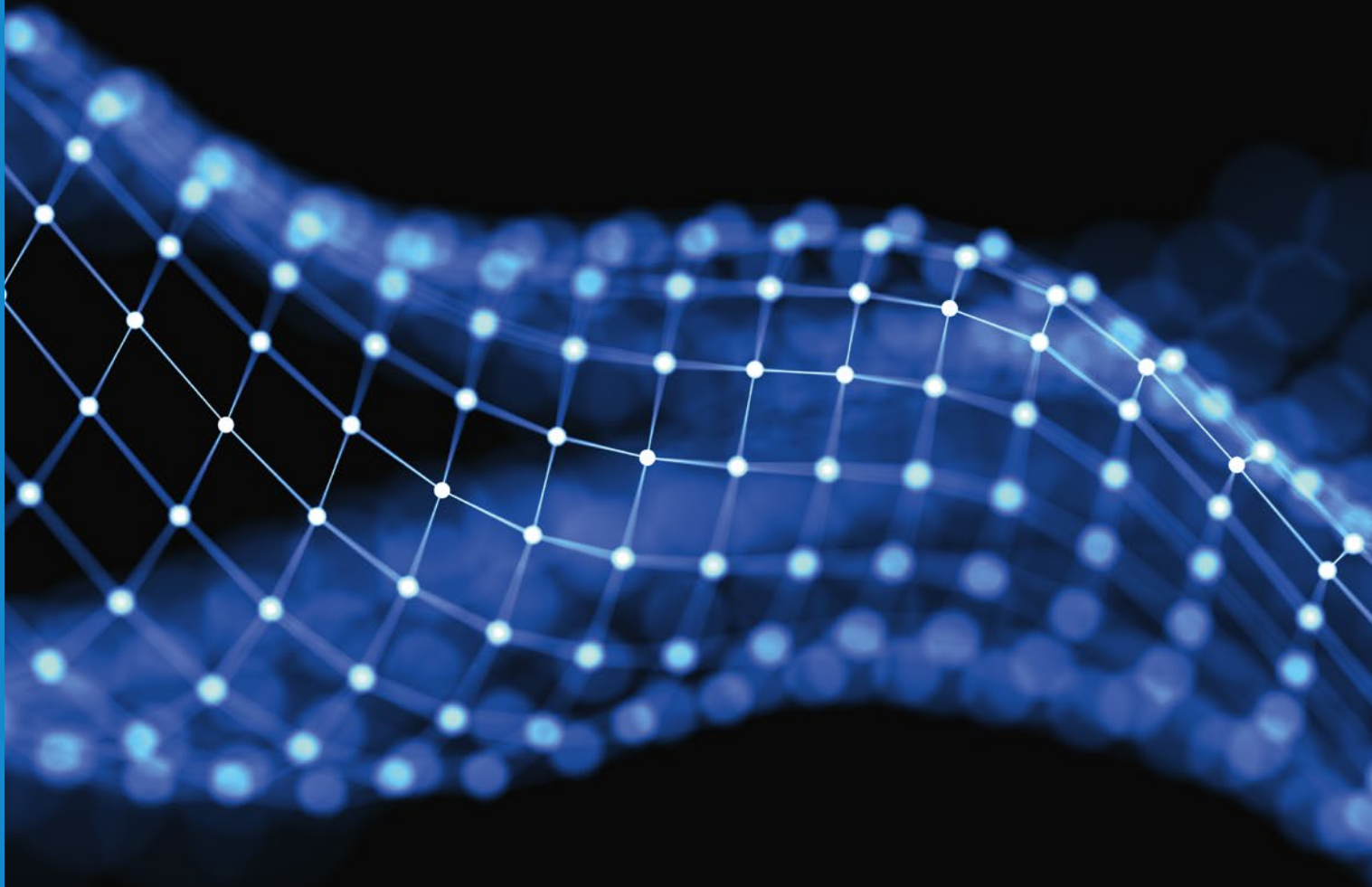


National Cyber Security in Practice



National Cyber Security in Practice

Publication composed by: Epp Maaten, Toomas Vaks
Contributors: Oskar Gross, Lauri Luht, Epp Maaten, Elsa Neeme, Kimmo Rousku, Toomas Vaks
Photos by: iStock
Design: Dada AD
Translation and editing by: Refiner OÜ

Published by:
e-Governance Academy
Rotermanni 8, 10111 Tallinn
ega.ee

The handbook “National Cyber Security in Practice” is financed by the Estonian Ministry of Foreign Affairs from the funds of development cooperation and humanitarian aid.



Tallinn, 2020
ISBN 978-9949-7467-1-2
© e-Governance Academy 2020

All rights reserved.
When using or quoting the data included in this issue, please indicate the source.

Contents

Foreword	5
Introduction	6
1. Resilient cyber security	8
2. National strategic planning for cyber security	11
3. Cyber security regulation in Europe	14
4. IT security incident response team	21
5. Law enforcement in the context of cyber security	25
6. Organisation of national cyber security	29
7. Critical infrastructure and cooperation with the private sector	35
8. How to develop a country's cyber security?	42
Contributors	47

Foreword

As governments begin to build an information society, they typically focus on providing more digital services and creating various service environments. Cyber security for a society will only receive more thought after an extensive or damaging security incident. At the same time, cyber security is an integral part of an information society. Electronic services such as e-banking or e-tax administration are of no use if their functioning, and the confidentiality of the data transmitted, are in doubt.

In 2007, Estonian e-services and websites became the target of mass cyberattacks. This was part of modern hybrid warfare. As a result of the attacks, an open debate arose in Estonian society at the time on how the state should prepare to defend itself in case the country comes under attack through cyber channels. The outcome of the debate were agreements between state authorities and the private sector, and already in 2008 Estonia's first cyber security strategy was prepared.

There are several international standards and guidelines for developing the cyber security of a single organisation, but it is difficult to find comprehensive tools for national governments. This handbook – *National Cyber Security in Practice* – is designed to fill that gap. The articles, written by seasoned experts, will give the reader an overview of the key elements that underpin the cyber security architecture of any country.

This handbook is aimed at policymakers, legislative experts and anyone responsible for ensuring the functioning and protection of digital services and services essential for the functioning of society.

Cyber security has been a very important area for Estonia as a digital state, both domestically and in

This handbook is aimed at policymakers, legislative experts and anyone responsible for ensuring the functioning and protection of digital services and services essential for the functioning of society.

international cooperation. Estonia is contributing to the United Nations Sustainable Development Goals through digitalisation and technological advancement, and supports the global development of resilient cyber defence capabilities. We wish to express our gratitude to the Estonian Ministry of Foreign Affairs for supporting the e-Governance Academy in publishing this handbook and developing the National Cyber Security Index (NCSI). In the following pages, Estonian and Finnish cyber security experts share their knowledge and practical experience on how to better harness globally accumulated NCSI expertise to enhance national cyber security.

The e-Governance Academy wishes to thank Epp Maaten, Toomas Vaks, Oskar Gross, Elsa Neeme, Lauri Luht and Kimmo Rousku for their contribution to the preparation of this handbook.

Happy reading!

Arvo Ott

Chairman of the Management Board
e-Governance Academy



Introduction

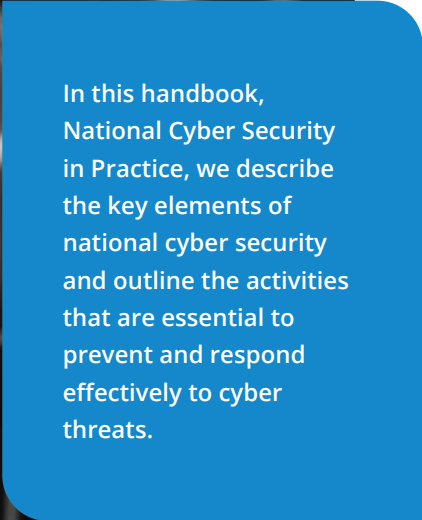


Epp Maaten | Programme Director of National Cyber Security
e-Governance Academy

There are many threats in cyberspace and the measures to counter them are also numerous. This raises the question of where a state should begin in order to better protect itself in cyberspace. The answer can be found in this handbook, *National Cyber Security in Practice*, which describes the key elements of national cyber security and outlines the activities that are essential to prevent and respond effectively to cyber threats.

The development of cyber security starts with mapping the situation and setting strategic goals. In the first chapter, we describe a model for resilient cyber security, which provides a framework for the activities described in the following chapters.

One of the first documents that states prepare when embarking on the development of their cyber security is a strategy paper. We focus on the cyber security strategy in chapter 2. This chapter lists the criteria for a good strategy and describes



In this handbook, *National Cyber Security in Practice*, we describe the key elements of national cyber security and outline the activities that are essential to prevent and respond effectively to cyber threats.

how to design a strategy, whom to involve, and why a strategy should be comprehensive.

Regulations are an important tool in building cyber security. In chapter 3, we outline the common approach of 27 European countries and how their measures for ensuring the cyber security of critical services can be harmonised to protect the EU single market. Chapter 4 discusses the strategic choices to be addressed when drafting legislation to ensure a legal environment that respects the fundamental rights of the people,

while being effective in preventing and responding to incidents.

In chapter 5, we discuss the objectives and key tasks of a computer security incident response team (CSIRT) and outline the incident response process. Cybercrime is discussed in chapter 6, which describes why it is important for the state to contribute to the establishment of a well-functioning cyber police unit and how this can be supported by the legal system and practical cooperation at the international level.

In the next chapter, on the organisation of national cyber security, we offer a close-up of Finland and Estonia as examples of how to ensure comprehensive coordination at the national level to help achieve the goals established in the strategies and legislation. In chapter 7, we introduce the concepts of essential services and critical infrastructure, discussing the basis for their identification and the role of the state and the private sector in their protection.

In the final chapter, we introduce in some detail a tool for enhancing national cyber security – the e-Governance Academy's National Cyber Security Index (NCSI). On the one hand, the NCSI acts as a systematic guide for building a secure and reliable information society, and on the other hand, as a description of the current situation, enabling the state to compare itself with other countries and formulate future plans.

Over the years, the NCSI has developed into a substantial public knowledge base, bringing together valuable information from over 150 countries worldwide. In addition, we have created a network of contacts to help keep the knowledge we have up to date and accessible to everyone online.

We hope that this handbook will provide guidance and support for anyone responsible for cyber security. Let us make the information society secure! Everywhere.



1.

