# Introduction

This cybersecurity strategy is Estonia's third national cybersecurity strategy document and defines the long-term vision, objectives, priority action areas, roles and tasks for the domain, being the basis for activity planning and resource allocation. The strategy is based on the lessons learned during the two previous strategy periods (2008-2013 and 2014-2017). As a horizontal strategy, it involves all contributing stakeholders in Estonia: the public sector (both civilian and defence), essential service providers, sectoral entrepreneurs, and academia. The aim of this document is to agree on and create conditions for the implementation of a comprehensive, systematic and inclusive sectoral policy.

The 2008 Cyber Security Strategy[1] was Estonia's first national strategy document that recognised the interdisciplinary nature of cybersecurity and the need for coordinated action in the area. It was also one of the first horizontal cybersecurity strategies in the world — it was only after the 2007 cyberattacks against Estonia that cybersecurity began to be perceived as an essential part of national security.

The Estonian cybersecurity strategy was among the first of its kind globally. Today, national cybersecurity strategies are commonplace,[2] as is the approach that the first Estonian cybersecurity strategy adopted. The 2013 European Union (EU) cybersecurity strategy[3] defined a national cybersecurity baseline (designating national competent authorities, establishing national incident response teams, developing a national cybersecurity strategy); the 2016 EU Network and Information Systems Security Directive[4] established these as a legal

> "Today, cybersecurity is universally accepted as an integral part of the functioning of the state, the economy, internal and external security.

1 https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf

2 https://www.itu.int/dms_pub/itu-d/opb/strategy/D-STR-GCI.01-2017-PDF-E.pdf

3 http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

4 http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32016L1148&from=EN

obligation. As of the development phase of this document, about fifteen nations and the EU have a second-generation cybersecurity strategy, Estonia among them.[5] With the third cybersecurity strategy, we are among the first countries in the world.

Today, cybersecurity is universally accepted as an integral part of the functioning of the state, the economy, internal and external security. The accelerating, diversifying and largely unpredictable digitalisation poses major challenges to risk identification and management. Next to these, the Estonian society today is not sufficiently well prepared for coping with existing cyber threats — the private and public sector alike are largely unaware of the risks and needs, in particular at the leadership level.

Digital technologies now have such an intertwined role in Estonian society that it is not possible to address all risks through a single planning document. The principles of cybersecurity are already partially integrated into sectoral planning processes. However, the maintenance and development of a sustainable digital environment also requires cross-sectoral focused cooperation. This can only be ensured by means of a strong and coherent sectoral strategy. In addition, the cybersecurity strategy plays the role of a communication tool for raising awareness in political decision-making processes, enhancing public-private partnership, and shaping Estonia's international engagement.

The Cybersecurity Strategy was prepared in a coherent process with Estonia's Digital Agenda 2020. Our experience has brought an understanding that in a successful digital society, developing information society and ensuring cybersecurity must be a strategic whole. The role of cybersecurity in the information society is to ensure conditions for efficient and secure use of opportunities offered by ICTs. The objectives and key indicators of the cybersecurity strategy are planned in a four-year perspective, with an interim review planned at the end of the current Digital Agenda in 2020.

The relevant terms and definitions are summarised in Appendix 1.

5 https://ccdcoe.org/cyber-security-strategy-documents.html

# The vision and fundamental principles of the cybersecurity strategy

## Estonia is the most resilient digital society.

Estonia can cope with cyber threats as a secure and undisrupted digital society, relying on the indivisibility of national capabilities, a well-informed and engaged private sector, and an outstanding research and development competence. Estonia is an internationally recognised leader in cybersecurity, a standing which supports national security and contributes to the growth of global competitiveness of companies operating in the domain. The Estonian society perceives cybersecurity as a shared responsibility in which everyone has a role to play.

## Estonia pursues this vision following four fundamental principles:

1. We consider the protection and promotion of fundamental rights and freedoms as important in cyberspace as in the physical environment.
2. We see cybersecurity as an enabler and amplifier of Estonia's rapid digital development, which is the basis for Estonia's socioeconomic growth. Security must support innovation and innovation must support security.
3. We recognise the security assurance of cryptographic solutions to be of unique importance for Estonia as it is the foundation of our digital ecosystem.
4. We consider transparency and public trust to be fundamental for digital society. Therefore, we commit to adhere to the principle of open communication.

# Key impact indicators of the cybersecurity strategy:

→ **No cyber incident causes significant disruptive social and economic effect on Estonian society or forces its residents to abandon the digital solutions they are accustomed to using.**

The 2007 cyberattacks have been the only cyber incident to disrupt Estonia's information society. Estonia has never been forced to abandon its digital solutions as a reaction to a cyber incident.

→ **Estonian residents feel secure online and trust digital public services.**

Metrics monitored:

| Metric | Starting level | Target level | Source |
|---|---|---|---|
| Percentage of residents who forgo electronic communication with public sector or service providers in order to avoid security risks[6] | 3.1% (2015) | ≤3.1%[7] (2020) | Statistics Estonia |
| Percentage of secure digital identity users[8] among all digital identity holders[9] | 57.6% (2017) | ≥65% (2020) | SK ID Solutions AS |

6 Internet users aged 16-74 who did not use the internet in the last 12 months due to security risks: communication with public sector institutions or service providers. https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database

7 The target level for both criteria will be updated in the course of the interim review in 2020

8 The electronic identities issued by the state were considered secure electronic identities in the case of the 2017 data.

9 The number of people who have used eID service at least once within the last year.

# Strategic objectives

In order to implement the vision, the strategy focuses on four strategic objectives. The related action areas consider the priority challenges identified in Section 1.3. The general trends that affect strategy execution and Estonia's strengths are described in Sections 1.1 and 1.2, respectively.

| Challenge (2018) | Ends 2022 | Ways |
|---|---|---|
| → Weak strategic integral management, insufficient cross-institutional situational awareness and fragmented organisation of information systems security<br>→ Insufficient consideration of security aspects during the development phase of information systems and services<br>→ Insufficient understanding of the impact of cyber threats, incidents and infrastructure interdependencies | OBJECTIVE 1<br>**A sustainable digital society**<br>Estonia is a sustainable digital society relying on strong technological resilience and emergency preparedness. | → Developing technological resilience<br>→ Ensuring cyber incident and crisis prevention, preparedness and resolution<br>→ Fostering comprehensive governance and development of a cohesive cybersecurity community |
| → Scarcity of Estonian enterprises successfully offering their cybersecurity products and services on the international market<br>→ Insufficient investments into R&D investment | OBJECTIVE 2<br>**Cybersecurity industry, research and development**<br>Estonian cybersecurity industry is strong, innovative, research-oriented and globally competitive, covering all key competences for Estonia. | → Supporting and promoting Estonian cybersecurity R&D and research-driven industry. |

| Challenge (2018) | Ends 2022 | Ways |
|---|---|---|
| → Retaining Estonia's reputation as a highly reliable international partner | OBJECTIVE 3<br>**A leading international contributor**<br>Estonia is a credible and capable partner in the international arena. | → Advancing substantial cooperation on cyber issues with strategic international partners<br>→ Promoting sustainable cybersecurity capacity building across the globe. |
| → Low cybersecurity awareness and deficient sense of ownership in risk management<br>→ Lack of specialists and insufficient supply of new talent | OBJECTIVE 4<br>**A cyber-literate society**<br>Estonia is a cyber literate society and ensures sufficient and forward-looking talent supply. | → Raising cybersecurity awareness among citizens, state and private sector<br>→ Developing talent to meet the needs of both state and private sector |

A pervasive underlying challenge is the limited capacity for specialisation in Estonia as a small population, which affects the public sector, enterprises and government entities alike. The problem is addressed by enhancing cooperation and communication mechanisms, consolidation, and reducing the fragmentation of expertise as top priorities of the strategy, thereby facilitating optimal use of limited resources.

The interrelationships between the strategic objectives are illustrated in Figure 1. The central objective is to ensure a sustainable and secure digital society, which then provides a basis for empowering R&D and the business environment as well as for a sustainable international leadership. This supports the internal strength and capacity of the state, cooperation with foreign partners, and furnishing of Estonia's international leadership role. An international leadership role based on substantive competence in turn strengthens the capacity to cooperate successfully with international partners in resolving cyber incidents and crises, and contributes to building and maintaining strong partnerships. Achieving the vision of the strategy is not possible without a high level of awareness of cyber risks and management, or without a competent workforce.

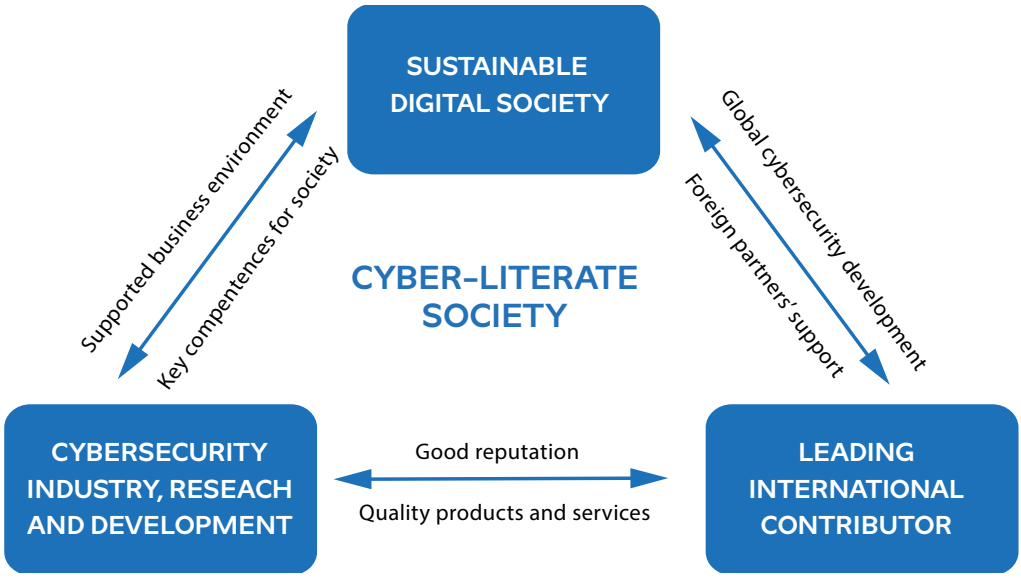


Figure 1: The objectives and interrelations of the Cybersecurity Strategy

# Priority activities

## We prevent:

→ The development of new services and databases will follow the principles of security and privacy by design. We will relinquish outdated platforms ('no legacy' principle). For this, we will develop a central security architecture advisory capability.

→ We will orient towards a risk-based approach in the national organisation of Estonia's information and network security and follow the best internationally recognised standards and practices. We support their broad-based implementation.

→ The state, in cooperation with all stakeholders, will have a comprehensive situational picture. For this, we will increase automated network intrusion monitoring and offer network monitoring capacity for private networks.

→ The security of essential services is ensured. To this end, we will systematically manage digital interdependencies and cross-border dependencies, and ensure security testing for the information systems underpinning the most critical databases and information systems.

→ Cybersecurity is acknowledged as a shared responsibility of all actors engaging in cyberspace.

## We protect:

→ We will consolidate the state's capabilities to do more with the resources we have. To this end, we will conduct an audit of cybersecurity capabilities and develop an appropriate organisational structure.

→ We will continuously include cybersecurity in the comprehensive approach to national defence. To do this, we will integrate cybersecurity even more into national security planning documents (the national defence development plan and the national defence activity plan) and regularly conduct joint exercises with vital service providers, senior political leadership and national defence organizations.

→ We will maintain an active and cohesive cybersecurity community. To do so, we will offer technical information streams, organize joint exercises and involve the private sector and academic competence in legislative drafting and strategic planning processes.

→ We will develop the capacity for cyber operations by continuing to develop the Defence Forces' Cyber Command further, developing cyber-attack capability and promoting "cyber conscription" where IT can be chosen rather than infantry for completing one's compulsory military service.

→ We will implement measures for combating cybercrime. To do this, we will create a framework for effective interagency cooperation and exchange of information, train processors, promote direct contacts between processors and international experts and increase the capability of law enforcement bodies.

→ We will ensure the security of critical databases and state data communication. To do so, we will implement the state communication concept and ensure that critical databases are mirrored to data embassies located outside Estonia.[10]

→ We will strengthen our practical everyday cooperation with our international strategic partners and allies.

## We develop:

→ We will ensure a future supply of IT specialists, viewing cybersecurity as a part of intensified IT studies and setting out expectations for universities when it comes to training of specialists.

→ We will support effective cooperation between state, academia and the private sector's key partners. To this end, we will launch a cluster that facilitates both domestic and international cooperation.

10 The definition and purpose of the term "data embassy" can be found in an agreement between Estonia and Luxembourg on hosting data and information systems. https://www.riigiteataja.ee/akt/228032018002

→ We will amplify the growth of cybersecurity as an economic sector, by supporting innovation and product development and strengthening diplomatic support for marketing activities.

