of Education and Research in cooperation with other ministries	31.12.2027	3
The Ministry of Economic Affairs and Communications, in cooperation with the Ministry of Education and Research, must prepare proposals on how to complement the curricula with topics of cyber hygiene and security.	Local knowledge of future technologies is growing significantly based on the national objectives of the cybersecurity sector (set out in the RDIE Strategy 2021–2035) and an environment promoting innovation and entrepreneurship.	Ministry of Economic Affairs and Communications and Ministry of Education and Research in cooperation with other ministries	31.12.2026	1
		Comment: *Curricula must be enhanced with in-depth teaching of natural sciences. The promotion of natural sciences and computer science is essential from the earliest stages of education.*		
It is necessary to develop cybersecurity microdegree programmes.	At least two Estonian higher education institutions offer various cybersecurity microdegree programmes on a long-term basis.	Ministry of Economic Affairs and Communications and Ministry of Education and Research in cooperation with other ministries	31.12.2028	3
		Comment: *The University of Tartu launched the Cyber Policy and Law microdegree in the spring of 2024, and starting from the autumn of 2024, it is possible to obtain the Digital Literacy and Cybersecurity microdegree at TalTech's Virumaa College.*		
It is necessary to establish a framework for the development of domestic know-how through research and development funding and to set strategic priorities in the field of research. **Comment:** *See also section 2.4*	Research and development funding targets strategic priorities that are in line with the country's development needs and support the development of domestic know-how and innovation.	Ministry of Economic Affairs and Communications and Ministry of Education and Research in cooperation with other ministries	31.12.2025	1
Methodological development and implementation of a cyber defence training platform.	The awareness of domestic companies about cybersecurity and the implementation of cyber defence measures has improved. On the cybersecurity platform / exercise field, 1,600 people have been trained.	**Ministry of Defence (CR14)**	31.12.2026	2