Resilient cyber security

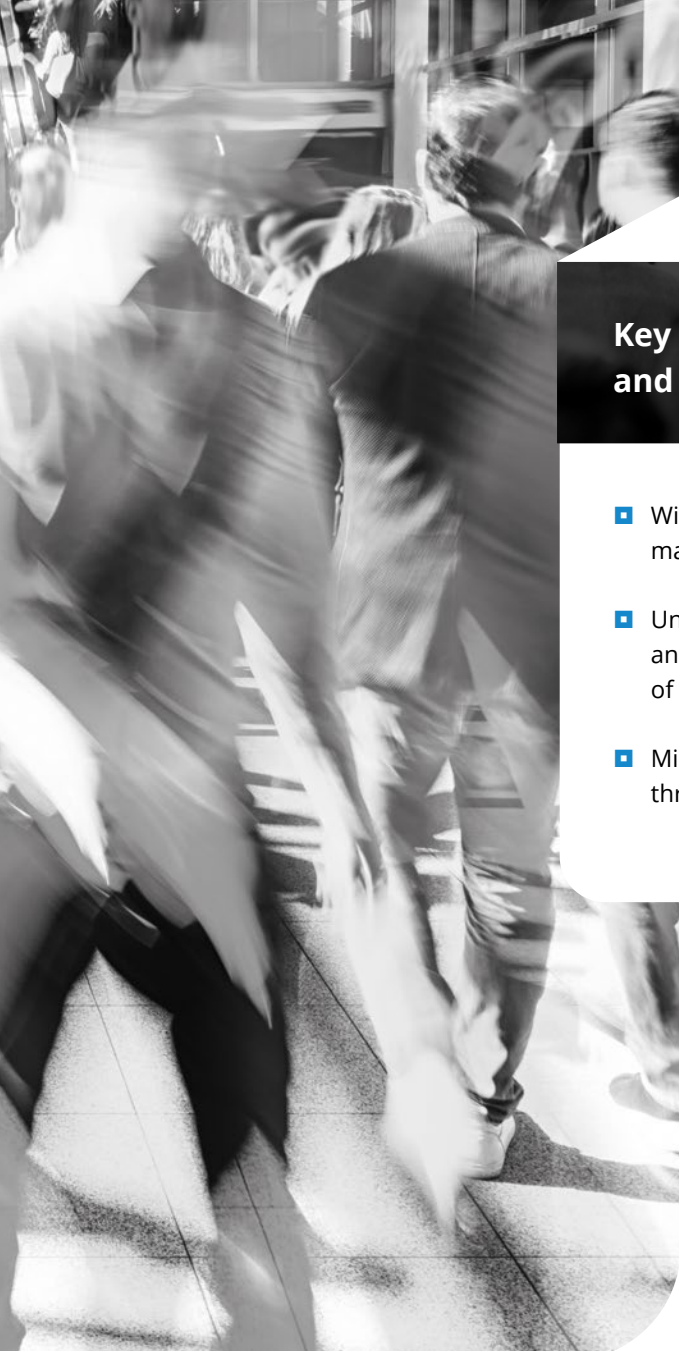


Toomas Vaks | Cyber security expert

Head of Cyber Security Branch, Estonian Information System Authority (2011–2017)

By the beginning of the third decade of the 21st century, the digital economy will represent a significant and growing part of the global economy, estimated to reach 15.5% of global GDP.¹ The development of information technology has affected all aspects of the economy and society, and the sharing economy and ‘smart agriculture’ are just a few examples of areas where information and communication technology (ICT) has

brought about profound changes. More than half of the world’s population uses the internet and almost 45% are daily users of social media. Along with changing the way communication works, it is also changing the way societies function. But in addition to new opportunities, IT development brings with it new types of risks that need to be addressed at the national level.



Key threats to the digital economy and digital society

- Widespread malfunctions of IT systems, which may be caused by faults as well as by targeted attacks
- Underestimating the technology-related risks and the consequent risk of becoming a victim of cybercrime and fraud
- Misinformation campaigns spread and managed through social media that can lead to widespread crises.

Did you know that a widespread malfunction may result from:

- **accidental unintentional activity**, such as device malfunction, usage error,
- **intentional actions**, such as unauthorised access, data theft, information system clutter,
- **environmental disturbance**, such as a flood in the equipment room, pollution or fire.

It is important to realise that cyber security incidents can never be completely prevented. The rapid development of technology and its accelerated spread also increases the potential for security incidents. Therefore, in addition to preventing incidents, the focus must also be on cyber resilience; that is, the control and reduction of damage caused by incidents. This requires two types of action: first, proactive measures aimed at preventing incidents, and second, reactive ones to control and reduce damage.

It is important to identify and understand potential threats (threat intelligence) and the risks associated with these threats (risk awareness). There is also a need for resources to detect and cope with incidents (incident management) and to plan activities and resources to deal with the damage caused by incidents (recovery). The existence of such measures will, on the one hand, increase the ability to prevent incidents by increasing overall security and, on the other hand, significantly reduce the adverse impact of incidents on society.

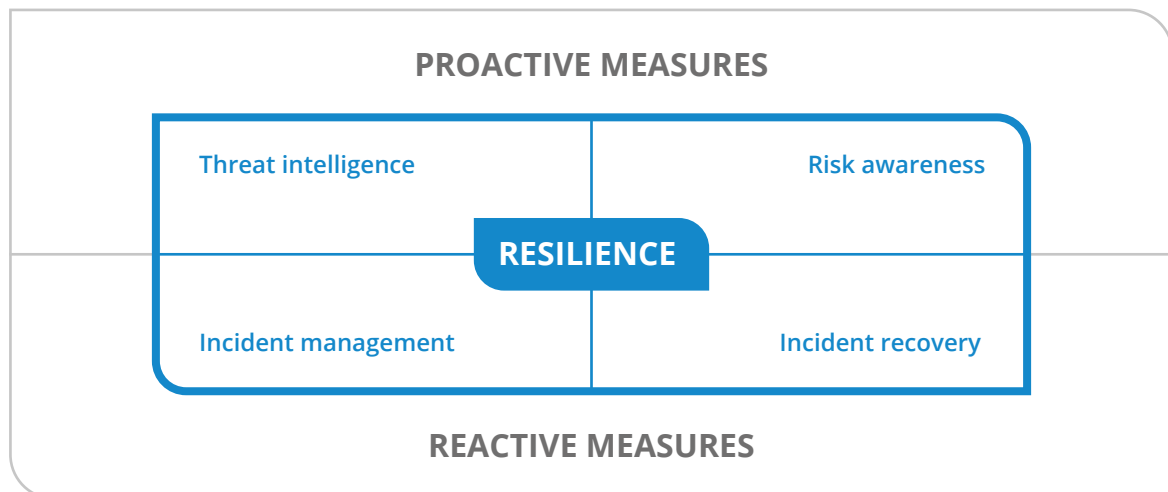


Figure 1. Measures to achieve cyber resilience

Means of performing essential functions

Threat intelligence tools

- establishment of incident response teams (CSIRTs/CERTs)
- cooperation and exchange of information between government agencies and the private sector to identify cyber threats
- mapping critical infrastructure and creating a national threat map
- international cooperation, participation in international networks (e.g. Trusted Introducer)

Tools for raising risk awareness

- information campaigns
- cyber security training, teaching cyber security as a subject or field of expertise in schools and universities
- continuing refresher training for officials and critical infrastructure companies on cyber hygiene

Incident management tools

- presence of a CSIRT/CERT
- existence of national and sectoral incident resolution plans
- existence of a police unit specialised in cybercrime

Incident recovery tools

- existence of national and sectoral crisis and recovery plans
- crisis exercises
- creating reserve and backup functions



2.

National strategic planning for cyber security



Toomas Vaks | Cyber security expert

Head of Cyber Security Branch, Estonian Information System Authority (2011–2017)

Strategic planning for cyber security is directly linked to the strategic planning of national security and the development of the corresponding strategies. In countries with a broader view of national defence issues, cyber security is seen as an important part of national security and perceived security in society. Until the early 1990s, national security strategies and development plans focused primarily on national military defence capabilities. Only afterwards did an understanding of the broader nature of national security emerge that includes

such important aspects as the protection of the population and the security of society as a whole, in contrast to a narrowly state-centred approach.

The issues of critical infrastructure protection and the provision of vital and essential services have emerged in connection with ensuring the security of society as a whole. This is because one method used today to undermine national security and the population's sense of security involves putting pressure on the country's population and dis-

rupting the operation of vital services and critical infrastructure.

Although cyber security strategies also address national defence issues, cyber security is nowadays part of a much broader approach, which can be called the comprehensive approach. It is therefore advisable to use strategic planning to address the field of cyber security in the broadest and most sustainable way possible, by developing a long-term national action plan or cyber security strategy.

Principles for drawing up national strategies

National strategic planning is often defined as an advisory and structured approach to making important decisions and implementing important actions. This approach shapes and underlies national arrangements, activities and their purposes. Strategy development is a continuous and forward-looking process. The final strategy must include informed choices and the resulting pattern

Cyber security covers all activities related to electronic information, media and services that affect national security.

Cyber safety usually refers to a situation where risks do not materialise and security is provided against threats that arise or are created through the operation of ICT equipment and systems.

of action for future decisions. The strategy also includes a high-level action plan on how to achieve the desired goals, as well as metrics against which to measure the achievements. A strategy is not static, but an integrated process for updating and adapting it to future needs must be foreseen, during the drafting stage.

What should we keep in mind when preparing national strategies?

- A strategy concerns public institutions, the private sector and society at large, as well as the international environment.
- Strategic decisions need to be understood as affecting overall wellbeing and not just a narrow group of public authorities or a specific area of government.
- A strategy must cover the objectives as well as the content of the activities and the process of achieving the outcome.
- Strategies can be created for different levels. A national strategy may also be supported by strategic plans with a narrower scope or time frames.
- National strategies have an important role to play in raising awareness of the issues and objectives in a particular field, both domestically and internationally. Domestically, these strategies provide an opportunity to explain and justify management decisions. Internationally, public strategies provide information to the country's partners on the country's national action plans.

Three key issues for a national cyber security strategy

- Do you consider cyber security and strategic planning as a nationwide process with heterogeneous actors? Do you involve the private sector, such as critical infrastructure and communication companies and other partners, and choose a comprehensive approach?
- Do you base your cyber security strategic planning on the need for extensive cooperation and coordination between government agencies? Do you approach cyber security inclusively across all government agencies?
- Do you address the international dimension of the strategic planning of cyber security? Is international cooperation necessary?

The process of designing and implementing strategies allows for the systematic management of the development of the field and is very useful for the country.

Key issues of cyber security strategy

Cyber security strategies have played an important role in declaring national priorities, explaining them to the public and to those who implement the strategy. The National Cyber Security Index² addresses the cyber security strategy as part of cyber policy development. The strategy preparation process includes the development of policy options, which will be realised during the implementation of the strategy.

Cyber security strategies can be conditionally divided into two: national defence-based and civil society-based. The boundary between the two has been blurred, however, by the adoption of a comprehensive approach to security. Strategic planning of cyber security should be based on a broader approach to the field and goal-setting, not just on the existing organisation of cyber security.

The process of designing and implementing strategies allows for the systematic management of the development of the field and is very useful for the country, despite the time and resources involved in developing and, especially, implementing the strategies.

The cyber security strategy process will also help to generate and maintain a broader interest in cyber security issues and the solutions to them. The existence of interest also has a direct impact on the development of the cyber security field beyond the strategy. For example, according to experts, the process of drafting the three cyber security strategies in Estonia in 2008–2018 has had a perceptible positive impact on the actual state of cyber security as well as on the development of Estonia's international reputation and competitiveness.