→ We will create a research and development plan for the cyber sector and a coordination mechanism for directing the R&D performed by universities and companies, to give substantive content to companies' support measures and funding educational projects and scholarships.

→ By analysing future trends and risks, we will ensure the capability to respond rapidly to new challenges and threats.

→ We will promote competitive and sustainable cyber capability in partner countries, disseminating Estonia's experience to third countries through the EU and international projects.

### To attain the vision, we will need the following at all levels:

→ Sufficient competence, human resources, and funding;

→ Integration of cybersecurity into all areas and key planning processes;

→ Administration of the complexity of projects and minimization of red tape for the state, private sector through both legal and public administration measures.

# 1. The current state of cybersecurity

Twenty years ago, Estonia made a conscious choice to pursue a digital society and it is still on that course today. It is a choice that generates noteworthy value-added for society. The eID ecosystem alone amounts to an estimated 800 million to 1.5 billion euros per year, which is 4-7% of GDP.[11] When it comes to carrying through the e-state and many e-services, Estonia is a or even the world leader — and this entails risks as well as opportunities. There is no serious alternative to digital society, and thus there are no alternatives to investing in security, either. For Estonia, cybersecurity does not mean protecting technological solutions; it means protecting digital society and the way of life as a whole.

11 Considering the average time saved by digital signing, total worktime-based expenses and number of digital signatures per year. Source data: Tarmo Kalvet, Marek Tiits, Hille Hinsberg (editors) (2013). E-teenuste kasutamise tulemuslikkus ja mõju (efficacy and impact of use of e-services). Tallinn: Institute of Baltic Studies and Praxis Centre for Policy Research (time savings); https://www.ria.ee/ee/pea-poole-miljoni-id-kaardi-sertifikaadid-vajavad-uuendamist.html (Average number of digital signatures and authentications and number of digital identity documents used); https://www.stat.ee/stat-skp-jooksevhindades (GDP in current prices).

Estonia's strategic decisions are significantly impacted by the global cyber environment and both desirable and undesirable developments. A characteristic of cyber threats is that they know no national boundaries and attacks can have global reach. Various domestic and international trends have a significant impact on the security of Estonian cyber space, which are dealt with more broadly in the annual publications of the State Information System Authority, the Internal Security Service and the Foreign Intelligence Service,[12] academic studies[13] and risk analyses,[14] and conclusions of cyber defence exercises. Lessons learnt directly from our own experience and that of our foreign partners are particularly valuable, as is feedback from the community received in the course of discussions on the preparation of the strategy. Estonia has also had a one-of-a-kind opportunity to learn lessons from unprecedented cyber crises — the cyber-attacks of 2007 and the vulnerability discovered in the chip on the ID card in 2017 crisis — the resolution of which required experiences to be applied directly in choosing strategic directions.

## 1.1 Trends affecting cybersecurity

Trends that affect cybersecurity shape the environment in which countries operate and which they must proceed from in planning their activities. These are trends that Estonia has very limited possibilities to affect but that need to be taken into consideration.

### Expanding use of technology, growing digital dependency and emergence of new technologies

As a whole, the digital environment is characterized by an intensive growth of volumes, rapid development of technology and increasing digital dependence of societies. Between 2015-2019, the number of internet users worldwide is estimated to grow by 1 billion, the number of smartphones by 2.6 billion and the number of devices connected to the internet by 8.1 billion. The global data traffic volumes are expected to more than double and the volume of stored data will quintuple.[15] By 2020, the number of devices in the Internet of things[16] is expected

12 https://www.ria.ee/public/Kuberturvalisus/RIA-kuberturvalisus-2018.pdf, https://www.kapo.ee/et/content/aastaraamatu-v%c3%a4ljaandmise-traditsiooni-ajalugu-ja-eesm%c3%a4rk-0.html, https://www.valisluureamet.ee/pdf/raport-2018-EST-web.pdf

13 „ID-kaardi kaasuse õppetunnid" (Lessons learnt from the ID card case), Tallinn University of Technology, 2018: https://www.ria.ee/public/PKI/ID-kaardi_oppetunnid.pdf

14 „Küberintsident. Hädaolukorra riskianalüüs" (Cyber incident. Risk analysis of emergency), State Information System Authority, 2018 (access restriction AK)

15 https://www.mcafee.com/enterprise/en-us/assets/reports/rp-threats-predictions-2016.pdf

16 Network of internet-connected devices that exchange information, potentially including smartphones, home appliances, smart watches, medical devices, buildings and aircraft engines.

to reach 20-50 billion and the cloud computing volumes will triple from 2015 levels.[17] At the same time, the environment will be impacted by machine learning and the development of artificial intelligence, rapidly advancing robotics and adoption of self-propelled objects, blockchain technology and the potential advent of quantum computers in the near future.

The development of new technologies will result in diversification of cyber-attack methods, means and targets and changes in the possibilities for safeguarding cybersecurity. Digital dependence of the state and private sector has grown, which also affects services in all walks of life, even ones that were hitherto only indirectly related to technology. A vital services business continuity survey commissioned by RIA in 2016 concluded that all providers of vital services in Estonia depended on ICT in their activities and close to one-half considered that dependence to be critical.[18] The ID card security vulnerability situation in autumn 2017 showed tellingly how much government, private sector and the normal functioning of society as a whole depend on the functioning of digital basic infrastructure and its availability.

### Growing, changing and service-based cybercrime

Considering that a significant share of people's activity has moved into cyber space, the largest share of offences is also committed by exploiting virtual means. A distributed denial of service stack or ransomware campaign no longer requires high technical skills or major resources to commit. This means a much larger pool of potential criminals with the capability of attacking Estonian state and people via the internet. According to a risk assessment of cybercrime published by Europol, the number of cybercrimes in some EU member states was on track to exceed that of traditional crimes by 2016.[19] The magnitude of global economic losses falls short of only that of corruption and drug crime, making up 0.8 per cent of the world GDP.[20] As the ICT sector develops, new means and methods for committing cyber-attacks will arise. The greatest number of cybercrimes will be committed using ransomware, although an increase in the number of DDoS attacks can also be noted, including ones that exploit security vulnerabilities in devices connected to the Internet of Things.[21] A number of factors affect the spread of cybercrime, such as the security of services architecture, the popula-

17 Cloud and IoT Threats Predictions. McAfee Labs, Nov 2016. https://www.mcafee.com/hk/resources/misc/infographic-cloud-iot-predictions-2017.pdf

18 https://www.ria.ee/public/Kuberturvalisus/Elutahtsate-teenuste-osutamist-mojutavate-tegurite-uuringu-kokkuvote.pdf

19 Internet Organised Crime Threat Assessment (IOCTA) 2016. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

20 McAfee, Economic Impact of Cybercrime, 2018. https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

21 Iocta 2017. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

tion's awareness of the dangers and how to protect themselves against them, the effort required to commit a crime; the gains they stand to pocket, and the likelihood of getting caught.

### A complicated (geopolitical) security situation

Estonian cybersecurity is inevitably also affected by the complicated security situation in this region and worldwide. The use of cyber operations to achieve the strategic objectives or influence sought by foreign powers has become more common and serious in recent years: democratic processes (elections, referenda and related campaigns) are subverted and vital infrastructure is attacked (above all, the energy, communication and banking sector).[22] The broader aim of cyber-attacks may be to achieve political or economic influence; means used include political influence operations (including public opinion) and, say, support for cybercrime or targeted attacks against vital sites. Carrying out cyber operations is also a way to probe for weaknesses and grey areas where objectives can be achieved at lower cost than with conventional warfare (considering that the conventional attacks pit strength against the strength of the party being attacked and causes greater blowback from the international community).

Above all, cybersecurity comes down to the existence of technological and institutional capability and using it in a deliberate, concerted manner, yet society's sense of security is impacted to a significant degree by the communication aspect — the perception of cybersecurity. According to various public opinion polls, the likelihood of a cyberattack occurring is rated rather low or medium.[23] Yet according to a survey conducted the year before, March 2017, 67% of Estonians consider an organized cyber-attack the most likely threat facing Estonia.[24] Above all from the standpoint of society's stability and a functioning economy, it is essential that inhabitants and foreign partners be convinced that Estonia needs the capability for coping with cyber threats.

### Limited technological autonomy

Estonia is part of the global digital environment and relies largely on foreign IT solutions. Computer and network hardware is produced largely in Asia, and

22 e.g. WannaCry and NotPetya. Energy infrastructure has become a frequent target of cyber attacks starting with the attacks on the power plants in Ukraine in 2015 and 2016.

23 27% of respondents said they felt commission of cyber-attacks against information systems was likely in a 2018 public survey on internal security. The actions of the Estonian government in fighting cybercrime were given a high rating in the same survey (64%).

24 67% said an organized (cyber-)attack against Estonian state information systems could take place and 61% said a foreign country could intervene to influence Estonian politics or the economy in its own interests.http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/avalik_arvamus_ja_riigikaitse_marts_2017.pdf

operating systems, software and services come mainly from the US. The result is that our cybersecurity situation is impacted by the security vulnerabilities in the IT solutions of other countries and attacks against them.[25] Our behaviour and that of other European countries is thus inevitably passive in many respects and focuses on responding to security flaws in solutions or risk prevention. The practices of Estonia's main allies show that the (cyber defence) software used in government systems as well and its origin can have implications for national security (for example, US and European government institutions have limited the use of products of Russian or Chinese origin in their systems). It is in the interests of both Estonia and the EU to increase strategic autonomy by strengthening the national and European cyber industry.

### Globalization of the cybersecurity debate

Cybersecurity has been developed into an important part of national security for the developed world, leading to increased attention and resources. Over the last decade, cybersecurity has become a priority for international cooperation formats.

In 2010, **NATO** acknowledged for the first time in its new strategic conception that cyber-attacks constitute a security risk.[26] At the 2014 Wales summit, NATO recognized the validity of international law in cyber space and declared that as the impact of cyber-attacks on contemporary society could be comparable to conventional attacks, cyber defence is part of NATO's collective defence mandate. [27]At the 2016 Warsaw summit, NATO called cyber space one domain of military operations where the alliance's defence capability must be ensured. [28]

On 6 July 2016, the **European Parliament** adopted a network and information security directive[29] for raising the level of cybersecurity; it includes the obligation for all member states to prepare a national strategy for network and information systems security. During the Estonian Presidency of the Council of the EU in 2017, the cybersecurity policy of the European Commission was updated , it also contained the updated[30] version of the EU Cybersecurity Strategy.

One of the most complicated and important topics under international discussion is the application of international law in cyberspace. Signalling the need perceived

25 2017's biggest cyber incidents WannaCry and Petya/NotPetya were connected to Microsoft vulnerabilities, but flaws with major international impact have been found in nearly all tech companies' solutions.

26 https://www.nato.int/cps/en/natohq/topics_82705.htm

27 https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

28 https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

29 http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32016L1148

30 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2017:450:FIN&rid=3
https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF

on the **UN** level for greater legal clarity and the fundamental readiness of countries to seek and create that clarity are the groups of cyber experts convoked by the UN General Assembly (UN GGE). Their reports from 2013 and 2015 recognize explicitly the application of international law in cyber space. The 2017 group did not however manage to agree on the final report and as of 2018 the countries did not get closer to a consensus on how international law is to be applied in cyber space.

At the OSCE level, confidence building measures have been agreed upon in 2013 and 2016 to reduce the risk of conflict through exchange of information and cooperation.[31]

As a key academic contribution, a manual on international law applicable to cyber operations was published in February 2017 under the aegis of the NATO Cooperative Cyber Defence Centre of Excellence. The Tallinn Manual 2.0[32] deals with cyber operations as a component in relations between countries in the context of international law, giving practical guidance to countries.

### An ever more comprehensive legal environment for market participants

With the growing importance of the digital environment and increased risks comes pressure and need to regulate the field to a greater extent at the EU level and within Estonia. Estonia's opportunity here is to keep the volume of regulations under control, as an effect of number of processes and procedures is that the total complexity of the rules increases — each new regulation is more precise and thorough than the previous one. The complexity of the state's IT solutions grows with the volume of regulations and IT itself becomes intrinsically more complex. On one hand, regulations must contribute to the substantive implementation of data security and ensure the security of society based on the weighty role played by the digital environment in the functioning of society. At the same time, it is also a challenge for cross-sectoral cooperation and pressure on Estonia's speed and flexibility, making it more complicated to resolve problems using new methods and Estonia's own rules, which has to some extent been the precondition for the success stories to date.

### Challenges posed by Internet freedom

All over the world, the availability of the internet has increased people's access to information and besides economic growth, it has also created greater transparency and created the possibility for better and less costly provision of public services, participation of civil society in decision-making processes, and raised

31 The value of the OSCE process is that it encompasses countries with very different views (including EU, the US and Russia).

32 Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017.

the effectiveness of global integration as a whole. Recent years have shown how internet freedom supports democratic processes but have also pointed up the growing crackdown on internet freedom by authoritarian regimes. There are countries and interest groups who emphasize the positive aspects of restricting users' access from the cybersecurity perspective: service providers and the corresponding national institutions have more flexible access to internet traffic and establishing restrictions allows, in their view, more effective protection for networks and critical infrastructure as well as more effective interdiction of crime. On the basis of Freedom House reports, Estonia has been one of the leaders and role models in internet freedom each year, but influencing global trends is a major challenge in a situation where global internet freedom has been in decline for the last seven years.[33]

## 1.2 Estonia's strengths

Relying on its strengths will allow Estonia to carry out its strategic goals and find effective solutions to the challenges. The following lists the five Estonian strengths in the cyber sector that have the greatest impact and potential.

### Secure basic architecture for Estonia's digital society

Estonia's digital architecture is based on the government-issued secure electronic identity and the X-road data exchange layer, which has helped to enable and leverage the rapid digital innovation and ensures that security is organized in a manner that is convenient and natural for citizens. X-road is the means for securely structuring state services and data exchange and cooperation and the ID card as the obligatory identity documents are the means used by the state to provide its citizens with a digital identity certificate (authentication and signing means) and encryption device, thus spreading secure technology to the general population. More than in just the existence of the technology, Estonia is distinct from other countries in terms of its capability of implementing the technology.

### A tested level of maturity

Estonia's current cybersecurity is reinforced by a functioning digital society infrastructure, a strong digital identity, obligatory system of security measures for government institutions and vital service providers, a central cybersecurity incident monitoring, resolution and reporting system, supportive legal space and functioning cooperation formats. The experience of two crises (2007 and 2017) have given Estonia the practical and tested assurance that the selections made to

33 https://freedomhouse.org/report/freedom-net/freedom-net-2017

develop the cybersecurity sector are largely the right ones and that we are getting on well in defending our digital society. Nor was this merely the outcome of successful PR or a case of individual innovative accomplishments — in the International Telecommunications Union (ITU) index,[34] Estonia placed fifth in the world and first in Europe in development of cybersecurity.[35]

### The efficiency and flexibility typical of a smaller country

A small and cohesive cybersecurity community and good interpersonal communication are prerequisites for responding effectively to salient problems. There is also an informal understanding of who takes care of what aspects, and subordination of decision-making processes is kept to a minimum: if needed, one can usually approach top executives/officials and senior politicians directly. Trust-based and efficient cooperation with market participants is supported by the openness of the state as a principle.

### Estonia's international influence

Estonia's high international reputation comes from the fact that in the last ten years, we have retained our international leading role and been an innovator — introducing and being the first adopter of novel cybersecurity concepts — and in so doing, we have led the way internationally. This has resulted in international interest in Estonia as a country with a top cybersecurity capability. Estonia is seen as a reliable partner and Estonia's voice has considerable influence in international discussions. Besides the cyber sector, this strengthens Estonia's position more broadly on security and economic issues.

### High trust among end users

Citizens' trust in the digital state and services and a basic societal understanding of the importance of cybersecurity were notably influenced by the successful resolution of the cyber-attacks of 2017 and the resolution of the vulnerability on the ID card in 2017, which provided a crash course for the general population in terms of how digital environment impacts everyday life and yielded the practical experience that ensuring security requires end users to be active as well (keeping software updated, purchasing alternative solutions). Trust in digital identity and services is also shown by the number of transactions and operations conducted in autumn 2017 using the ID card,[36] which remained at close the same level as before the crisis.

34 https://www.itu.int/dms_pub/itu-d/opb/strategy/D-STR-GCI.01-2017-PDF-E.pdf (2016)

35 https://ncsi.ega.ee/ncsi-index/ (2018)

36 In 2017, 108m authentication operations were performed and 123m digital signatures were given by users of ID cards and mobile ID (RIA, 2018)

## 1.3 Challenges for Estonia

Key challenges for ensuring Estonian cybersecurity are not significantly different than those facing comparable countries. Estonia is one of the world's most digitally dependent countries and thus the potential impacts of cyber threats are much more significant than in the case of many other countries. The following lists the seven highest priority problems and challenges identified during preparation of the strategy, which currently hinder the optimum functioning and development of the field and which the standardized solutions applied to this point have not rectified.

### Limited capability for specialization

Limited specialization capability in the public sector, private companies and research institutes is a fundamental problem for a small and decreasing population. Even though the small community of experts and good interpersonal relationships ensures efficiency and flexibility in the first response to crises and incidents, the strength it represents is not sustainable in a situation where the complexity of IT systems and threats keeps on growing. The fragmented nature of sectoral expertise prevents specialization at a top level, and the result in turn is the danger that top-level specialists will leave Estonia and, above all, the public sector.

### Lack of integral leadership

Strategic integral leadership in the field of cybersecurity and united coordination are major challenges: planning in the sector still takes place more as a sum of the areas of responsibility of the institutions, each one having its own priorities. This is also the reason for insufficient interinstitutional situation awareness and fragmented, inconsistent and inefficient organization of protection for information systems, despite the general direction taken to consolidating resources.

### Insufficient understanding of the influences of cyber threats and incidents and cross-dependencies

The spacious autonomy when it comes to development and administration of IT systems results in a situation where institutions organize administration of cybersecurity risks often without appraising the broader impact of their decisions, even though they are connected to the public infrastructure (state network). Disregard for or the absence of common security principles and standards jeopardizes the functioning of Estonia's digital services, which are based on dispersed architecture. The state still lacks a systematic view of the mutual cross- and cross-border dependencies and potential impacts of systems and a clear view of ensuring the minimum level of services that should also be operational in a crisis.

### Insufficient awareness and low sense of ownership

Awareness of cybersecurity is still insufficient both among state and private sector leaders and in society in general, which in turn leads to a low sense of responsibility. The above contributes to cybersecurity being given short shrift in the development of information systems and services. The ensuring of cybersecurity is not sensed as a personal responsibility or risk to the organization's main activity; rather, it is treated predominantly as an arcane technical topic that someone else must deal with. The volume of resources directed to ensuring information security in developing and administering systems is not keeping up with needs arising from the development of the field and growth in the burden on regulators — this is a challenge that the growing complexity that is part of technology's constant development keeps on intensifying.

### Lack of specialists, including insufficient training of new specialists

The low level of competence workforce in the public and private sector affects fulfilment of all strategic objectives. The cybersecurity (labour) market is global and subject to constant competition for the best talent. The top specialists who support critical state functions are actively sought by Estonian and foreign companies. The challenge for the government sector is to offer enough meaningful solutions, freedom and opportunity to carry out novel and unique solutions. At the same time, as the international reputation of the tech sector and cybersecurity in Estonia increases (something that the state itself is actively amplifying), pressure is increasing for recruitment of specialists away from Estonia into the private sector and international companies. Moreover, current cybersecurity curricula do not yet take the needs of the Estonian labour market into sufficient consideration, as the needs for workforce have not yet been clearly mapped and commissioned. The lack of flexible re-training possibilities can also be cited as a shortcoming in cybersecurity curricula. A problem sensed by the community in the sector is the acquisition of the necessary cyber competencies in curricula outside the field of IT and cooperation between public and private sector with research institutes, which is not sufficiently systematic.

### Low number of successful companies in the sector and insufficient volume of R&D

The number of Estonian companies successfully developing their cybersecurity product or service on international markets is still low, considering that cybersecurity and security industries have major export potential considering Estonia's strengths in the sector. An important factor that curtails development is the shortage of specialists, which impedes growth throughout the ICT sector as a whole. There are also not enough resources in strategically important research areas such as cryptography or secure identification solutions. A key question is

insufficient cooperation between state and research institutions, which stems from limited understanding of the current and future priorities for the state and the challenges in planning research activity. Just as large a problem is insufficient cohesiveness between research and enterprise — the commercialization of research results is a problem in Estonia and across Europe: research is published but does not result in real prototypes, products and patents. Strong and capable enterprise in the sector and research and development does not only contribute to the development of the state (economic growth); it also has a very direct impact as a provider of security service the state needs — the highly digitalized public administration in Estonia occasions the need for innovative and flexible solutions that are often unavailable from foreign enterprises — and it also has a role as a crisis reserve for the lean state, ensuring the existence of knowledge and talent that can be drawn on when the state needs emergency assistance.[37]

### Maintaining Estonia's reputation as a trusted and valuable international partner

Estonia's role among the cybersecurity leaders in the world, which supports exchange of the information and knowledge Estonia needs with strategic partners and amplifies Estonia's voice on the international arena, is not something that is self-sustaining — after all, this is a rapidly changing and competitive field and rapid development is taking place in many other countries. Thus, Estonia's international image is not to be taken for granted — although we have grown used to doing so — and will not be sustained by inertia. Therefore, additional efforts and allocations of additional resources are needed.

# 2. Coordination and implementation of the strategy

## 2.1 Role and scope of the cybersecurity strategy

The Cybersecurity Strategy is a horizontal document regarding agreements and coordination in the field of cybersecurity, which all the most important Estonian cybersecurity stakeholders helped to draft: government institutions, academia and think tanks and the private sector. The strategy does not provide detailed coverage of all necessary activities for ensuring cybersecurity, of which a key part has already become a natural part of the planning processes in various sectors. The purpose of the Cybersecurity Strategy is to form the big picture, as it were,

37 ˇThis was shown clearly by both the response to the 2007 cyber attacks and the autumn 2017 ID card crisis.

avoid redundancy and overlapping efforts, and ensure that the principles and objectives agreed upon during drafting the strategy are implemented through a combination of all parties and processes.

The strategy's focus lies on problems affecting state and society and which require cooperation between stakeholders to resolve. The role of the strategy is to ensure a framework for ensuring cybersecurity, which enables and amplifies productive dialogue between science and technology, private enterprise and public administration, thereby supporting a well-functioning economic environment and guarantees for national security.

## 2.2 Linkage with other strategies

At the most general level, the objectives of the Estonian cybersecurity sector proceed from the agreements stated in the **fundamental principles of Estonian security policy.**

The **Digital Agenda 2020 for Estonia** deals with objectives related to the development of the e-state, ensuring data communications and general ICT skills and its content is planned as a unified process with the Cybersecurity Strategy. Solely by uniform planning of development of digital society and data security can the implementation of the security by design principle be guaranteed in practice, which requires that seeking and prevention of security vulnerabilities be an integral part of the development of network, service and basic infrastructure and the personal responsibility of the service owner. Addressing these separately or adding them later will not generate good outcomes. The following sets out the key topics from the standpoint of ensuring the state's general cybersecurity, which are laid out in detail in the Information Society Strategy based on the holistic view of development of the e-state, not just from the aspect of ensuring data security:

→ **The security of electronic identity and electronic authentication capability,**[38] which is in essence the basic capability for ensuring Estonia's cybersecurity. In addition, the functioning of public services Is based on it, and it is therefore a broader societal security issue.

→ **Following the "no-legacy" principle** — the public sector should not make use of significant ICT services and solutions that are outdated. The up-to-dateness of ICT solutions and services ensures that the systems' security level meets unified quality requirements.

38 The precise content stems from a white paper being prosduced in collaboration between government institutions and private sector on identity management and identity documents, which contains broad-based future scenarios and strategic choices for electronic identity and its carrier.

→ **Development and broad adoption of a government cloud solution,** which will hedge the infrastructure risks stemming from IT, allowing information systems to be kept in a secure environment and guaranteeing that security is up to date.

→ **Secure internet voting** — all voting technologies must be tested, audited and secure, and meet the legal requirements applicable to elections. Elections and democracy in general have become the second most important target for attackers after critical infrastructure when it comes to the national security perspective.

The National Defence Development Plan 2017—2026 is the central planning document for national defence, and its goal is to set out, based on existing threat scenarios, for the next ten years, the non-military and military capability developments that are necessary and in line with the state's possibilities.[39] The main cyber priorities in the national defence development plan are to establish a big picture for monitoring developments in cyber space in real time and development of a cyber command and "cyber conscription".

The planning of implementation of activities related to development anti-cybercrime capability and identifying attacks that endanger the state's internal security is dealt with by the **Internal Security Development Plan 2015–2020** in line with the objectives of the Cybersecurity Strategy 2014-2017 and the **Internal Security Development Plan 2021–2030 (in the development phase),** in which the main activity areas when it comes to ensuring the cybersecurity of Estonian society are the following: promoting capability for detection and investigation of cybercrimes that takes into account developments in ICT; ensuring readiness for future threats and challenges related to cybercrime and security; promoting domestic and international practical cooperation and information exchange between partner institutions; dissemination of information; gathering and analysis of relevant information to achieve as complete an overview of the cybercrime situation; the combating of the sale of illegal goods and services online; analysis and mitigating of risks related to e-Residency and digital identity.