2 National Cyber Security Index (NCSI), <https://ncsi.ega.ee>.

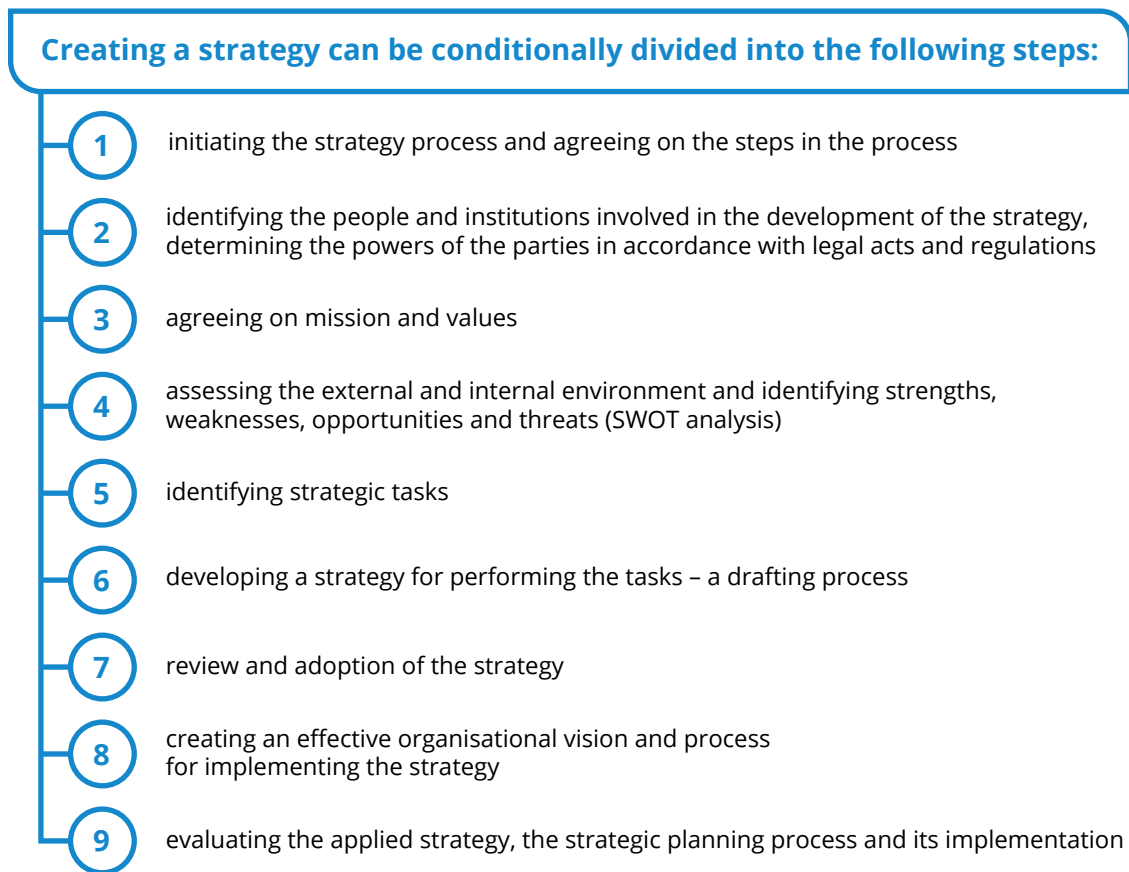


Figure 2. Strategy development process

The involvement of stakeholders is key

It is important to involve all stakeholders in the process of strategy development. First, successful strategic planning requires a clear message from the national leadership on the need for it, and the active involvement of the leaders of the organisations involved in strategy development. The awareness and involvement of managers and other employees in the strategy creation process is necessary but often complex in practice, as involving a large number of people makes the process slower and more expensive. It is important to strike a reasonable balance, so that people who have the necessary information or on whom the implementation of the plan depends will be involved.

For the strategy to succeed, it is important to identify the stakeholders that are relevant to the strategy as precisely as possible. These are individuals, groups of individuals or organisations with a legitimate interest in the field or how it is organised. Stakeholders may include:

- 1) implementers of the strategic plan,
- 2) beneficiaries of the strategic plan,
- 3) actors that can make a significant contribution to or obstruct the implementation of the strategy.

In the absence of a complete overview of all stakeholders at the time the strategy is initiated, you should be prepared to involve them later.



3.

Cyber security regulation in Europe



Elsa Neeme | Legal adviser
*Legal expert at the Cyber Security Branch
of the Estonian Information System Authority (2016–2018)*

What is cyber security?

Cyber security is a globally recognised concept widely used in both expert language and common usage. However, few European Union member states have defined cyber security at the level of national law.³

The 2016 European Union Network and Information Security Directive (EU NIS Directive) does not define cyber security, but uses the concept of **security of network and information systems** instead. It describes the ability of network and information systems to resist, at a given level of confidence, any action that compromises the

³ Bulgaria, Czech Republic, Poland, Estonia, Romania, Portugal and Slovakia.

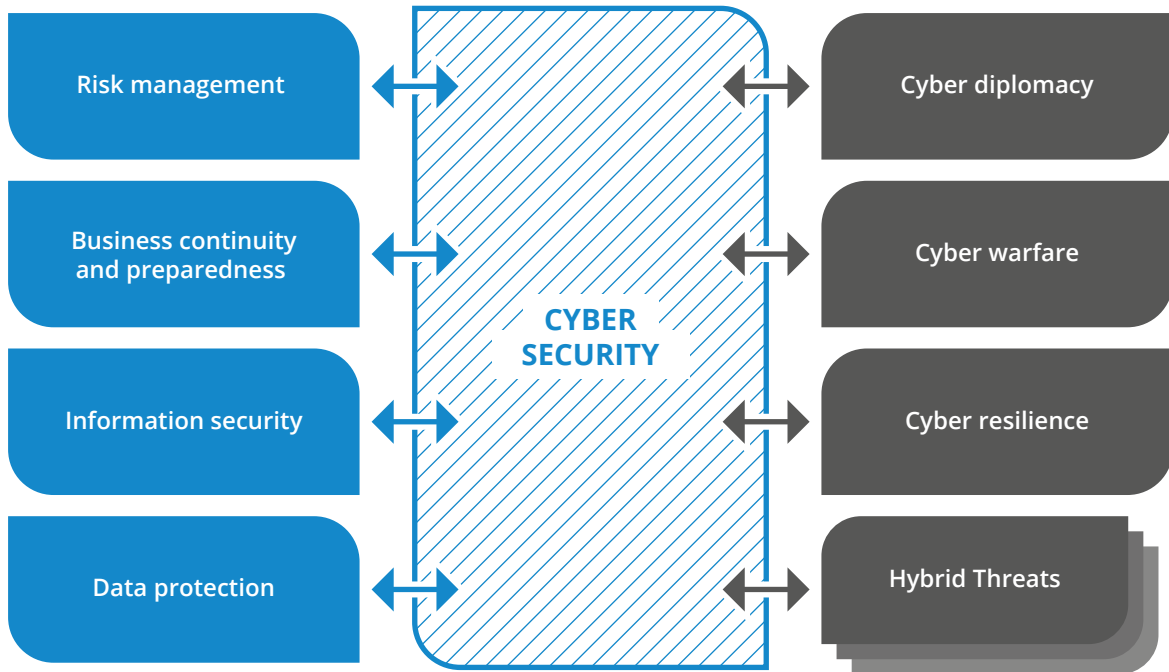


Figure 3. Areas of cyber security

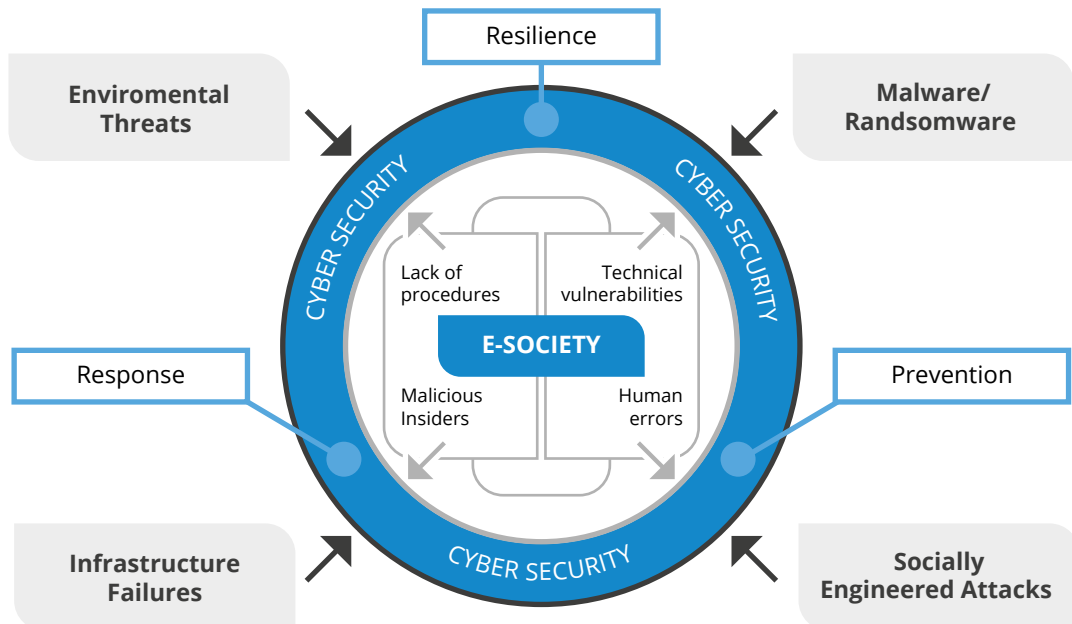


Figure 4. Cyber security forms the defence of a digital society, ensuring that the likelihood of internal and external threats to its operation is low

availability, authenticity, integrity or confidentiality of data or the related services.⁴

The Estonian Cybersecurity Act⁵ of 2018 also does not define the concept of cyber security, but the explanatory memorandum to the act explains cyber security as a state of society characterised by a low probability of threats to public order, people's health, property and the environment materialising through network and information systems, and the ability to respond to and mitigate the adverse effects of such threats.

The EU Cybersecurity Regulation⁶, which entered into force in 2019, defines cyber security as the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats. It follows from these two examples that cyber security always involves the well-being of a digitally minded society.

The main objectives of network and information system security, commonly referred to as the CIA triad (confidentiality, integrity, availability), are also the objectives of cyber security legislation. What the above shows is that there is no clear understanding in the EU as to which term is more accurate – 'cyber security' or 'network and information system security'. The purpose of the actions through which both concepts are defined is similar, only the level of detail of the definitions differs.

Design of European regulatory models for cyber security

As the internet is cross-border, cyber security legislation and strategy cannot develop in isolation, but have to consider the trends in other coun-

tries. Regulations in European countries have been developed primarily on the basis of the Treaty on the Functioning of the European Union.⁷ On the one hand, they are based on agreements aimed at ensuring an integrated approach to freedom, security and justice, covering, for example, cooperation in criminal and police investigations into attacks against information systems and cybercrime. On the other hand, the legislation on cyber security is based on the objective of ensuring the functioning of the single internal market. Although each regulation has a different scope and circle of addressees, they share the common feature that, in order to ensure the safe functioning of the internal market, these acts require market participants to:

- (a) inform the competent authority of security incidents;
- (b) take the necessary security measures.