**The development areas for criminal justice policy up to 2030**[40] is a document that defines the long-range goals of criminal justice policy, the focus areas of which also devote attention to reducing cyberbullying and — in the field of criminal proceedings — to fighting cybercrime.

**The Violence Prevention Strategy for 2015–2020"**[41] focuses above all on ensuring that children and teens use media and the environment safely to protect them

39 https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/rkak_2017_2026_avalik_osa.pdf

40 https://www.just.ee/et/kriminaalpoliitika-arengusuunad

41 https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/vagivalla_ennetamise_strateegia_2015-2020_kodulehele.pdf

from dangers lurking online, including cyber bullying, and planning activities for prevention of incidents of violence against children committed online. The strategy is supported also by the **Children and Families Development Plan 2012–2020,**[42] which deals with providing advisory service on internet security, including developing parental skills and running an information hotline for reporting illegal content and activities.

A fixture of Estonia's image in terms of ensuring cybersecurity and rapid response to cyber threats is set forth in the proposal for the drafting of a **Foreign Policy Development Plan 2030.**[43] This strategy will deal with raising awareness of international law topics in the cyber sphere, dealing with promotion of development cooperation, envisioning Estonia's active participation in the creation of an EU cyber assistance network and stressing the need to ensure that the population has trust in cyber space. Estonia's desire to support multifaceted adoption of ICT and e-state solutions in developing countries is set out in the **Development Cooperation and Humanitarian Aid Development Plan 2016–2020.**[44] Estonia's goal is to raise broad awareness of the potential of ICT and the e-state and agents of development in the EU's development policy, ensuring that functions that are important from the standpoint of ICT and the e-state are resilient to cyber threats as well.

**As part of the Lifelong Learning Strategy 2014–2020,**[45] efforts are being made to ensure that competences pertaining to digital skills also include cybersecurity, and that besides digital technology, elementary knowledge related to cybersecurity are also integrated into curricula. The objective of the lifelong learning strategy's digital revolution programme is the smart and knowledge-driven integration of digital opportunities into the academic process and thereby ensuring the development of digital competence (including competences related to security in the field of general education.

To achieve innovative and competitive enterprise in the cybersecurity sector and research and development activity, important points of cooperation are the **Knowledge-Based Estonia, the RD&I Strategy for 2014–2020**[46] and the **Estonian Enterprise Growth Strategy 2014–2020".**[47] The strategy seeks to ensure that the state as customer and initiator of R&D enjoys successful substantive

42 https://www.sm.ee/sites/default/files/content-editors/Lapsed_ja_pered/laste_ja_perede_arengukava_2012_-_2020.pdf

43 https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/valispoliitika_arengukava_koostamise_ettepanek_kodulehele.pdf

44 https://vm.ee/sites/default/files/content-editors/development-cooperation/2016_2020_arengukava_tekst.pdf

45 https://www.hm.ee/sites/default/files/strateegia2020.pdf

46 https://www.hm.ee/sites/default/files/tai_strateegia.pdf

47 http://kasvustrateegia.mkm.ee/

cooperation with companies and research institutions, which would boost the creation of innovative products.

The Estonian government cabinet has set a goal of adopting an activity-based budget for the year 2020 in order to proceed from performance management, linking the strategy's administration with financial accounting. This planning logic is also the basis for the framework for implementing the Cybersecurity Strategy: the measures, activities and financing plan necessary for achieving the priorities agreed in the Cybersecurity Strategy are planned in detail in the cybersecurity programme and other development plan programmes that belong to responsible ministries' performance areas. The linkages between the Cybersecurity Strategy and other sectoral planning processes are illustrated in Figure 2.

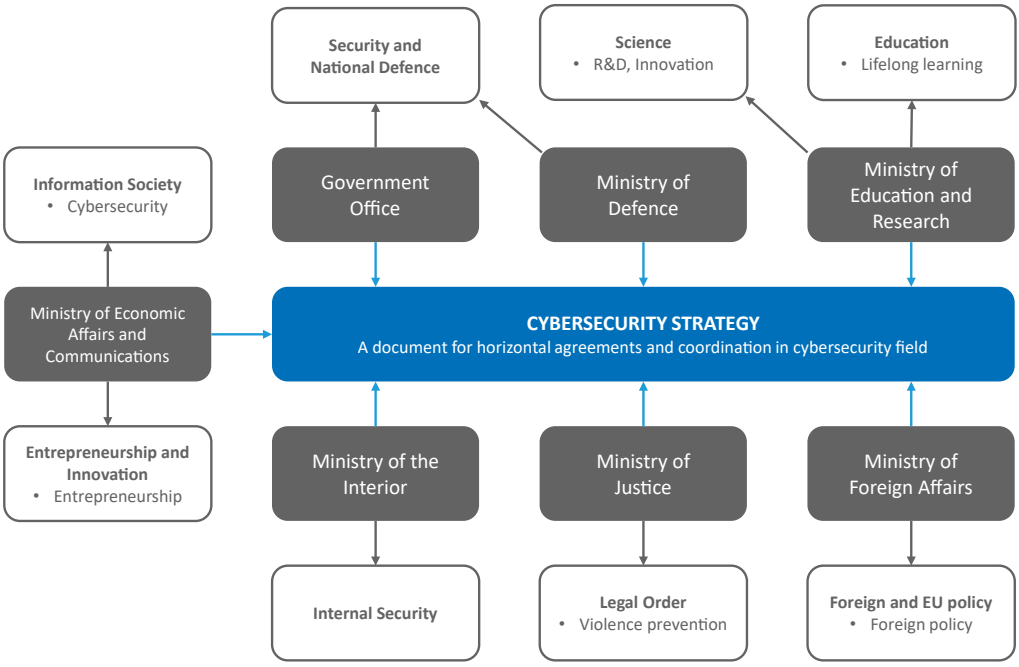


Figure 2: Performance areas connected to planning activities necessary for implementing the objectives of the Cybersecurity Strategy

## 2.3 Linkage with strategies of other countries and international strategies

Strategic planning of Estonian cybersecurity proceeds from the international situation, taking into account the strategic intentions of countries that are important for Estonia and providing general support for the strategic objectives of the EU and NATO cybersecurity policy. That means that the decisions related to Estonian cybersecurity overlap with the joint positions expressed in the EU's 2017 cybersecurity package and that continuity of vital services and operational cooperation with other member states for preventing and resolving incidents are part of the strategy's priorities. Having joined the Cyber Defence Pledge,[48] Estonia and other allies have confirmed that they are committed to protection of national infrastructure and networks, thereby promoting NATO cybersecurity as a whole.

## 2.4 National cybersecurity coordination and organization of management

The planning of cybersecurity policy and implementation of the strategy are coordinated, and corresponding cooperation with government and society at large are organized, by the Ministry of Economic Affairs and Communications. At the strategic level, coordination takes place through the **Government of the Republic security committee's cybersecurity council,** which ensures the implementation of the Cybersecurity Strategy objectives through the responsible government institutions' planning documents, programmes and work plans. The primary responsibility for the implementation of the nationwide cyber sector policy agreed in the Cybersecurity Strategy lies with the government institutions that contribute to the work of the cybersecurity council. The areas of responsibility of the different institutions are described in the list below and the Cybersecurity Strategy management system is illustrated in Figure 3.

→ The **Ministry of Economic Affairs and Communications** manages and coordinates the preparation and implementation of the Cybersecurity Strategy as a part of the integral view of the Information Society Strategy, and in cooperation with the **State Information System Authority (RIA),** the ministry holds the central role in activities related to developing technological resilience, crisis and incident management, development of enterprise in the cybersecurity sector, and guiding research and development. RIA's functions are broad-based in the cybersecurity field, including ensuring the security of all network and information systems important for the functioning of the state and with exceptions arising from legislation.

48 https://www.nato.int/cps/su/natohq/official_texts_133177.htm

Among the agencies in the jurisdiction of the Ministry of Economic Affairs and Communications, other contributors to ensuring Estonian cybersecurity and strategic planning are the **Technical Surveillance Authority (TJA)** whose functions in the ICT field are promotion of security and trustworthiness of electronic communication equipment and supervision of the providers of certification services and timestamping services; the **Estonian Internet Foundation (EIS),** which is the organization that represents the Estonian internet community and administers .ee domain names; the **State Infocommunication Foundation (RIKS),** which is tasked with ensuring the continuous, high-quality, secure and cost-effective information communication and infrastructure service for the state (such as government cloud and government communication concept); and **Enterprise Estonia (EAS)** and **Startup Estonia (SUE),** which contribute to supporting the development of enterprise and innovation in the sector.

→ The **Ministry of Education and Research** takes into consideration the priorities agreed in the Cybersecurity Strategy's objectives in its planning of lifelong learning strategy activities, supporting the acquisition of basic knowledge for graduates at all educational levels so that they can cope with cyber threats.
In the area of government of the ministry, the fulfilment of the strategy objectives is supported by the **Information Technology Foundation for Education (HITSA),** which contributes to the training of specialists in the field through coordinating both the Targalt Internetis ("Staying Smart Online") programme and the IT Academy programme.

→ The **Ministry of Justice** contributes in cooperation with the **Office of the Prosecutor General,** which is in charge of pre-trial criminal proceedings. The ministry contributes to planning judicial and criminal justice policy throughout the sector, and through violence prevention strategy activities, it plans sectoral prevention activities.
Institutions that are considered important from the standpoint of the cybersecurity field are, in the Ministry of Justice's area of administration, the **Data Protection Inspectorate (AKI),** which performs supervision regarding the rights and responsibilities in the field of protection of personal data; the **Estonian Forensic Science Institute (EKEI),** which deals with expert analysis on information technology, among other functions, and the **Centre of Registers and Information Systems (RIK),** which develops and administers important registers and information systems.

→ The **Ministry of Defence,** in cooperation with the **Defence Forces, Defence League and the Foreign Intelligence Service,** is in charge of implementing activities related to the military defence part of the strategy and contributes throughout to creating cross-sectoral cooperation and coordination mechanisms and getting a uniform reading on the situation.

→ In cooperation with the **Police and Border Guard Board** and the **Internal Security Service,** the **Ministry of the Interior** deals with prevention, combating and detection

of cybercrimes, and prevention and combating offences that jeopardize cybersecurity. It also implements the activities of the domestic security development plan and related programmes, and contributes to cross-sectoral cooperation and coordination mechanisms and establishes a unified assessment of the current situation.

→ The **Ministry of the Interior's Information Technology and Development Centre (SMIT),** which ensures the administration and development of information systems related to domestic security.

→ The **Ministry of Foreign Affairs** directs and coordinates the international cooperation activities related to the strategy.

→ The **Ministry of Finance** takes part in developing the different parts of the strategy substantively, including in ensuring sustainability and ensuring integration with other strategic planning processes. In addition, it makes sure that the finance sector is involved. The **Financial Supervision Authority** also ties in with the cybersecurity themes, as it performs supervision over financial institutions. The **Bank of Estonia** does the same through the requirements established by the European central banking system.

→ **The Government Office** ensures that cybersecurity is integrated into national defence planning documents (the national defence development plan and the state defence activity plan).

Both in planning and implementing the strategy and more broadly in ensuring the cybersecurity of the Estonian state, close cooperation between the competence centres and think tanks, universities, research institutions and private sector partners with knowledge and capability in the field is important. The state uses the capability of think tanks as strategic partners in developing sectoral competence and international cooperation. As the host and framework country for the **NATO Cooperative Cyber Defence Centre of Excellence (CCD COE),** Estonia has a strategic interest in promoting the development of the centre as an international organization of like-minded countries, making active use of the cyber defence exercises, international discussion forums and research studies offered by the centre. The **E-Governance Academy (EGA),** being a consultation and think tank centre for information society, supports the international adoption of Estonia's digital (including cybersecurity) solutions. The **International Centre for Defence and Security (RKK)** is a leading think tank in Estonia, specializing in foreign policy, security and national defence. The concerted use of Estonian experts' cyber defence expertise is used to support the development of comprehensive national defence, among other things. The **TalTech Centre for Digital Forensics and Cybersecurity** consolidates the primary public sector institutions responsible for the cyber sphere, and the goal set in cooperation is to rise Estonia's cybersecurity competence and capability by way of education and R&D.