In the European Union, the 2016 Network and Information Security Directive (EU NIS Directive) marks a milestone in the development of cyber security legislation. The main driving force behind the EU NIS Directive was the growing importance of network and information systems for the provision of essential services to society, such as power generation, passenger and freight transport, health care, and more. In order to protect the EU single market, it was necessary to harmonise national measures to ensure the resilience of the network and information systems for critical services. There was also a need to establish pan-European strategic and operational cooperation mechanisms.

The EU NIS Directive approaches national cyber security management in a comprehensive and systematic way, imposing the following obligations on member states:

- a) develop and implement a national cyber security strategy,

4 Article 4(2), Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016.

5 Cybersecurity Act, State Gazette I, 22.05.2018, 1. <https://www.riigiteataja.ee/akt/122052018001>

6 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019.

7 Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2012/C 326/01 OJ C 326, 26.10.2012, p. 0001 - 0390.

- b) designate at national level the providers of services essential for the sustainable functioning of society,⁸
- c) establish the necessary security measures for providers of services essential for society in order to ensure the reliability of network and information systems,
- d) ensure the availability of a capable and competent CSIRT⁹,
- e) designate at least one cyber security authority in the country to coordinate activities under the EU NIS Directive.

Extent of the territorial impact of cyber standards

Globalisation is increasingly giving rise to questions about the extent of the territorial impact of legislation. Several legal experts have stressed that the EU rules on the protection of personal data also apply outside the EU. The General Data Protection Regulation (GDPR) unequivocally provides that personal data may only be transferred to third countries and international organisations in full compliance with the regulation.¹⁰ The cross-border nature of data protection requirements is also supported by case law. For example, in its judgment in *Google v Spain*, the European Court of Justice notes that the European Union legislature has prescribed a particularly broad territorial (cross-border) scope to ensure individuals the protection guaranteed by the GDPR.¹¹

The implementation practices of the EU NIS Directive have not yet been considered by the courts, but similar legal proceedings to those concerning the

protection of personal data can be expected. For example, if a digital service provider¹² is not located in the European Union but provides services in the EU territory, it must appoint a representative in the EU,¹³ in which case the company is subject to the jurisdiction of the country of residence of the representative. As a result, for example, cloud providers offering services in Europe may simultaneously be subject to the legal systems of several EU member states. This happens when the provider of an essential service identified in one member state uses a cloud computing service, the provider of which is under the jurisdiction of another member state, while the data centres for cloud computing are located in a third and perhaps a fourth member state. Although in the above example, cooperation is required between the member states' competent authorities under the EU NIS Directive, supervision may prove difficult in practice.

Given the global trend in economic activity, it may be said in the light of the above examples that the scope of the cyber security requirements imposed by the EU legislator is not limited to the jurisdiction of a single country or the EU, but may extend to third-country operators.

A cyber-secure society and the protection of human rights

EU data protection rules apply only to the processing of personal data. The standards for the protection of services essential for society focus on ensuring the reliability of the network and information systems directly related to the provision of services. In both cases, the EU has committed data controllers and

8 For example, electricity suppliers and producers, airlines, rail infrastructure companies and financial institutions. It is notable that the market participants in such sectors traditionally form the core of the country's critical infrastructure.

9 CSIRT – computer security incident response team.

10 GDPR, recital 101.

11 Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD)*, paragraph 54.

12 A company that provides cloud computing services, operates an online marketplace or provides search engine services.

13 Article 17(3).

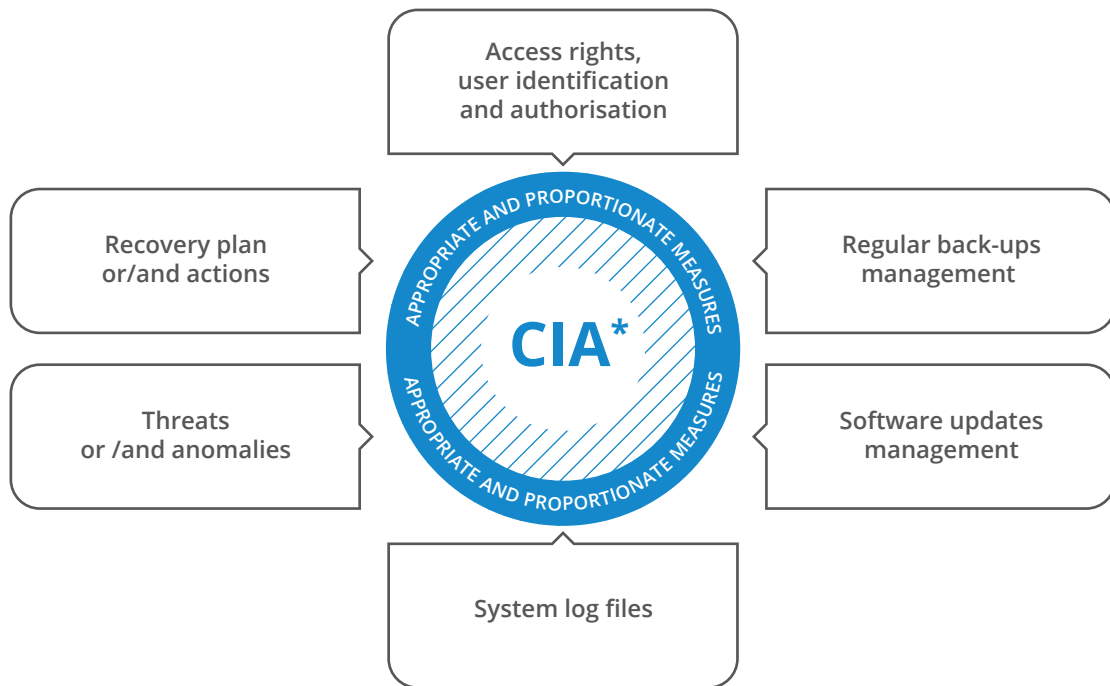


Figure 5. Ensuring confidentiality, integrity and availability are the starting points for implementing appropriate and proportionate security measures

operators of services to implement organisational, IT and physical security measures to ensure the confidentiality, integrity and availability of data.

The EU NIS Directive requires operators of essential services and digital service providers to take technical and organisational measures to manage the risks to the security of the network and information systems that they use in their operations. The General Data Protection Regulation imposes an obligation on data controllers to ensure the secure processing of data; that is, the obligation to take appropriate technical and organisational measures in the light of the threat to the rights and freedoms of the individual.

Therefore, both regulations are characterised by the obligation to implement appropriate and proportionate security measures based on the

assessed level of risk. The Estonian National Cyber Security Strategy emphasises that, despite separate regulations, it is no longer reasonable or feasible for the implementers to separate the protection of personal data from ensuring cyber security, but that the legal obligations must be viewed in their entirety and in harmony with each other.¹⁴

Both personal data protection, and network and information system protection legislation seek to promote a risk management culture that directs the operators of essential services and data processors to critically evaluate their activities and the digital environment risks that affect them, rather than prescribing precise rules. Depending on the activity and potential environmental risks, precautionary measures must be taken to prevent or minimise such risks.

¹⁴ Cyber Security Strategy, p. 22. Available at: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf.

When establishing cyber security requirements in the digital society, care must be taken not to sacrifice essential human rights and fundamental freedoms for the sake of security.

Restriction of fundamental rights and freedoms to ensure cyber security

When establishing cyber security requirements in the digital society, care must be taken not to sacrifice essential human rights and fundamental freedoms for the sake of security. The privacy of people is particularly at risk in modern society. But freedom also has its limits. The extent to which the fundamental rights of individuals are permitted to be undermined in order to ensure the safety of society needs to be assessed.

In cyber security, this issue arises prominently in the work of computer security incident response teams or CSIRTs. For example, according to the EU NIS Directive, CSIRTs must provide national cyberspace monitoring, risk and incident warnings, incident response, and situational awareness.¹⁵ Therefore, the main task of a CSIRT is to ensure the early detection of threats to the digital society and to respond effectively to cyber incidents resulting from the materialisation of threats. In both cases, the processing of personal data is inevitable. Article 17 of the International Covenant on Civil and Political Rights (ICCPR) provides for the right of every person to be protected from arbitrary or unlawful interference with their privacy or correspondence, as well as against unlawful attacks on their honour and reputation. This Article requires the state to take legislative and other measures to prohibit interference with a person's privacy and attacks.

Recital 49 of the General Data Protection Regulation confirms that network and information security and incident response functions are the responsibility of CSIRTs, but it should be noted that the least intrusive means for achieving the objectives should be used and the necessity, scope and lawfulness of personal data processing should be assessed. Any limitations of fundamental rights must:

- be provided for by law,
- respect the essence of fundamental rights,
- genuinely meet the objectives of general interest or the need to protect the rights and freedoms of others,
- be necessary,
- be proportionate.¹⁶

Legislation supports the achievement of the country's objectives and is an instrument for implementing the cyber security strategy. The role of legislation is to support strategic choices, and in the process, ensuring a proportionate and human rights-based environment, while being effective in preventing and responding to incidents.

Legislation supports the achievement of the country's objectives and is an instrument for implementing the cyber security strategy.

In each country, consideration should be given to how much society is willing to yield and surrender the right to privacy in the exercise of its protection function. It is a matter of trust and legal order. The legal system must also support a risk-based and technology-neutral approach to cyber security. Therefore, the minimum technological requirements should be preferred and the focus should be on the goal. The legal system thus designed will provide sufficient mechanisms and tools for building trust and maximum safety in society.

¹⁵ Annex I to the NIS Directive.

¹⁶ https://edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf



4.

IT security incident response team



Toomas Vaks | Cyber security expert

Head of Cyber Security Branch, Estonian Information System Authority (2011–2017)

IT security incident response teams are known internationally as CSIRTs (computer security incident response teams) or CERTs (computer emergency response teams). The name 'CERT' is internationally protected and requires the permission of its owner, Carnegie Mellon University, which is why more and more teams nowadays use the name 'CSIRT'.

CSIRTs are set up by public authorities, private companies and universities; other CSIRTs specialise in economic sectors such as banking or e-commerce. Their setup can be very different – a CSIRT can be a public authority, a private-sector service provider, or a public-private partnership.

Tasks of a CSIRT:

- 1) providing assistance to its constituency in responding to IT security incidents in an agreed manner and to an agreed extent, which may include technical incident resolution, response coordination or consulting,
- 2) collecting and analysing information on incidents and security vulnerabilities, monitoring cyberspace,
- 3) participating in international CSIRT networks and cooperating with other CSIRTs for incident resolution as well as cooperating with other agencies, organisations and the community to resolve incidents,
- 4) informing its constituency and the public about security threats and incidents.

Some CSIRTs have a national role, in which two types of approaches can be distinguished. Referred to as national CSIRTs, they are responsible for dealing with security incidents in the national internet domain,¹⁷ where the CSIRT usually has a mainly coordinating and counselling role and is an important national contact point for other CSIRTs.

A practical example would be a malware-infected information system in a country's internet domain that attacks information systems in another country. When this happens, the country under attack needs to contact the owner of the systems where the attacks originate, so that the owner could fix the systems and stop the attacks. In such cases, the national CSIRTs will contact each other through reliable channels and work together to respond to the incident. National CSIRTs are usually technical teams that work with both the private and public sector, and are often very closely associated with academic institutions, sometimes being part of these institutions for historical reasons.

It is considered good practice for a CSIRT to describe and disclose its constituency, roles and services in accordance with the RFC 2350 format developed by the Internet Engineering Task Force (IETF), which enables all parties to understand these in a uniform manner.

Government CSIRTs (Gov CSIRTs) are primarily responsible for incident resolution within government agencies. These entities may also have the broader role of protecting critical infrastructure companies and institutions from cyberattacks. Such CSIRTs are usually either independent public authorities or located within a public authority. As a clear trend in the past decade, national CSIRTs have increasingly cooperated with national defence and security agencies, or even been integrated into security agencies. Still, such integration depends on the overall national security arrangements of the country and the traditional areas of the activity of the authorities.

The cyberattacks of 2007 and 2008 against Estonia and Georgia showed that society's dependence on IT services has grown to the extent that CSIRTs play an important role in the functioning of essential services as well as in the functioning of society in general. Over the past 15 years, the field of activity for CSIRTs has changed considerably, and so has their role vis-à-vis the state, the economy and the individual. The role of CSIRTs in responding to cyberattacks and resolving security incidents is difficult to overestimate. It is a well-functioning team of competent professionals with clearly defined tasks, who can reduce the adverse effects of incidents, speed up their resolution and even help prevent incidents.

17 For example, the Estonian national domain is .ee.

The following are key to the successful fulfilment of this role.

- 1) **Expertise and sufficient resources.** The team should include experts in network security, log analysis, computer forensics and reverse engineering, as well as security architecture and advanced information security. It is also important for the team to have its own development resources because the specific nature of a CSIRT's work means that all the necessary tools cannot be outsourced, but some of them have to be developed by the team itself. Success in responding to incidents at the national level also requires knowledge of the functioning of the state and of critical services, risk and crisis management and business continuity. The required hardware and software, communications, a secure location, and other things necessary for the job must also be provided.
 - 2) **Threat intelligence.** Continuous gathering and analysis of information on security incidents both domestically and internationally makes the rapid identification of threats possible and the resolution of incidents more effective. The concept of an incident should be precisely defined along with the process for incident reporting and analysis. In addition to collecting information from public sources (OSINT), national reporting and information exchange, international information exchange with sister organisations from other countries is highly desirable.
 - 3) **International cooperation and participation in international cooperation networks.** As cyberattacks and other security incidents are generally global in nature and not bound by national borders, it is essential to have good contacts and information exchange with the international community. Active participation in networks, such as Trusted Introducer¹⁸, helps build the reputation and credibility of the team, which in turn allows for faster communication with the international CSIRT community.
- Generally, this community sticks together, and contacts at the specialist level often transcend the traditional boundaries of transnational communication.
- 4) **Cooperation with the national IT community.** It is important to understand that the functioning of the IT services needed by society is largely dependent on private-sector companies. Typically, IT professionals develop their own spontaneous or organised communities, from professional alliances to online forums. It is important for a CSIRT to work with and be visible to these communities. It provides quick access to necessary information on security changes, accelerates information exchange, and even outlines the availability of specific IT expertise or resources that can be used to respond to incidents in an emergency.
 - 5) **Clearly defined national working arrangements for information exchange and incident response.** The roles of the various organisations and agencies, their cooperation and the arrangements for the exchange of information must be clearly defined and organised. IT incidents tend to escalate very rapidly. The effectiveness of their resolution depends largely on the speed of response, in which previous planning and agreed working arrangements are key. The public also needs to have a clear understanding of the role of a CSIRT. Given the need for extensive cooperation with the private sector, it is advisable to clearly define the role of the CSIRT and to establish clear demarcation lines, for example, with regard to the role of the police or security authorities. Giving a CSIRT a public oversight role is not desirable; it is preferable that the team is perceived as a 'firefighter helping to put out the fire' rather than a 'police officer that cuffs your hands'.
 - 6) **Exercises.** Regular exercises are required to test incident resolution plans as well as team skills. Exercises should be organised both within teams and at the national level, involv-

18 TF CSIRT, <https://www.trusted-introducer.org>

ing partner institutions as well as private companies. Teams should certainly take part in international exercises, which have become increasingly popular in recent years (e.g. Cyber Europe organised by ENISA and the technical exercise Locked Shields organised by CCDCOE).

- 7) **Communication and visibility.** Informing the public as well as partner institutions about secu-

urity threats must be a regular activity and there must be a clear process in place to that end. Although information campaigns and media communication may also be conducted through partners, it is advisable to have a corresponding function within the CSIRT itself. A CSIRT should also be visible in social media and interact with its constituency as much as possible.

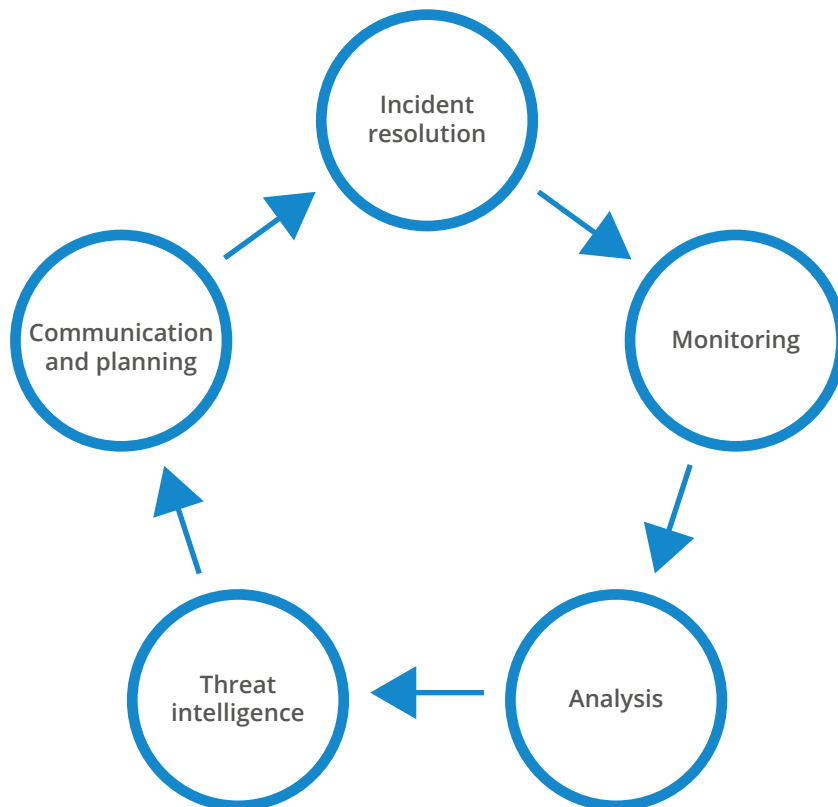


Figure 6. Tasks of a CSIRT



5.

Law enforcement in the context of cyber security



Oskar Gross | Head of the Cybercrime Bureau of the Central Criminal Police
Police and Border Guard Board

Although cyber and digitalisation have in recent years become increasingly popular topics, in the context of law enforcement these are nothing new. As early as 1988, Robert Tappan Morris was able to infect the internet with a worm from M.I.T campus. He was caught and charged with violation of the Computer Fraud and Abuse Act.¹⁹ However, even though cybercrime has existed for

almost as long as the internet, it has changed from some clever enthusiasts testing the limits of the internet to a huge underground economy making it one of the least risky forms of criminal activity. It is almost impossible to calculate an actual figure for the global losses from cybercrime due to the indirect costs (loss of data, revenue, emotional harm etc.), but for instance considering that

19 United States v. Morris (1991), 928 F.2d 504, 505 (2d Cir. 1991).

havebeenpwned.com reports 9 billion breached accounts, we can quite safely say that almost everybody has been a victim of cybercrime in one way or another. Although the Estonian criminal police have quite a long history with cybercrime investigations, the Estonian Police and Border Guard Board decided to create a specialist bureau for investigating cybercrime in Estonia in 2016.

What is cybercrime?

Cybercrime as a term covers an extremely wide spectrum – essentially all the bad things you can do with a computer. There are numerous approaches that try to structure this topic. One is to categorise cybercrime from the perspective of the point-of-failure, either human or computer. The term cyber-dependent is used to describe crimes that cannot be carried out without a computer (e.g. ransomware, DDoS attack, RAT, etc.), while the term cyber-enabled crimes is used for crimes which can be scaled to massive proportions with the help of computers (e.g. fraud, child sexual exploitation, illegal drug trade etc). Another way is to divide the different *modi operandi* by type of crime: extortion (e.g. ransomware, sextortion), fraud (e.g. CEO fraud, business email compromise attacks), stealing (e.g. illegally accessing bank information systems or client accounts) and so on. In essence, there is no right or wrong way, but I personally prefer the latter, as I find that it is important to demystify the field.

A large part of successful cyber cases surprisingly rely on classical criminal police work.

The role of law enforcement

Law enforcement has an important role to play in cyber security. As in real life, we expect that at least to some extent people are also protecting themselves (e.g. locking their doors, using seatbelts, etc.) on the internet (e.g. strong passwords, 2 factor authentication, etc.). Another pillar of

cyber security includes Computer Security Incident Response Teams (CSIRTs) and Computer Emergency Response Teams (CERTs), who actively prevent and respond to cyber incidents. The difference between CSIRTs/CERTs and regular law enforcement is that the goal of law enforcement is to identify and prosecute the people behind malicious attacks, whereas the work of CSIRTs/CERTs is to take a cyberattack under control and get systems working normally again. These lines of work might seem similar but in practice the overlap is rather limited – some technical details are relevant during the investigations, but a large part of successful cyber cases surprisingly rely on classical criminal police work. From the societal point of view, the importance of law enforcement is deterrence. As long as we are only deactivating the weapons used by criminals, they will just attack us again either with the same or new weapons. In order to complete the valuable work of CSIRTs/CERTs, it is important to find and prosecute the people responsible. Considering the speed of digitalisation we have to keep in mind that it is wise to jump on an accelerating train rather sooner than later.

Model for cyberpolice

Dealing with cybercrime has a couple of unique aspects compared to criminal policing in other fields. Most of these stem from the fact that cybercrime is global and a large amount of evidence is located online. This, in turn, means that the tools used by regular criminal police are usually not an exact fit for analysing the type and amount of information that cybercrime investigators face.

Technical specialists

In Estonia we have seen that having highly-skilled technical specialists at the cybercrime unit makes a big difference – it enables the unit to design their own tools for searching or (automatically) analys-

ing large amounts of information and this makes it much easier to gain an insight into the technical aspects and nuances of cybercrime. Theoretically, outsourcing the IT skills would be an alternative, but in the long term, this is not realistic – the ecosystem of cybercrime is constantly changing, technologies come and go, and therefore being able to adapt quickly is vital. It seems to be quite common that half of the cyber units consist of technical specialists and the other half of police officers.

Probably one of the most pressing issues with technical staff is hiring and the problem is two-fold. First, the IT sector around the world is growing and the salaries for IT experts are usually higher than for the public sector, which makes it a challenge for the public sector to accept. Second, our experience shows that you need specialists with a wide spectrum of skills and an ability to constantly learn and integrate new available technologies.