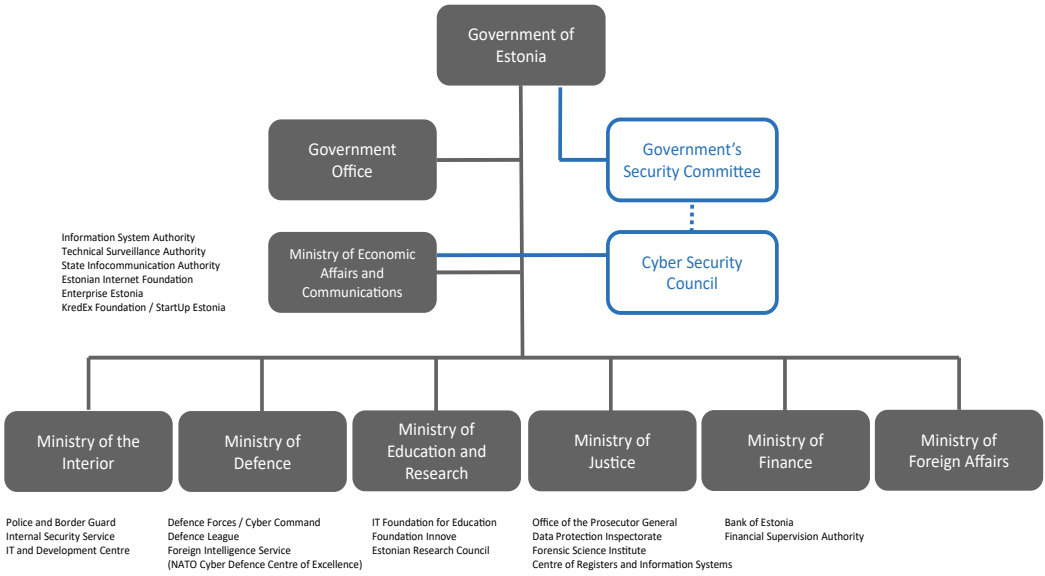


Figure 3: System for management of the cybersecurity sector

For the coordinated implementation of the objectives agreed in the Cybersecurity Strategy, the ministries that contribute directly to the implementation of the strategy[49] and the Government Office appoint a responsible official who is the liaison for issues related to ensuring national cybersecurity in their jurisdiction and ensures that the priorities agreed in the Cybersecurity Strategy are carried out through the respective ministry and planning documents in its jurisdiction, preparing on this basis an annual report for the cybersecurity council. The cooperation and exchange of information between the responsible officials is organized by the Ministry of Economic Affairs and Communications.

Once a year, the Government of the Republic's security committee approves the consolidated report on activities in the field of cybersecurity, and within the report on implementation of the information society strategy, an overview of the activities carried out is provided to the Government of the Republic.

# 3. Strategic objectives

To implement the vision, the strategy focuses on four overarching objectives, the activity areas of which cover all the focus problems mapped as priorities when the strategy was drafted (detailed descriptions in sub-chapter 1.3.). The implementation of the objectives is impacted by general trends (described in sub-chapter 1.1.) and enable Estonia's strengths (see 1.2.).

49 Ministry of Education and Research, Ministry of Justice, Ministry of Defence, Ministry of Economic Affairs and Communications, Ministry of the Interior, Ministry of Foreign Affairs.

| Problem (2018) | Problem (2018) | Activity areas |
|---|---|---|
| → Weak strategic integral management, insufficient cross-institutional situation awareness, fragmented organization of information systems<br>→ Cybersecurity not given its due in the development of information systems and services<br>→ Insufficient understanding of the impacts of cyberthreats and incidents and infrastructure (cross-) dependencies | Estonia is a sustainable digital society with strong technological resilience and readiness for coping with crises. | → Making technological resilience more effective<br>→ Prevention of incidents and crises, readiness and resolution<br>→ Integral management of the field and developing a cohesive community |
| Low number of successful Estonian companies developing their own cybersecurity product or service, including on international markets, and insufficient volume of R&D. | Estonia has strong, innovative, research-based and globally competitive cybersecurity sector enterprise and R&D, which covers the key competencies that are important for the state. | Support and promotion of cybersecurity R&D and research-based enterprise. |
| Keeping Estonia's reliability as international partner high | Estonia is a strong partner to be reckoned with on the international arena | → Making cooperation more efficient with strategic partners abroad<br>→ International promotion of sustainable cyber capability. |
| → Low cyber awareness and sense of a personal stake for taking responsibility for cybersecurity risks<br>→ Lack of specialists and insufficient supply of young talent | As a society, Estonia has high cyber awareness and the supply of young talent in the sector is secure | → Raising cyber awareness among citizens, state and private sector<br>→ Development of talent corresponding to state and private sector demand |

In addition, a pervasive fundamental problem is the limited capability for specialization in Estonia, due to its small population, in the public sector, companies and government institutions. The problem is addressed by making cooperation and communication mechanisms more effective, consolidating them, and reducing fragmentation of expertise, which will al allow limited resources to be used more efficiently.

# A sustainable digital society

**Objective 1: Estonia is a sustainable digital society with strong technological resilience and readiness to cope with crises.**

The primary function of the strategy is to ensure that vital functions (strategic infrastructure and services) are resilient to cyber threats. The objective focuses on resolving today's problems that have the most impact, and ensuring readiness for coping with future trends. The basis and enabling element for both is having a strategic big picture at the national level, interoperability, a functioning community and inclusive planning.

The objective is given substance by three activity areas:

1. Technological resilience
2. Managing and being prepared for crises, attacks and incidents
3. Integral leadership of the field and a cohesive community

**Performance indicators:**

| Indicator[50] | Starting level | Target level | Source |
|---|---|---|---|
| Total number of open services[51] in the state network | 50 | 16 | State Information System Authority |
| Total number of open services in Estonian cyberspace | 26 000 | 8000 | State Information System Authority |

50 The indicators are based on the RAPID7 National Exposure Index https://www.rapid7.com /

51 An open service is a service provided in Estonian cyberspace, which is accessible to all internet users but should not be accessible to all internet users (such as administration interfaces that should not be available).

## Activity area 1.1
## Making technological resilience more effective

Functioning cybersecurity covers the whole information system and service life-cycle starting from **architecture**, which is an organic part of service. To allow this principle to have a practical outlet as well, both technical design and process design and regulatory requirements must be considered when developing state information systems and digital services. Security competence and testing must go hand in hand with service design right from the start of the development process.

2018 saw a new Cybersecurity Act come into force, which transposes requirements from the European network and information security directive and the GPDR into national legislation. Regardless of separate regulations, it is no longer to take an approach to data protection and information security as separate disciplines, nor is within capabilities. Thus, in planning further activities, we will proceed from the principle that even though the regulations are separate, the implementation of **information security and data protection requirements** must be treated as a whole, ensuring reliability of the development and operational process, striving toward harmonious and holistic implementation. This approach will require a legal space and administrative system to make it possible and support the process.

In addition to managing acute risks today, **the long-term view must be considered.** There is reason to believe that by the end of the strategy period, a large part of the core technologies of Estonia's e-state will have undergone major developments, and that goes for encryption algorithms as well. The Estonian digital ecosystem is particularly sensitive to developments in cryptography and related threats, as the solution used for government-issued digital identity is based on it. We must protect data and guarantee the validity of digital signatures even decades down the road. Strategically, readiness for this will require us to ensure adaptivity and response capability, adherence to the no-legacy principle — i.e., giving up obsolete systems and software.

### Adherence to information security and data protection principles in the state information system architecture

The state's information systems and digital services must be developed securely right from the start, considering both technological and organizational requirements, principles and standards. This will ensure that new services and databases are built using the principle of security and privacy by design. The adoption of most public sector IT solutions considers the aspect of security, but responsibility is decentralized and central support is not sufficiently systematic. Making the principle of security and privacy by design more effective and systematic should be done by the creation of a system of instructional materials for ensuring the quality of development processes along with a feedback and control mechanism. This will provide the necessary guidance and support, while following the principle that ensuring security is the personal responsibility of every service owner.

### Broad-based implementation of baseline security requirements

When it comes to ensuring the state's cybersecurity, it is of key importance that parties adhere to basic security requirements stemming from information security solutions at least at the level required by law. The basis for ensuring information security at public sector institutions is the adherence to basic security requirements based on the three-level ISKE baseline IT security system, which has been in force since 2003.[52] Today ISKE's complexity is still a problem and smaller parties such as local governments see it as beyond their capacity, above all from the administrative point of view, to implement. Besides government institutions, small businesses, NGOs and individuals also need guidance and support in managing cyber-risks and complying with data protection/info security requirements. To ensure the applicability of basic security requirements in the necessary extent, additional support from the state is needed to systematically ensure the availability of a simple tool, instructional materials and trainings. The aim is to create an updated, systemic and broadly used baseline security requirements system that covers data security and data protection minimum requirements. It will provide support for those subject to ISKE or equivalent information security standards[53] and smaller service providers and businesses as well. In addition, it should be considered that the information security requirements stemming from baseline security standard will not remain static; they will have to be kept updated systematically. The organization of Estonian information and network security must stem from the best international standards that have been localized and adapted to Estonia's needs. In 2018, BSI IT-Grundschutz, which is the basis for all of ISKE, is being updated, and this would also reform Estonian ISKE, transitioning, among other things to risk analysis-based organization of information security: this means that as a part of ensuring information security, risk analyses will start to be prepared by all government institutions and vital service providers. By updating the baseline security requirements system, the legislation pertaining to ensuring of security of information systems will also be reviewed to decrease the administrative load arising from various regulations and implement integral data management. To ensure the coping of institutions with limited capacity with the adherence to security requirements, the centrally provided information security services will also be systematized to make their outsourcing a more easily available alternative.

52 Information security standard published by Germany's *Bundesamt für Sicherheit in der Informationstechnik*, English: *Federal Office for Information Security*) avaldatav infoturbe standard — IT Baseline Protection Manual (German: *IT-Grundschutz*).

53 Government institutions and service providers for the purposes of the Cybersecurity Act, including digital service providers

### Ensuring secure exchange of data between government institutions

It is critical important for the state to ensure secure and functioning communication and data exchange between systems meant for various areas of administration and authorities (including telephone communication and internet connection). To do this, it is planned to develop for the first time a comprehensive vision — a state communication concept that will map out the need for communication on in both ordinary and crisis situations. Based on this, it will be possible to map development needs, plan activities and put in place the division of tasks and how they are organized between different parties. Further, it is planned to continue expanding and developing the state data communication network and the transition to encrypted e-correspondence and data communication for ensuring secure communication between government institutions.

### Ensuring the security of critical databases necessary for the functioning of the Estonian state

The preservation of Estonian statehood means increasingly not only defending Estonian territory but also maintenance of digital assets. The digital assets that require protection the most are the basic data the state has on citizens, the territory of the state and legislative drafting — in other words, databases of critical importance.[54] If critical data for the state are modified in unauthorized fashion or destroyed, there is a risk that the state cannot manage its principal duties. To ensure the security of critical databases, it is not within capabilities to maintain the existence of data centres at a uniformly high level at all government institutions, as this would require major investments. A cost-effective solution for ensuring a standardized level of data security is being developed — to move critical databases and the most important Estonian e-services to the government cloud.[55] Outside Estonian territory, a network of data embassies will be developed, and from there applications and databases could be activated.[56] Both in the case of government cloud and the data embassy solution, high availability is ensured based on the principle that the data stored there can be used and the services operated in real time. That means that if Estonian data centres become inoperable for any reason, the state can provide critical services remotely via the data embassy's technical solution. To ensure sustainability the next step will be to

54 Critical databases include the Land Register, Commercial Register and Population Register. The updating of the list takes place regularly in cooperation between the cybersecurity council and architecture council.

55 Government cloud is a cloud environment administered by the State Infocommunication Foundation, which enables government institutions and vital service providers to use convenient and secure cloud solutions (https://riigipilv.ee/ ).

56 As of 2018, one data embassy in Luxembourg's state data centre has been launched. The possibility of setting up additional data embassies will be analysed on the basis of the Luxembourg project experience.

develop a systemic set of rules for regularly updating the list of critical databases and the security and backup requirements applicable to them, and also create a legal framework for determining parties involved in maintaining critical databases and their roles.

### Systematic assessment and administration of risks related to next-generation technologies

Even though future risks are largely unpredictable, Estonia will have to develop definite principles and political anchor points on key issues regarding future technologies. Coping with future risks will require discussion in society, and to do this, complicated information and technical messages need to be sent out in a comprehensible manner, without "dumbing things down" and gliding over key details. With such an approach, we will make sure that indeterminate risks can also be addressed based on competence and knowledge, not reactively and based on fears. To achieve the goal, we will have to rely on research competence and in priority fields for the Estonian state such as cryptography, blockchain technology, AI and secure identity management, we will have to ensure that the development of critical capabilities and competence are represented at the level of fundamental and applied research.

In order to practically mitigate technological risks, we envision mainly keeping IT solutions up to date, ensuring architectural solution that allow changes to be introduced flexibly and the existence of alternative solutions. Besides prevention of cyber threats, keeping up with new technologies and advances will be important in the fight against cybercrime and potential hybrid threats.[57]

In the international view, we are increasingly linked with global developments and are an integral part of the European IT landscape — for this development to accommodate Estonia's interests and needs, it will be necessary to participate in dialogue in international formats. As a country, we are inevitably integrated with private sector and major manufacturers'' services (Google, Apple, Microsoft etc.) — the potential impact of these degenderizes was illustrated tellingly by the ID card crisis in autumn 2017. To cope with such risks and dependencies, we have to develop a competence centre that is able to assess the security of technologies and services and has a central overview of the main risks, provides advice to public and private sector institutions on matters related to future technologies and is included in international formats.