It is quite common that cybercrime units also provide different digital forensic services to other criminal police units – providing first responders to crime scenes/searches, identifying digital devices, making forensic copies, analysing and documenting findings.

In Estonia, this is a bit different – the Cybercrime Bureau focuses only on their own investigations and then we have a specialist unit in the regular criminal police departments to assist with digital forensics. Although formally, this is just a structural aspect of the organisation, from the perspective of awareness, the impact has been positive – it has sent a strong message that digital forensics is part of all investigations and not something specific to cybercrime and vice versa, the core of cybercrime is not making traditional disk forensics. This also means that the IT specialists in the Cybercrime Bureau can invest 100% of their time in increasing our capabilities.

The usefulness of a specialist digital forensics unit

- Digital forensics is part of all investigations and not something specific to cybercrime
- Cybercrime investigations are treated more broadly than just conventional disk forensics
- The Cybercrime Bureau can focus on its core responsibilities and capacity building

International cooperation

Though international cooperation and experience exchange is important in all fields, investigating cybercrime in isolation is a short-term solution. It is quite unusual for cybercriminals to target their own country of location, meaning that in most cybercrime cases the evidence exists in at least two countries. It is also important to note that to an extent cybercrime investigations are solidary – by investigating people located in our jurisdiction, we are usually protecting people who are targeted as victims in other countries. So the stronger we are globally on average, the safer cyberspace is. All this makes it even more important to have operational level cooperation between countries.

The stronger we are globally on average, the safer cyberspace is.

In addition to sharing information on a query basis, it is also relevant that cooperation is happening at an operational and technical level. As mentioned before, the ecosystem of cybercriminals is in constant change, which also means that at all times we need new tools, approaches and creativity for law enforcement to

stand a chance. This is why it is perfect when countries find common interests and work towards goals together – be they analysis tools or methods, or information sharing.

In the end, good tools and information are the only way we can achieve an intelligence-led approach, which enables us to investigate cases that have the greatest impact, either on our own country or the whole cybercriminal environment. Effectiveness and focus are extremely important because the amount of noise is huge – even petty crimes and ineffective simplistic frauds are so scalable that they might drive us away from more important targets.

Legal aspects

Due to extremely rapid digitalisation, it is important to keep the legal framework up to date to enable law enforcement to do their work. When countries adopt a similar approach to the criminalisation of cybercrime, it makes the legal process clearer and cross-state investigations faster.

In cybercrime investigations, reaction time might have a huge impact. However, it is not only about the officers reacting fast but also the legal framework giving them the right tools – whether to obtain data or at least preserve information such that it is later collectable through the legal process. On a more general note, it is also important to consider different privacy related regulations; for example, data retention, the right to be forgotten and so on.

In terms of data retention – although storing data about people's actions violates their privacy, in the end we need to consider the balance between security and privacy. In cybercrime cases, a large part of the evidence is circumstantial. The problem with circumstantial evidence is that sometimes the conclusions are wrong – unfortunately, the less historic information we store, the less information law enforcement has to make their educated

Cyber crime unit is crucial

Although cybercrime is not a new phenomenon, it is amazing how versatile the opportunities it affords criminals – from illegal markets to money laundering and extremely technical methods to obtain illegal access to computer systems. Although we are investing considerable effort to defend against cybercrime, it is crucial that we also invest in well-functioning law enforcement cybercrime units because otherwise there is no actual deterrence and the amount of criminal activity just increases. The pillars of effective cybercrime investigations are motivated people with skills, the right tools, actionable intelligence, supportive legal system, and last but not least practical international cooperation.

The legal framework should give the right tools to investigate cybercrimes.

guess. If the situation becomes too unbalanced, law enforcement themselves may inevitably violate somebody's rights much more than they would have otherwise. However, finding this balance is no trivial task, and unfortunately is out of the scope of this article.

Organisation of national cyber security



Elsa Neeme
Legal Advisor
Legal Expert at the Cyber Security Branch of Estonia's Information System Authority (2016–2018)

Epp Maaten
Programme
Director of National Cyber Security
e-Governance Academy

Kimmo Rousku
General Secretary
Finnish Public Sector Digital Security Management Board (VAHTI)

The organisation of national governance for cyber security is a matter of choice for each country and largely depends on the country's existing legal environment. Legal choices may be influenced by factors such as the availability of cyber security expertise, considerations regarding funding as well as national strategic development plans on topics like national internal security and economic security.

In its shaping of the legislative field around cyber security, Estonia is guided by the broad concept of national defence and the principles of Estonia's security policy.²⁰ When looking at other European countries, cyber security governance models generally follow either a decentralised or a centralised approach.

²⁰ National Security Concept of Estonia, p. 2. Available at: https://www.riigiteataja.ee/aktiisa/3060/6201/7002/395XIII_RK_o_Lisa.pdf#

The organisation model for **decentralised cyber security** is based on the principle of subsidiarity and is characterised by a system of sectoral legislation. In this model, there are several national authorities competent in cyber security issues, who coordinate the implementation of cyber security in their sectors. A decentralised approach can facilitate information exchange with market participants. The advantage of this approach is the inclusion of network and information security measures in existing sectoral legislation, already familiar to the sector's industry, making it easier for them to adopt and effectively comply with new requirements.

Regardless of whether a decentralised or a centralised model is used, cooperation between various public authorities in preventing and responding to cyber incidents is always essential.

In countries with **centralised cyber security**, a single authority with broad expertise in many, or even all, critical sectors is designated to ensure the cyber security of essential social services. These countries also establish comprehensive cyber security legislation. The tasks of the central authority sometimes also include preparation for emergencies and crisis management²¹ and it often includes a national unit for cyber incident response.

A strictly sector-based approach is not always beneficial when protecting the critical information infrastructure and ensuring the cyber security of essential service providers. A sectoral approach can lead to conflicting legal provisions or, conversely, to the emergence of several similar regulations on the same subject. In contrast, centrally organised systems and comprehensive legal requirements for providers of essential services help to prevent the uneven and incomplete implementation of regulatory

provisions. Moreover, it is irrelevant whether the responsibilities to ensure cyber security are dispersed across several pieces of legislation or laid down in one single legal act.

Regardless of whether a decentralised or a centralised model is used, cooperation between various public authorities in preventing and responding to cyber incidents is always essential. The legal bases for national administrative cooperation can be established either by law or by an administrative act or contract. Responsibilities for cross-border cooperation must also be clearly defined when developing an administrative model.

21 In France, for example, the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) has been designated as the supervisory authority for critical operators that has the power to oblige critical operators to comply with security measures and is also authorised to conduct security audits. In addition, ANSSI acts as the emergency authority for the protection of critical information infrastructures. Estonia applies the more commonly used decentralised approach to the management of critical infrastructure protection. According to the Cybersecurity Act, the coordinating authority in Estonia is the Information System Authority. Under the Emergency Act, the same organisation also manages the emergency response to a cyber incident. Source: Communication COM(2017) 476 final/2 from the Commission to the European Parliament and the Council, <https://eur-lex.europa.eu/legal-content/EN-ET/TXT/?uri=CELEX:52017DC0476&from=EN>.

6.1 Organisation of national cyber security in Estonia



Epp Maaten | Programme Director of National Cyber Security
e-Governance Academy

The **Security Committee of the Government of the Republic** analyses and assesses the national security situation and coordinates the activities of the authorities of executive power in planning, developing and organising national defence. The committee is chaired by the Prime Minister, and its members include the Minister of Foreign Trade and Information Technology, the Minister of Justice, the Minister of Defence, the Minister of Economic Affairs and Infrastructure, the Minister of Finance, the Minister of the Interior and the Minister of Foreign Affairs. The secretary of the commission is the director of national security and defence coordination.

The task of the **Cyber Security Council** is to contribute to smooth cooperation between various institutions and ensure the implementation of the objectives of Estonia’s Cyber Security Strategy through the planning documents, programmes and work plans of the responsible government institutions. The council is chaired by the secretary general of the Ministry of Economic Affairs and Communications.

The **Ministry of Economic Affairs and Communications** coordinates cyber security policy development and the implementation of the Cyber Security Strategy, as well as the cooperation between state authorities and the wider community.

The **Information System Authority**, which organises the development and maintenance of information systems that ensure the interoperability of the state information system, manages activities related to information security and handles cyber incidents that occur in Estonian computer networks. The Information System Authority’s tasks in cyber security include ensuring the security of all network and information systems essential to the operation of the state.

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

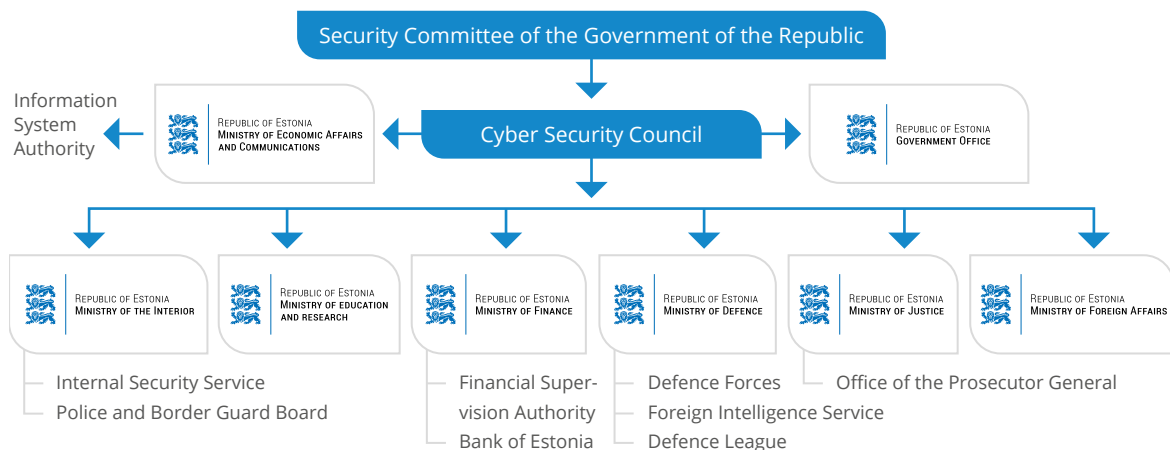


Figure 7. Organisation of national cyber security in Estonia

The **Ministry of the Interior**, in cooperation with the Police and Border Guard Board and the Internal Security Service, ensures the prevention of and response to crimes that endanger cyber security, and devises policies for the prevention, detection, response and processing of cybercrime, and for digital forensics. The ministry ensures the implementation of the priorities of the Cyber Security Strategy through the activities of the internal security development plan and related programmes, and contributes to the establishment of mechanisms for cross-sectoral cooperation and coordination, as well as the creation of a unified situational picture.

The **Ministry of Defence**, in cooperation with the Defence Forces, the Defence League and the Foreign Intelligence Service, manages the implementation of activities related to the digital aspect of the military defence side of the national defence development plan and contributes to the establishment of mechanisms for cross-sectoral cooperation and coordination, as well as the creation of a unified situational picture.

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

The **Ministry of Education and Research** takes into consideration the priorities agreed in the objectives of the Cyber Security Strategy in its

planning of lifelong learning strategy activities. The ministry supports the acquisition of basic knowledge for coping with cyber threats for graduates at all educational levels. The Information Technology Foundation for Education (HITSA) supports the Ministry of Education and Research in meeting the Cyber Security Strategy objectives in its area of administration.

The **Ministry of Justice**, in cooperation with the Office of the Prosecutor General, which is in charge of pre-trial criminal proceedings, contributes to planning regulatory and criminal justice policy throughout the digital sector, and plans sectoral preventative actions through violence prevention strategy activities. Among the Ministry of Justice's area of administration is an institution that is considered important from the standpoint of cyber security – the Data Protection Inspectorate (AKI), which supervises the rights and responsibilities in the field of the protection of personal data.

The **Ministry of Finance** helps in developing the different parts of the strategy, including ensuring sustainability and integration with other strategic planning processes. The ministry also ensures the involvement of the financial sector. Other authorities working with cyber security include the Financial Supervision Authority, which monitors financial institutions, and the Bank of Estonia, which follows the requirements established by the European System of Central Banks.

6.2 Finnish national digital security model



Kimmo Rousku | General Secretary

Finnish Public Sector Digital Security Management Board (VAHTI)

Finland does not have a single body responsible for the centralised management and steering of digital or cybersecurity at the national level. Instead, each administrative branch and competent authority is for its part responsible in its own area according to that provided in legislation.

This is possible thanks to the excellent coordination, reconciliation and development of activities conducted with businesses across administrative boundaries, which can be considered an important resource for Finland.

Key roles and responsibilities

The Prime Minister's Office is responsible for monitoring the implementation of the Government Programme and assists the Prime Minister in the management of the government. The office secures the operating conditions of the Prime Minister and the government in all circumstances. The area of responsibility of the Prime Minister's Office includes government awareness, preparedness and security, general coordination of the management of incidents, and joint information and document management for the government and its ministries.

The Ministry for Foreign Affairs co-ordinates this international cooperation activity. The cyber domain and cybersecurity have become an important part of Finland's foreign and security policy as cyber threats do not respect national borders. The ministry also acts as the National Security Authority (NSA) that is responsible for protection and processing of international classified information and, among other things, for the preparation of international information security agreements.

The Ministry of Finance is responsible for an economic policy that strengthens the preconditions for stable and sustainable growth, good management of public finances and effective public administration. The Ministry of Finance is responsible for the general principles of information policy, information management and electronic services in public administration. To that end, the Ministry of Finance prepares the general principles and requirements for the digital security of the ICT infrastructure, digital services and data in public administration as well as the policies, regulations and development programmes for digital security in public administration. The ministry also appoints the necessary management groups and cooperation networks. For example, the ministry has appointed a strategic management group for digital security in public administration.

The task of the **Digital and Population Data Services Agency (Finnish Digitalisation Agency)** is to promote the digitalisation of society, to secure

the availability of data, and to offer services for life events and to guarantee the undisrupted, secure and smooth operation of services that are important for the functioning of society. The agency provides population information, certification services and support services for the use of e-services that contribute to creating the preconditions on which digitalisation can be built. The agency is responsible for the expert services in digital security and prepares recommendations and instructions. It is also responsible for the operation of the Public Sector Digital Security Management Board (VAHTI).

The Ministry of Transport and Communications is responsible for the development of information security in electronic communication services and networks. The ministry develops strategy and regulations concerning the information security of electronic communication services or networks and other general guidance. The Finnish Transport and Communications Agency Traficom operates under the Ministry of Transport and Communications. The Cyber Security Director working at Traficom is responsible for implementing Finland's Cyber Security Strategy.

The National Cyber Security Centre belongs to the Finnish Transport and Communications Agency and plays a central role in the preparedness of a digital society. Through its activities, the agency ensures the functioning of society and services, like public communication networks in the event of disruptions and emergencies. In addition, the agency ensures the availability of radio frequencies and cryptographic material and is responsible for Finland's national domain extension .fi, maintaining the fi-root name servers and monitoring the registrars of domain names. The agency also carries out the CERT function (Computer Emergency Response Team).

The Police are responsible for the prevention, detection and investigation of offences and the consideration of charges. Cybercrimes are investigated by police departments on a regional basis.

- National Bureau of Investigation includes the **Cyber Crime Centre**, which is responsible for

the investigation of the most serious cyber-crimes, internet and network intelligence and maintenance of situational awareness.

- **The Finnish Security Intelligence Service** (SUPO) is responsible for preventing and combatting the most serious threats to national security, such as terrorism and illegal intelligence gathering by foreign states. The Intelligence Service also performs these tasks in the digital operating environment. It conducts intelligence analyses to support the government and other authorities in their decision-making.

The Finnish Defence Forces create a comprehensive cyber defence capability for their statutory duties as part of securing the vital functions of society. 'Cyber defence' refers to the area of national cybersecurity related to national defence, which consists of the capabilities of intelligence, influence and protection. The cyber defence capabilities produce intelligence data to support the government and the defence forces in their decision-making, while supporting the operations.

The Security Committee assists the government in broad matters related to comprehensive security. The committee monitors the development of Finland's security environment and coordinates the proactive preparedness related to comprehensive security. According to the guidelines of the 2013 strategy and of the renewed 2019 strategy, the Security Committee monitors and coordinates the implementation of the strategy. The goals of cybersecurity coordination include the avoidance of unnecessary duplication, the identification of possible shortcomings and determining the competent entities. The competent authorities will make the actual decisions subject to the provisions.

The **Data Protection Ombudsman** is a national supervisory authority overseeing compliance with data protection legislation. The task of the Data Protection Ombudsman is to promote the realisa-

tion of the right to access information and other fundamental rights in the processing of personal data. The Ombudsman processes notifications of data security breaches, approves certification authorities and inspects information systems.

The Information Management Board was established in 2020 to enhance and implement the information management and information security requirements. The board may set up temporary divisions, publish recommendations and organise seminars and other events.

The National Emergency Supply Agency belongs to the Ministry of Economic Affairs and Employment. It is responsible for the planning related to the maintenance and development of security of supply in Finland and the related operative activities. In cooperation with other authorities and businesses, the National Emergency Supply Agency ensures the continuity of the most critical systems in terms of the functioning of society in all circumstances. The agency manages and allocates the resources for the Digital Security Programme 2030 aimed at meeting the needs of businesses that are critical for the security of supply, while improving the security of cyber and digital infrastructures.

Municipalities and unions of municipalities are responsible for providing basic ICT-services, procurement and tendering of information technology, and their development and maintenance. There are differences between municipalities and the unions of municipalities, and their organisational approach depends on the size of the municipality. It is estimated that about one-third of services is outsourced, but often these outsourced services are provided by companies owned by municipalities and the unions of municipalities. The task of the municipal council is to ensure the organizing of risk management. By the end of 2023, municipalities are required to implement the minimum information security requirements in accordance with the Information Management Act.



7.

Critical infrastructure and cooperation with the private sector



Lauri Luht | Head of National Situation Centre
The Estonian Government Office

The concept of critical information infrastructure

It is up to the state to ensure that people's basic needs are met and basic services provided, so that society can function. Services that are critical to the day-to-day functioning of society and/or for dealing with crises are called **vital or essential services**. Such services include the generation and distribution of electricity, various telecommunica-

tions services, water supply, financial services and various transport services.

Vital services require infrastructure, both on a daily basis and in times of crisis, and people to maintain the infrastructure. The infrastructure that enables a vital service to function is known as **critical infrastructure**. Due to process automation and the transition to digital production equipment, a very large part of critical infrastructure is

dependent on information and communications technology (ICT). With the addition of ICT, the concept of critical infrastructure protection (CIP) has expanded to include **critical information infrastructure protection (CIIP)**. Therefore, in addition to the protection of physical processes, digital systems and processes that are integral to the operation of services must now also be addressed.

The roles of the state and the private sector

The protection of vital and essential services is one of the most strategic tasks in the internal security of states. The transition to automated and digital processes and systems has significantly changed the risks, which also need to be addressed from a cyber security perspective. This means that service providers must inevitably apply cyber security measures to ensure the reliability and resilience of the systems as well as national security.

As a rule, the state is not the sole provider of all essential services. Therefore, it must work closely with private-sector providers of these services to society. The role of the state is to design the right environment or ecosystem in which service providers can operate. Simply put, creating an environment means that the state develops legislation, policies, frameworks and guidelines (e.g. creating a cyber security strategy or guidelines for ensuring

the security of information systems). The state must also provide competent, up-to-date information on cyber threats and vulnerabilities. When designing the right environment, it is important to engage private-sector companies in activities that increase their preparedness for incidents and crises.

It is the responsibility of the state to establish trusted and effective cooperation between the competent authority/authorities responsible for cyber security and private-sector service providers, and to maintain a unified and informed community. Setting up various processes, such as regular seminars, threat briefings, shared communication channels and conferences, will also allow the private-sector providers to communicate better and more efficiently among themselves, and this serves national security. Maintaining and managing an informal cooperation network will improve preparedness for handling crises involving multiple stakeholders.

The role of service providers is to protect their processes and systems to ensure the delivery of the service to society. These organisations must, on the one hand, follow national requirements, and on the other, rely on international cyber security best practices. In addition, they must actively participate in networks and events provided by the state. Both the public and private sector must actively engage in trust building to ensure a smooth exchange of information, which can prevent many incidents.

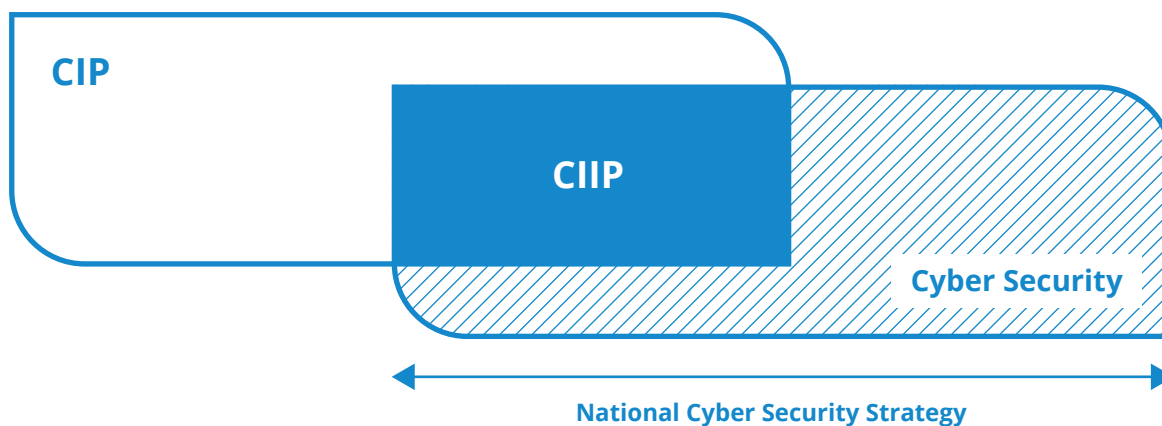


Figure 9. Critical information infrastructure protection brings together cyber security and critical infrastructure protection

The tasks of the state:	The tasks of organisations:
<ol style="list-style-type: none"> 1) developing the ecosystem: legislation, policies, frameworks and guidelines; 2) provide competent, up-to-date information on cyber threats and vulnerabilities; 3) involve companies in activities; 4) organise information events for private organisations and state agencies; 5) create and manage an informal network. 	<ol style="list-style-type: none"> 1) protect organisational processes and systems; 2) provide resilient services to society; 3) follow national requirements and international best practices; 4) participate in the work of national cooperation networks.