57 A hybrid threat is one that combines elements of conventional and non-conventional methods that states and other forces can use in coordinated fashion without resorting to official warfare. Besides directly causing damage and exploiting vulnerabilities, the goal is also to destabilize society and create insecurity that hinders decision-making processes.

## Activity area 1.2
## Prevention of, readiness for and management of incidents and crises

During the two strategy periods, the main emphasis of state cybersecurity has lain on ensuring continuity of vital services and prevention of incidents with a significant impact. During the last four years, a nationwide 24/7 monitoring and incident resolution capability (CERT 24/7) and there exists also the framework necessary for prevention of and response to cyber incidents in regard to vital services for the state and private sector — the Emergency Act and the Cybersecurity Act create a sufficient legal framework for managing more serious risks. To this point however, a problem area is the preparation of risk analyses and continuity plans and their fluctuating quality. A challenge addressed during the current strategy period is the attainment of a new level in risk management, the practical implementation of the legal framework that is in place today, and the transition to a capability-based resolution of cyber crises, which means that specific capabilities of different institutions, thus ensuring optimum response capability and more effective use of the state's resources.

### Strengthening capability for early detection and prevention of cyber threats

Today, Estonia has above all a qualitative overview of the situation concerning developments and in cyberspace and the cybersecurity situation, but lacks a quantitative overview that is consistently prepared, comparable in time and based on clear indicators that could be used to assess the health of cyber space on objective grounds and make executive decisions. The state is constantly monitoring its network and attack space, measuring specific incidents, events, technical data and their dynamics. The next step is to develop situational awareness tools for systematic analysis of technical monitoring data and an automated quasi-real-time snapshot is developed that will measure the technical cybersecurity level, allowing conclusions to be drawn regarding the maturity of Estonia's general cybersecurity, ensuring comparison with respect to time for illustrating the developments and creating a comparative basis with other countries.[58]

Substantively implementing the Cybersecurity Act will provide a basis for evaluating and managing risks and determining responsibility at the company level. To ensure the security of information systems of service providers[59] who are important for society, and yield an up-to-date and integral understanding of the threat trends and early detection of threats, a systematic and continuous overview of the architectural security and traffic in service providers' networks and cross-de-

58 Above all, the Nordics and Baltic states are comparable to Estonia

59 Vital services are the services defined in the Cybersecurity Act, where the definition stems from the concept of operators of essential services in the NIS Directive. This is a broader definition than the list of vital service providers in the Emergency Act.

pendencies and cross-border dependences. To do this, a network monitoring system will be developed, of which a working prototype exists as of the start of the strategy period,[60] the implementation of which will be expanded to private networks and analytical capability will be increased through automating monitoring and further development of solutions. To gain a retrospective look in more important public sector databases and information systems, a central obligation will come into effect to maintain critical logs.[61] To test security, practical attack/penetration tests will be carried out in a significantly greater volume, which will show whether and how potential attackers can achieve access to the critical assets management, communication or IT systems of the tested establishment, following by provision of specific recommendations and a regular control mechanism.

To determine the cross-dependencies and cross-border dependences of vital service providers, a primary study was conducted in 2016. The next ambition is to develop a conception for dealing with cross-dependencies and cross-border dependencies. The inter-dependencies between the critical network and information systems used for provision of vital services and ensuring the functioning of the state will be determined societally. The goal is to possess a systematic overview of the most important cross-dependencies and cross-border dependencies and encourage institutions to adopt measures to hedge the risks.

For a better overview of the situation facing state networks and information systems, government institutions and local governments will be connected in as great an extent as possible to the state network. To ensure better network security, a pilot project will be conducted to implement a central system for preventing intrusion.

To mitigate cyber risks in the private sector in general, demand and supply of cyber insurance service[62] in Estonia will be analysed and on that basis, cooperative principles for related parties will be agreed upon, including information sharing, preparation of risk assessment etc. Today, suppliers of cyber insurance service are few on the Estonian market and it is necessary to first map who offers what. The complexity of insurance protection is often considered a hindrance to the development of the cyber insurance market.

60 In the context of the prototype completed by end of 2018, interfaces have been created for the government institutions and private sector providers included in the project for exchange of information and data streams, plus resources for data analysis.

61 The set of critical logs include the detailed trails of all applications' authentication actions and detailed trails for all incoming queries received by publicly accessible services on the internet.

62 OECD, Enhancing the Role of Insurance in Cyber Risk Management. https://read.oecd-ilibrary.org/finance-and-investment/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en#page

### Integrating cybersecurity with planning of national defence and preparedness for coping with crises

The objective is first to include cybersecurity in national defence planning and exercises, which will ensure planning of cybersecurity activities and capabilities pursuant to the risk scenarios underlying planning of national defence. By these means, the country's capability to operate in cyberspace to repel security threats and resolve national defence crises will be increased. Secondly, cybersecurity will continue to be integrated with plans ensuring readiness of government institutions and vital service providers and risk assessments. Through these activities, the capability of preventing cyber risks from becoming realized in Estonia and escalating into crises will be raised. Readiness for resolving crises caused by cyber threats or incidents and performing damage control will also improve. As one capability that will be developed, a uniform situation map of Estonian cyber space generated in real-time will be developed and shared with all key parties. To ensure practical readiness to cope with crises, regular joint cooperative exercises will be held with the state's political leadership, vital service providers and structures that ensure military defence. Capability-based resolution of cyber crises will be implemented in the public sector to make optimum use of the competence of various institutions.

## Activity area 1.3 Integral management of the sector and shaping a cohesive community

Ensuring cybersecurity that is based on optimum cooperation and interoperability, inclusive, dynamic and effective is a key prerequisite for achieving the vision of the entire strategy, enabling maximum use of Estonia's limited resources. Important dimensions of cooperation and interoperability are integral management, inclusive planning and a functioning community.

### Integral management of the cybersecurity sector and consolidation of capabilities

The basis for ensuring nationwide cybersecurity is the systematic planning of the necessary capabilities, a well-functioning cooperation and interoperability and management of the cyber sphere as a whole, not based on jurisdictions. To plan resource and activities across the entire breadth of the state and to do more with existing resources, the first step is to map the capabilities of various ministries' areas of government when it comes to cybersecurity, areas where they overlap and shortcomings, in the course of a sector capability audit. Based on the results of the audit, the state situation snapshot and management of the administration of government network security will be consolidated. As a preliminary step before this activity, the nation-wide cybersecurity centre (NCSC) will be established on the basis of the State Information System Authority's cybersecurity

division, which will see further development based on the results of the audit. For the purpose of unified management and cross-institutional planning of nation-wide cybersecurity policy, the Ministry of Economic Affairs and Communications in cooperation with other ministries and the cybersecurity council and with the support of the Government of the Republic's security committee, organizes the coordinated implementation and updating of the cybersecurity strategy.

### Shaping a unified cybersecurity community and ensuring a consistently inclusive planning process

One of the foundations of the unified functioning of the field is good movement of information, strong partner relations and personal contacts between and among experts from different fields, encompassing government institutions, the private sector and academia.

Strong, cohesive everyday cooperation that is based on a community culture has been a basis for Estonia's success so far in ensuring cybersecurity and preventing incidents with extensive consequences — this practice will be continued and strengthened in the new strategy period as well. To include a broader community, the cooperation formats involving information security leaders and managements of vital service providers for government institutions and the public will be reinforced, including in strategic planning processes. Effective domestic cooperation between different agencies is a precondition for both ensuring cybersecurity, achieving the priorities of international cooperation and keeping cybercrime under control. To do this, domestic cooperation formats will be provided, the necessary interinstitutional cooperation agreements for ensuring productive cooperation will be effected, and interinstitutional rotations for direct sharing of competence will be promoted.

# Cybersecurity Industry, Research and Development

**Objective 2: Estonia has strong, innovative, research-based and globally competitive enterprise and R&D in the cybersecurity sector, covering the key competences that are important for the state.**

In universities, private companies and public sector alike, Estonia has outstanding competence in different spheres of cybersecurity, above all in the fields of secure digital identity cryptography, data integrity, cybersecurity skills, education and exercises. To develop internationally successful research and development and enterprise in the sector, Estonia will clearly have to focus on its unique strengths, which are above all its ecosystem based on electronic identity and the secure architecture of the X-road data layer along with its trust services. Strong sectoral competence in the private sector and research institutions means that Estonia will have potential for economic growth as the sector grows as well as readiness for coping in crisis situations as hiring all of the competence needed in the public sector is not a feasible option.

**Performance indicators:**

| Indicator | Starting level | Target level | Source |
|---|---|---|---|
| Export volume of companies in the sector[63] | 15,86 million | /to be determined/ | Cyber sector workforce need study[64] and the growth area promotion study[65] |
| Number of new start-ups in the cybersecurity sector | 22 | 42 | Start-up Estonia |
| Number of doctorates defended in the cybersecurity sector | 1.7 doctorates per year (during the period 2014-2017) | 2.5 doctorates per year (2019-2022) | TalTech, University of Tartu |

63 It is a challenge to define cybersecurity as a sector, as it cannot be done automatically based on Commercial Register data. Professional organizations' resources and regular surveys must be used.

64 Praxis (2018)

65 TÜ, TalTech, Technopolis Group Eesti OÜ (2018)

## Activity area 2.1
## Supporting and promoting cybersecurity R&D and research-based enterprise

The objective is to create effective cooperation and better cohesiveness between research, enterprise and government to improve the capacity to take developments in universities to applications in private sector and state services. Estonia's small market can be seen as an advantage in the incubator phase, where a product working at the level of society can be rapidly taken to completion. The most important prerequisite for achieving the strategic goal is ensuring functioning cooperation mechanisms between academia, private business and government institutions, which will ensure that strategic priorities will guide the focus of R&D in academia as well as in the private sector, thus ensuring the existence of key competences for the state.

### Leveraging productive cooperation between private sector, state and academia

To enable productive cooperation, there is today an information and cybersecurity cluster called the Estonian Information Security Association — EISA. It supports cooperation between universities, business and government. The next challenge is optimally launching the new cooperation format to create the possibility for the competencies to meet and ensure an administrative support mechanism for unified cross-sectoral participation in bidding on international contracts and competition, thereby ensuring preconditions for amplifying export and raising funding for research. At the same time, a contribution will be made to create possibilities for developing ways for the defence industry to take part in the EU's defence initiatives like the European Defence Fund and the European Defence Industrial Development Programme.

### Preparation of a nationwide cybersecurity R&D plan that defines priority focus areas for the state

Estonia lacks a uniform R&D plan that deals with information society and cybersecurity and their technical solutions. The ICT development programme initiated by the cabinet[66] covers the corresponding measures to a limited extent and specifies the primary cybersecurity research areas. Also providing impetus for research in the field of ICT is the research measure launched as part of the IT Academy programme in 2018. The next step in light of the broader strategic plan is to establish a coordination mechanism and define the focus areas for R&D in the field of cybersecurity. Based on priority research issues for the state corresponding to them, guidelines can be provided in future for R&D conducted at universities and

66 ICT sector development programme concept

companies, for providing substance to support measures for companies and educational projects and scholarships.

### Support for innovation generation and export potential

To improve the sector's global competitiveness, the creation of innovation and increase in the volume of productization must be promoted. To do so, innovation support measures aimed at the cybersecurity sector must be systematized and their active adoption must be supported. To amplify export potential, the state should find ways to engage (small) companies in the cybersecurity sector in business diplomacy visits and delegations.

The NATO cyber training ground operated by the Defence Forces also has potential for supporting development of companies and creation of innovation — a virtual environment that enables information and communication systems to be built and run through situations that cannot be done in the networks used daily. The primary goal of the cyber training ground is to consolidate cyber defence exercise and training experience but the applications can be broadened. By developing the Open Cyber Range platform further, allowing to offer solutions to sectoral (start-up) companies and universities for carrying out R&D activities, testing and products and training.

To enable effective cooperation between public and private sector for productizing novel solutions commissioned by the state, the regulations on handling of intellectual property need to be updated as well,[67] as today they are focused on products and services in the physical space, without taking into account the essential characteristics of digital environment. In the first phase, it is planned to map in more detail today's situation and the range of problems, considering the current procurement and licensing practices at institutions, best practices and regulations in other countries and specific features of cybersecurity solutions. Based on the analysis performed, an integral state software intellectual property rights strategy can be developed, one that would support the development of Estonian software companies and their competitiveness in the world and introduce the necessary legislative amendments to make it possible. The goal is to create the opportunities flexibly and to commercialize the software commissioned by the state in a manner that promotes the development of enterprise so that the intellectual property rights to the software might be held by private enterprises that developed the software and the state licenses the right to use it, while the state is guaranteed the possibility of patching and developing the software further for its purposes.

67 Governed by the State Assets Act

### Ensuring an environment conducive to the inception and development of start-ups

The goal of the state is to ensure the optimum environment for the inception and growth of companies developing cyder technologies — that also means support activities aimed at the start-up community in the sector. Today, a two-year pilot phase made possible by cooperation with Startup Estonia and the Ministry of Defence is behind us, during which functioning cooperation formats and network were built and a small number of potential start-ups' teams took shape. In the new strategy period, Startup Estonia will continue developing the community in cooperation with the Ministry of Economic Affairs and Communications to support initiatives for organizing regular seminars and events, launch regular mentorship programmes and move ahead upon reaching a sufficient development level with creating an accelerator for companies in the cyber sector to offer value for global growth of companies that are past the first development phase.

# Leading international contributor

## Objective 3: Estonia is a credible and strong partner in the international arena

The strength of Estonia's cyber trademark requires a conscious and integral approach to international topics. Estonian foreign relations on cyber themes must be proactive to keep up with the stiffening global competition. In this endeavour, Estonia can rely on its existing strengths, but it will have to continue to develop areas where Estonia could be in the lead role and continue to be globally visible. As a good example, the NATO CCD COE in Tallinn makes it possible for Estonia to be in the lead role on NATO cyber defence issues. IN addition, it should more actively be involved in the EU's international cyber initiatives and continue participating in the UN, Council of Europe, OSCE and other international organizations' cybersecurity cooperation formats. Considering Estonia's successful experiences in conveying cyber expertise to this point, activities related to development

International cyber defence exercise Locked Shields. (Photo: CCDCOE).

cooperation in the field of cybersecurity should be made more effective. It should also be involved in cooperation between like-minded countries when it comes to cyber deterrence, attribution of attacks and collective countermeasures. It is also important for law enforcement bodies to work together actively at the international level, which is a precondition for solving cybercrimes successfully and offering more effective protection.

There are two activity areas for achieving the objective:

→ Making cooperation with strategic foreign partners more effective

→ International promotion of sustainable cyber capability

**Performance indicator:**

| Indicator | Starting level | Target level | Source |
|---|---|---|---|
| Annual expert assessment from the Ministry of Foreign Affairs and other responsible institutions[68] as to the substantive quality and focus of Estonia's international relations. | Cooperation with international organizations and other countries takes place through individual initiatives, which are structured unevenly through different sectors and institutions. There is a lack of an integral and systematic overview of cooperation mechanisms so that resources can be used pursuant to Estonia's foreign policy priorities. | → Under the leadership of the Ministry of Foreign with the involvement of other responsible institutions, cooperation with different international organizations and other countries is coordinated in a meaningful and systematic fashion.<br>→ The basis for creating the systematic approach is Estonia's foreign policy priorities.<br>→ In cooperation with strategic foreign partners there is a strong practical dimension in the form of joint exercises and technical exchange of information, which ensures successful resolution of incidents. Estonia has increased its visibility through increasing development cooperation. The Ministry of Foreign Affairs is the central institution through which exchange of information takes place as regards rotation of cyber diplomacy experts at international organizations. | Ministry of Foreign Affairs |

68 Ministry of Foreign Affairs, Ministry of Economic Affairs and Communications, State Information System Authority, Ministry of Defence

## Activity area 3.1
## Making cooperation with strategic foreign partners more effective

Estonia's main interest in international relations in the cybersecurity field is to ensure stability in cyberspace through its own participation in bilateral and multilateral cooperation. To do this Estonia engages in intensified cooperation with key allies at the political and practical level, including in the context of larger international organizations. One example of Estonia's international cooperation to this point is the field of cyber norms, trust measures and international law, where it will be important to continue Estonia's participation in UN and OSCE processes. The prerequisite for intensified cybersecurity cooperation with the closest partners states is relevant cooperative frameworks and procedures and their regular implementation. Estonia also has a considerable and globally competitive expertise in this field, which merits additional development. To keep cooperation formats competitive, sufficient funding must be ensured. International cooperation with various key partners for cyber exercises is critical for national defence and general cybersecurity. It is in Estonia's interests to ensure the successful resolution of cyber-attacks, for which cross-border cooperation must be maintained and promoted, including ensuring rapid and effective obtaining of procedural information from other countries and strengthening general exchange of information and cooperation.

Estonia's inclusion in international discussions and processes related to cybersecurity is ensured by the capability to hold substantive dialogue with key partners. To maintain a substantive dialogue, Estonia must be able to contribute on the international arena with information and analysis of cyber incidents and attacks.

Throughout all aspects, it is important to coordinate international activities domestically, and to ensure this, a strong and consistent coordination format will be maintained. This will ensure that Estonia's international messaging is relevant and consistent and that all international actions follow the commonly agreed priorities.

### Estonia must be sufficiently represented and have competence on cyber topics at Estonian foreign representations and at the EU, NATO and the UN

The objective of the activity for Estonia to have a visible footprint on European Union and NATO cyber cooperation and a continuing participation in UN cyber processes. The precondition for achieving the objective is substantive messaging and expertise in setting foreign policy goals.

The prerequisite of successful international cooperation is for Estonian diplomats and other officials representing Estonia to be capable of forwarding uniform messages coordinated domestically regarding policies in the Estonian cybersecurity field. Estonia's active participation in the EU, NATO, UN and other international

organizations' processes allows the country to advocate better for its interests and priorities. To maintain cyber competence up to date, the cross-institutional rotation of diplomats and officials should be promoted along with knowledge sharing. Including experts from the cybersecurity field into the foreign service allows more multifaceted and technical knowledge into policy planning processes, which in turn will contribute to taking higher quality decisions at the international level.

The Ministry of Foreign Affairs has a strong role to play in this field, as its function is to train diplomats on cybersecurity topics and ensure that they have sufficient cyber competence; and to develop a rotation for cyber experts serving at international organizations.

### Estonia contributes to processes of shaping international law by lobbying for its positions

Through Estonia's active contribution, the number of countries that actively recognize the validity of international law in cyberspace and work to this end actively. The field of cyber norms, trust measures and international law are an important global process in cybersecurity policy, and here it is important to continue Estonia's existing successful participation in UN and other processes. The development of certain specific fields is also considered; for example, it will be important to develop competence in analysis of validity of international law, which to this point has received spotty coverage. The issuing of the Tallinn Manuals by NATO CCD COE has been a success story that should be made a fixture in Estonia's image. Estonia's positions should be visibly presented in various cooperation formats, ensuring that their impact can be felt in internationally agreed upon positions.

### Estonia develops bilateral cooperation formats with key partners and regularly holds joint exercises

The objective of the activity is to develop substantive cooperation with key partners, including the mutual sharing of analyses, technical information and practical knowledge and experiences. The Estonian state's cyber awareness, readiness and capability of establishing and dealing with new threats and reliability will be increased by way of engaging in active cooperation through partners and holding regular exercises. For Estonia, it is important to engage systematically in bilateral cyber cooperation with various key countries and the cyber agencies located there, and the cooperation should consist of political dialogue, regular sharing of analyses, cooperative events and other cooperative formats.

### Estonia takes part in international defence cooperation and contributes to increasing cyber stability

The purpose of the activity is to ensure that Estonia has a strong image as a recognized conscientious partner in international defence cooperation and con-

tributor to increasing international cyber stability. It is important to determine the necessary priorities, establish regular dialogues with different strategic partners both in bilateral cooperation and with international organizations (particularly, the EU, NATO, OSCE and UN). Developing collective countermeasures to cyber-attacks will be based on bilateral and multilateral international cooperation. Active efforts in the context of larger organizations is important, especially in strengthening EU and NATO deterrence stances. Also helping to reinforce Estonia's active role in the cybersecurity field are large-scale exercises held in Estonia (such as Locked Shields or Cyber Coalition).

It is in Estonia's interests to be cohesive with the allied military presence (NATO eFP — Enhanced Forward Presence), including in the cybersecurity field. That means development of new cooperation mechanisms and procedures for establishing a common view of cyber threats and situation, which contributes to a stronger NATO deterrent stance in the region. Estonia will need to enter into the relevant cyber defence cooperation frameworks and organize regular joint exercises.

The goal is to develop in Estonia, at the political, legal and technical level, a working procedure to attribute cyber-attacks and to take part in deterrence and attribution related cooperation formats with likeminded countries.

## Activity area 3.2
## International promotion of sustainable cyber capability

A secure, trustworthy and stable cyberspace is a prerequisite for the use of functioning and effective digital solutions and thus an important field for many countries in developing their digital sectors. Estonia has, already today, potential to become an important cyber capability promoter worldwide and to take part in larger EU and other international projects. Estonia's active participation in creating an EU cyber assistance network and in promoting a sustainable and competitive cyber capability will help Estonia continue to be in the ranks of leading cyber states and also bring in additional resources in the form of foreign projects.

Estonia has competence in creating and building a national cyber coordination model, which could be shared with other countries. Provision of cybersecurity assistance is only in an early stage and at the moment, there are no organizations at the international level that would be able to coordinate cooperation between donor countries and offer development of cyber capabilities in destination countries. The EU has decided to create a network that would start dealing with consolidation and development of cyber competence for new assistance projects. Estonia could fulfil many goals in activities in the field of developing the above-mentioned cyber capabilities that are currently not covered.

### Estonia makes a leading contribution to ensuring competitive and sustainable cyber capability in partner countries and takes part in creating a European Union cyber assistance network

The objective of the activity is to ensure that Estonia would be able, if necessary, to promote a competitive and sustainable cyber capability in partner countries. Estonia can share its experiences with other countries, by taking part in EU, NATO and other international projects. In addition, specific fields that are within Estonia's capabilities and necessary for Estonia must be defined in international digital and cyber cooperation — for example, planning of policies and strategies in the cybersecurity field, e-governance, a certain geographic focus, countries in other regions, etc. In cooperation with RIA, TalTech and other institutions, a corresponding training system should be developed, the value added would also be the inclusion of Estonian IT security and cyber defence industry in cooperation projects and introduce those projects. Being involved in international standardization and certification processes is also important.

It is also important for Estonia to systematically support the development of cyber capabilities outside EU and NATO and to do so, Estonia could for example take part in creating the EU cyber assistance network to develop a competitive and sustainable cyber assistance provision capability that would in turn reinforce Estonia's identity as one of the world's leading cyber countries and bring in additional resources for Estonia.

# A cyber-literate society

**Objective 4: As a society, Estonia is cyber literate and a future supply of specialists in the field is guaranteed.**

In 2015, 30% of internet users in Estonia had some contact with a security vulnerability.[69] On the private sector side, the general ability to cope with attacks is reflected by the low awareness of the implementation of security policies, as only 17% of all Estonian companies had implemented security policies as of 2015.[70]

For all members of society to be able to operate securely in cyberspace, it is top priority to ensure a future supply of specialists for organizations responsible for cybersecurity, devoting attention to talent search programmes, and formal and continuing education. A clear demand for specialists is seen in three groups — public sector institutions responsible for cybersecurity, vital service providers and enterprise in the cyber field.

It is necessary to keep talking about the prevailing risks to the general public, dispensing advice for mitigating risks and emphasizing that development of knowledge and skills in the field of cybersecurity is the joint responsibility of everyone in cyberspace.

To achieve the objective, activities will be implemented using two activity areas:

→ Raising cyder awareness among citizens, state and private sector

→ Developing talent corresponding to state and private sector demand

69 Information technology in households 2015 www.stat.ee

70 Information technology in companies 2016 www.stat.ee

**Performance indicators:**

| Indicator | Starting level | Target levels | Source |
|---|---|---|---|
| Percentage of those who sustained losses from being exposed to a security vulnerability online (%)[71] | 44.8% (2010)<br>27.7% (2015) | ≤ 20% (2022) | Statistics Estonia |
| Use of an officially confirmed ICT security policy in companies (%)[72] | 16.9% (2015) | ≥ 25% (2022) | Statistics Estonia |
| Level of cyber awareness and skills among employees at government institutions and local governments, measured on the basis of a practical skills test | N/A (2018)[73] | ≥ 75% level satisfactory (2022) | State Information System Authority |
| Estimated workforce deficit[74] | /to be determined/ | /to be determined/ | Study of workforce needs in the cyber field: Praxis 2018 |

71 Share of internet and computer users aged 16-74 in the last 12 months who experienced at least one of the following security vulnerabilities: Infection with virus or other malware resulting in lost data and/or time; abuse of personal data entered on the internet or other infringement of privacy; financial losses sustained from following instructions in a malicious email, spoofed website; falling victim to card fraud; children accessing inappropriate web content.

72 Sample included companies with 10+ employees.

73 The starting level will be determined according to results of the target group taking the test as of the end of 2018.

74 In 2018, a cyber workforce study was commissioned by the Ministry of Economic Affairs and Communications for the first time. It mapped cybersecurity specialists' professional profiles. As a result, the need for workforce today and in five years' time was assessed. The assessment of availability of workforce was provided to the companies in the sample as a subjective rating and this pinpointed the 2018 status. If the various measures are successfully applied, the workforce deficit or perceived deficit will not have grown by the end of the strategy period.

## Activity area 4.1
## Raising the cyber awareness of citizens, state and private sector

Rapidly changing cyberspace leads to the neds to deal consistently with developing the knowledge and skills of different target groups. To achieve this, on one hand it will be necessary to have a constant overview of the threat trends and on the other hand, the level of knowledge and skills among various target groups. Cybersecurity is a keyword that has become important not only in the IT field but in all walks of life. Different parties emphasize the importance of component skills in the digital competencies acquired at the general educational level[75] including in cybersecurity — the better the baseline skills and knowledge young people emerge with, the easier it is in later educational levels and continuing education to deal with developing more specific skills. Early exposure to IT studies (e.g. programming, robotics etc.) in general education is an important positive influence factor for continuing studies in ICT specialities, including on the cybersecurity front.

On the job market, mid-level managers and top executives, providers of essential services and employees of government institutions (including local government) have become an ever more critical target group with each passing year. Continuing to make up a risk group are private firms and small businesses, who often lack the capability to cope with cyber incidents on their own — each month, about 10 private businesses turn to RIA seeking help.

As a result of the foregoing, activities related to raising cyber awareness will be consolidated in a common platform and possibilities for independent learning will be offered. Cybersecurity will be dealt with in the educational systems at all levels of education as part of developing digital competencies.

### Activities for raising awareness aimed at the general public will be carried out

Over the years, institutions with clear roles and responsibility have developed within Estonia, who look after ensuring cybersecurity including deal with spreading information to the general public. At the same time, this has over time led to fragmentation of information and some overlapping of activities — information on cyber cybersecurity has become divided among a number of (project-based) environments (such as the RIA blog,[76] the Police and Border Guard Board website,[77] *Targalt Internetis* project website) and there is a lack of a central channel for putting out information to citizens. Estonia also has untapped potential to offer e-courses (MOOCs) and independent learning opportunities that contain local context.

75 Learner's digital competency model

76 https://blog.ria.ee/

77 Police and Border Guard

As expected, the RIA 2018 yearbook notes that the lion's share of cyber events in 2018 affected the private sector, which has the greatest number of users. This includes both large and small businesses, NGOs and individual computer users whose digital dependency and cybersecurity awareness vary widely. It is also true that she importance of the functioning of digital solutions tends to be neglected and instead of risk prevention, security is scrutinized only after an incident occurs.

Based on the above, the objective of the activity is to achieve a situation where in cooperation between different agencies, the general public's awareness of cyber threats is raised, both in terms of protecting oneself against the dangers and what action to take after an attack. Following the entry into force of the Cybersecurity Act, RIA has taken the central role in cyber hygiene, state prevention activity and increasing awareness in society. Similarly to the Police and Border Guard Board and the Rescue Board, broad-ranging prevention and awareness campaigns will be launched to spread the word about cyber threats to different target groups, including businesses. A format will be created for coordinating activities related to awareness building in Estonia and information on preventive actions will be consolidated in a comprehensible and publicly available manner in one place. To raise the level of cyber hygiene at government institutions, it will become obligatory for government institutions' and local government employees to pass tests on knowledge of cybersecurity. Trainings and information outreach for target groups will be continued.

### Knowledge and skills of students and teachers will be measured systematically and a supply of training in the field of cybersecurity will be provided for general educational school and vocational school teachers

A key prerequisite and input for planning cybersecurity trainings will be to document the level of knowledge and skills, which at the current time is spotty.[78] Security is dealt with briefly in the state digital competence test held for the first time in 2018 and the *KüberPähkel* study/competition held for academic purposes.[79] At the same time, there are a lack of systematic comparable measurement results among teachers and students.

One important solution for raising cybersecurity awareness is coverage of the topic in general and vocational education. Estonia has an agreement as to what cybersecurity knowledge and skills youth should receive at the general education level and this is described in state curricula in the context of digital competence.[80] Curricula of electives have been prepared at both the basic school and upper

78 More research studies must be conducted in Estonia, and various tools must be created for better finding solutions for growing awareness of cyberdefence in society (cyberhygiene). Recommendations stemming from the overview of the *KüberPähkel* study 2018

79 www.kyberpahkel.ee

80 Digital competence in curricula


*KüberPähkel* study / competition. (Photo: Romil Rõbtšenkov).

secondary school[81] level along with corresponding materials that include methodological materials. These are a good basis for administering trainings. Yet there is a nationwide shortage of motivated and competent teachers who are able to teach the relevant knowledge integrated with other curricular topics — the cybersecurity topic is often not seen as a co-responsibility of school and teacher. To this point, thorough trainings that deal only with cybersecurity have been largely project-based (such as in the *Targalt Internetis*[82] programme, and in cooperation with the Cyber Defence League and TalTech).

That makes it important to keep up to date students' and teachers' cybersecurity component skills in digital competency models and systematically deal with measuring the competences. As a result of the activity, elementary levels exist for various target groups, they are comparable in time and provide an input into thematic trainings, and development of curricula and materials.

### A systematic, nationwide platform for government institutions and local governments for raising cyber awareness will be developed

The Cybersecurity Act that came into force in May 2018[83] puts the role of prevention and resolution coordinator on RIA; which means that for the first time the

81 To be completed in 2019

82 http://www.targaltinternetis.ee/

83 Cybersecurity Act

responsibilities of RIA that the institution has performed for years have been codified. For the better fulfilment of the coordinator's role, a central cyber knowledge measurement and training platform will be introduced as a tool, including central tools for government institutions, local governments and society for measuring the level of knowledge and skills, analysis and information outreach and training activity. As a result of the activities, all government institutions and local government units have begun to use cyberawareness testing (among other things, compulsory testing is now used in the case of all new hires in the public service); vital service providers can use them voluntarily as well.

### The knowledge and skills of the state's mid-level and top officials will be strengthened

Prioritizing cybersecurity in institutions depends directly on attitudes and knowledgeability of the officials. Yet the competency model for senior officials, developed by the Government Office,[84] does not include competences pertaining to digital skills (such as cybersecurity) and as a result there is no systematic approach to developing the corresponding skills. Analysing the activities of government institutions and local government units, one might conclude that information systems security is largely a management issue, and only then a question of resources. All too often, the lack of knowledge about cybersecurity is due to lack of interest and vice versa. Because of the lack of knowledge, too much is made of the dearth of resources as a hindrance. Organizations' IT personnel's knowledge in the field of prevention and minimization of losses have improved but the pattern of recurring incidents is still cause for concern. The recurrence of incidents of the same type shows that the top ranks of organizations are not sufficiently aware of the risks that routinely come up in the activities of employees or of their actual impact on the services provided by the organization.

To improve the senior officials' knowledge and skills, the level of knowledge will be mapped, trainings held (including on risk awareness and management) and exercises and higher cyber defence courses. As a result of the activities, the topic of cybersecurity will be integrated into the state's mid-level and top leadership training programmes and there will exist a good foundation for coping better in crisis situations.

84 https://riigikantselei.ee/et/tippjuhtide-kompetentsimudel

## Activity area 4.2
## Development of talent corresponding to state and private sector demand

The OSKA ICT workforce analysis conducted in 2016[85] showed that each year, the different economic sectors in Estonia required a total of about 1.5 times more ICT specialists. The same is shown by discussions with interest groups — the quantity and quality of graduates with a higher education degree does not meet demand on Estonia's workforce. There is also a lack of a detailed overview of the workforce needs and competencies in the cybersecurity sector. The latter has particularly critical importance for society in the context of sectors engaged in providing essential services — the specialists being hired must ideally get their specialized cyber skills from formal education (e.g. energy and communication engineers, healthcare professionals and others). Yet there is a lack of understanding of the specific needs for cyber skills in priority fields. The problem is the lack of descriptions of the relevant competencies in places like the professional standards and they are not integrated into the relevant curricula.

Although Estonian officials do have good cyber hygiene, incidents at government institutions show that solely raising cyber awareness does not guarantee security and the focus must lie on secure architecture, investment into compliance with requirements and ensuring the existence of information security competence at institutions.[86] Agreement must be reached on the content of skills and skill levels encompassed in information systems security competence and in the scope of the need by each institution. Thereafter it will be necessary to map the corresponding supply of higher education and in-service training in Estonia and abroad and create need-based support measures.

The goal is to ensure the cyber sector workforce needed by the state and public sector, developing for this purpose talented youths in formal education and non-scholastic activities and to train cybersecurity specialists in conformity with the demand for workforce.

### Cyber defence studies will be developed in general education schools and effort will be made to raise the potential of talented youths

As of 2018, national defence studies are being taught at 127 upper secondary schools and 22 vocational schools.[87] Cyber and internal security are viewed as a natural part of national defence studies, but the volume of lessons planned for conveying these topics is not sufficient for an in-depth approach. As a result, it is

85 Future view of workforce and skills needs: Information and communication technology 2016.

86 State Information System Authority Cybersecurity 2018

87 Source: Ministry of Defence

important to integrate cybersecurity with information science syllabi and facilitate in-depth cyber defence studies reaching as many upper secondary schools as possible and laying the groundwork for training a future supply of cyber specialists through the formal educational system.

While youth with an interest in ICT can participate in robotics and programming clubs, hobbyist/extracurricular activity in the field of cybersecurity is nearly non-existent. At the moment, Estonia also lacks a clear expectation and view of how and with what content to incite interest in cybersecurity among young people and thus create a rising generation of cybersecurity specialists. The format of compulsory military service as a targeted way of developing workforce in the cyber field is not being used. At the same time, through the contribution of the Ministry of Defence and the rest of the state sector, "cyber conscription" could be used as a primary recruitment platform.

To realize the opportunities described, a programme of extracurricular activities for talented youths interested in cybersecurity will be created based on the *Küber-Naaskel*[88] (competition) model. This in turn will create a pool for finding people who will complete their military service in a cybersecurity field and conscription would become a part of the cyber defence educational path and a state recruitment platform.

### A systematic overview of workforce needs for cyber defence specialists will be created

The abovementioned OSKA report describes the need for cyber competences within ICT core professions, but does not map the workforce needs for cybersecurity specialists specifically sought by the state and private sector. This is a significant link in the process of planning student places, determining academic areas with greater potential and the need for continuing education for top specialists, including external trainings and industrial PhD studies. In future, systematic research will ensure an overview of the workforce needs for cybersecurity specialists, which will be linked with policy recommendations. The studies will be a basis for strengthening cooperation in the field of talent development between companies and universities, which will ensure the up-to-dateness of curricula and the necessary competencies among university graduates.

### The quality of specialists in the cyber defence and internal security fields and of continuing education will be ensured.

In developing cyber defence studies, Estonia has thus far proceeded from the needs of the public and private sector, trying to furnish relevant curricula with as broad a spectrum of knowledge as possible. The cyber defence master's degree

88 www.kybernaaskel.ee

programme at TalTech and the University of Tartu has been acclaimed by international students. At the same time, it is necessary to analyse both the potential of academic and research areas to increase their funding and quality.

While the development of higher education in cyber defence can be deemed systematic as TalTech has the Centre for Digital Forensics and Cybersecurity , including all strategic partners, the in-service training of cyber specialists working for the state sector lacks a unified approach and planned resources, which can be seen as a risk in the context of broader cybersecurity management. The solution is to create a cross-institutional technical training system to support conversancy with innovations and risks and thereby reduce the number of security incidents and mitigate security risks in the most important government institutions.

For example, it must be ensured that specialists responsible for internal security get corresponding training. Today cybersecurity is dealt with only in the framework of an elective in the Academy of Security Sciences internal security master's programme. It is also necessary to create possibilities of continuing education for specialists already working in the field.

Besides this, the sector-specific cyber skills of specialists engaged in providing essential services to society must be mapped and integrated into the relevant curricula.

### Developing Estonia's international cyber law competency.

In 2016, the University of Tartu launched an IT law training and research programme aimed at education highly qualified lawyers for working in the ICT and cybersecurity sector. For the last eight years, TalTech has had a chair technology law. The existence of such academic units is a good precondition for establishing an international cyber law centre that would ensure that Estonia has sufficient expertise to actively contribute to international projects in the speciality and take part in thematic debates along with leading EU and NATO countries. The NATO CCD COE in Tallinn is a key competence centre in international law matters, but there is currently a lack of an organization in the entire EU for substantively taking the topic forward on the civilian side of international law. For planning further activities, first an analysis of an applied nature will be conducted for mapping the possibilities of creating such an international cyber law centre. The goal is to merge academic competence — well developed in Estonia — with foreign policy planning in the cyber field, create opportunities for training a future pool of experts in the law, and establish Estonia's cyber law competence through participation in international projects.