The state must work closely with private-sector providers of vital and essential services to society.

Identifying essential services

Each country identifies its essential services in accordance with the needs of the population and known risks. Therefore, no universal list of these services exists, but the most common items on the lists of different countries are as follows:

- energy,
- communications,
- transport,
- financial services and banking,
- health,
- food and water supply.

In addition, countries may consider other services as essential, such as search and rescue, law enforcement, environmental protection services, or specific services related to the country’s climate or location, such as district heating, sea rescue and water level management.

Each of the above is further divided into sub-services. For example, a state can include both emergency medicine and inpatient specialist care among its vital health services, and list either electricity generation or gas supply as its vital energy services.

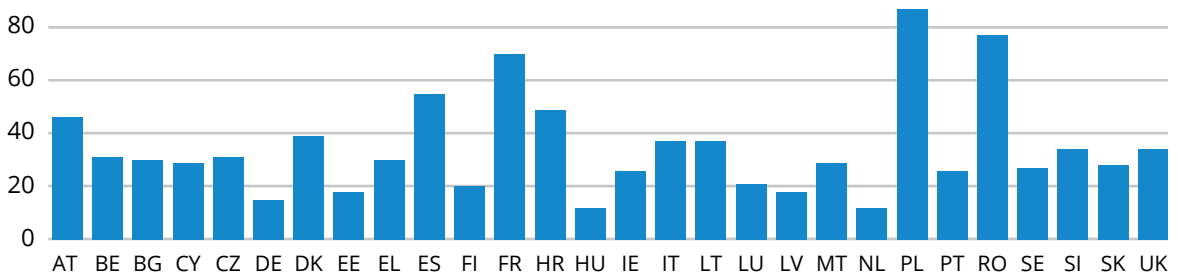


Figure 10. Number of essential services identified by EU member states, September 2019.²²

22 <https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52019DC0546&from=EN>

Regardless of which services a state identifies as vital, further defining its critical information infrastructure (CII) requires an assessment of the extent to which the service is dependent on ICT. An essential service need not always be subject to CIIP.

Once the essential services have been identified, the companies providing such services must be identified in terms of market share, production capacity, regional coverage or other criteria. In some cases, the service provider may have a 100% market share, which will make it easy to identify a service as vital. On the other hand, there are services that may be regionally distributed in a country in such a way that no company has a significant market share in the given industry, which may make all the providers vital (e.g. family physicians).

Essential services and critical (information) infrastructure should be identified and the requirements applying to them specified in collaboration between the state and the private-sector service providers; only then can the parties find a common understanding of what the state's CIIP capabilities are and what should be addressed outside the public sector.

There are two further key questions that the state should answer with regard to its services:

- (1) Which public-sector services should be considered as vital?
- (2) What requirements should be established for the public-sector services?

A risk-based approach to ensuring the continuity of services

Every provider of a vital service must have developed and implemented processes to ensure service security, incident preparedness and incident resolution.

The simplest form of risk management process for any service provider consists of four components:

1. risk identification (according to the organisation's risk profile);

EU NIS Directive

The European Union Network and Information Security Directive (EU NIS Directive) requires all EU member states to identify the operators of essential services as of 2018. At the same time, the directive leaves the member states sufficient leeway, so that they can identify service providers according to their needs and risk profiles. The directive sets out the following criteria for identifying service providers:

- the entity provides a service that is essential for the maintenance of critical societal and/or economic activities;
- the provision of that service depends on network and information systems; and
- an incident would have significant disruptive effects on the provision of that service.

2. risk assessment (the probability and consequence of the risk materialising);
3. risk control (various controls to mitigate or accept risks);
4. review of controls (a process specifying the mechanisms that help control risks).

The risk management process must take into account that different sectors have specific international standards and approaches that should be applied.

Service continuity assurance is aimed at finding ways to maximise the ability of an organisation's systems and processes to function in the event of incidents and crises, and to recover from disruptions as quickly as possible. Continuity assurance can be described in four steps:

1. understanding the organisation (its capabilities and potential gaps in them);

The example of Estonia

Estonia established a list of vital services in the Emergency Act of 2009. The list is rather comprehensive, containing 43 vital services from electricity distribution to the continuity of the Government of the Republic.

This means that the state imposed on itself requirements similar to those it has imposed on the private sector. The services were agreed across the ministries, involving private-sec-

tor companies and professional associations. The identification of services was discussed in several working groups with the participation of experts from different fields. This created a coherent approach, leading to greater trust and, ultimately, better quality of implementation. At the same time, ICT requirements were laid down for all service providers, as Estonia's high level of digitalisation comes with a dependence on ICT services.

Vital services under the Emergency Act

- (1) electricity supply,
- (2) natural gas supply,
- (3) liquid fuel supply,
- (4) ensuring the operability of national roads,
- (5) telephone service,
- (6) mobile phone service,
- (7) data transmission service,
- (8) digital user identification and digital signature,
- (9) emergency care,
- (10) payment services,
- (11) cash circulation,
- (12) district heating,
- (13) ensuring the operability of local roads,
- (14) water supply and sewerage,

Essential services under the Cybersecurity Act

- (1) a provider of a vital service under the Emergency Act,
- (2) a railway infrastructure manager or rail transport service provider,
- (3) an aerodrome operator,
- (4) a port service provider,
- (5) an electronic communications company,
- (6) a regional hospital or central hospital providing in-patient specialist medical care and an ambulance crew providing emergency care,
- (7) a family physician,
- (8) an administrator for the top-level domain name registry for .ee,
- (9) a provider of communications services, marine radio communications services and operational communications network services,
- (10) Estonian Public Broadcasting.

2. ensuring preparedness (for various incidents/ crises);
3. responding (to various incidents/crises and managing them);
4. adapting and improving (by learning lessons and defining future developments).

As in risk management programmes, continuity assurance also has sectoral international best practices in place, which are tailored to the sector but are also applicable to cyber security.



Figure 11. The risk management process of a service provider

Every provider of a vital service must develop and implement processes to ensure service security, incident preparedness and incident resolution.

Using the two support processes described above – risk management and continuity assurance – it is possible to build an organisation’s **resilience**, which enables it to better handle incidents and crises internally.

Ensuring preparedness through exercises and clear crisis management

The best way to understand and improve the preparedness of the state or private-sector organisations is to conduct exercises that focus on testing system performance and identifying deficiencies, and to make corrections after the exercises. Exercises can and should be conducted at different lev-



Figure 12. Four steps to continuity assurance

els, both for the management/leadership and for general and technical personnel.

The main types of exercise are:

- table-top exercises (TTX),
- command-post exercises (CPX),
- technical exercises (TE).

Table-top exercises tend to be conducted for senior staff to discuss escalated issues, raise awareness and find solutions.

Command-post exercises are primarily designed to test or practise routines established for operational teams (such as information exchange, incident management and escalation, or developing and delivering public messages).

Technical exercises are conducted in technical environments to practise and test incident and cyberattack response capabilities in systems and information assets.

Regardless of their different objectives and types, exercises can involve multiple levels of management as well as participants from outside the organisation.

For example, exercises between the national cyber security authorities and other agencies, including service providers and law enforcement agencies, are very useful. Such exercises can be either technical, command-post or table-top exercises.

As a rule, table-top exercises are used first to start building and enhancing collaboration, familiarising the participants with the expectations and actions in crisis situations; the next step is to move on to command-post or technical exercises to test and practise the agreed routines.

The lessons learned from exercises and the resulting preparedness, an effective risk management framework and established continuity requirements, form a strong basis for both the state and the service providers to be able to handle a crisis.

Exercises can also be used to update incident and crisis response plans as well as service recovery plans. Crisis preparedness requires developing a reasonable selection of alternative solutions to be able to provide the best possible access to services

essential for society. Today's crises affect very many stakeholders. Therefore, fast, trust-based cooperation between service providers and the authority coordinating cyber security and critical information infrastructure protection is essential and beneficial.

The lessons learned from exercises and the resulting preparedness, an effective risk management framework and established continuity requirements form a strong basis for both the state and the service providers to be able to handle a crisis.

Practical recommendations for the state and private-sector service providers in preparing for and during a crisis

The tasks of the state in complicated situations

- organise high-quality, rapid exchange of information
- maintain an up-to-date situational picture and communicate it to those affected by the crisis
- analyse potential developments and plan further actions
- organise or support public communication
- define the necessary decisions to be taken by the parties
- support decision-making and enforcement

- Designate an authorised **contact person** to be contacted as needed, to agree on further actions. This person must have a mandate to contact the various staff members of the institution to agree on the necessary division of labour and communicate this outside the institution.
- Define **key processes and workflows** that trigger in the event of a crisis. The key processes and workflows must be practised through exercises, so that their functioning and shortcomings are known.
- Ensure **open communication and exchange of information** with partner institutions and relevant stakeholders.



8.

How to develop a country's cyber security?



Epp Maaten | Programme Director of National Cyber Security
e-Governance Academy

Growing threats and a lack of awareness of the field of cyber security usually lead to the following questions: how secure is the cyberspace of our state and what should we do to improve the situation?

Several methodologies have been developed around the world that assess the development of

the information society and cyber security from different perspectives. One of the best known and most valued of these is the Global Cybersecurity Index developed by the International Telecommunication Union (ITU).²³ This is a survey of all UN members that provides a simple answer to the question of a country's position in comparison to the rest of the world when it comes to matters of

23 See <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>



Figure 13. A screenshot of the National Cyber Security Index website

The NCSI is one of the most detailed cyber security indices in the world. Its advantage over others is the opportunity it provides for countries to identify areas of cyber security in need of improvement.

cyber security. Despite this comprehensive overview, the survey is not very clear regarding the bases on which the countries are ranked.

The e-Governance Academy has developed the National Cyber Security Index (NCSI), which also provides an assessment of the state of a country's cyber security, but in addition offers an opportunity to see the sources on which the assessment is based. In its 2017 comparison of cyber security indices, the International Telecommunication

Union found the NCSI to be one of most detailed. Its advantage over others is the opportunity it provides for countries to identify areas of cyber security in need of improvement. In recent years, the National Cyber Security Index has gained international recognition and rapidly increased the number of countries covered by the index. At the beginning of 2020, the index contained data on more than 150 countries.



Figure 14. The ranking of countries in Asia

How to use the NCSI

The website of the National Cyber Security Index (ncsi.ega.ee) displays a world map and a ranking of countries. The website makes it possible to compare the rankings of countries globally, at regional level or within international organisations.

For each individual country, the index provides an overview of its position based on various commonly used digital indicators such as the International Telecommunication Union's ICT Development Index,

the Global Cybersecurity Index and the World Economic Forum Index. The index also confirms the claim that cyber security supports the country's overall digital development. This means that the indicators of developed digital nations are balanced as they also focus on developing cyber security. When a country's cyber security indicators are significantly lower than its digital development indicators, there is reason to think about how to increase that country's level of cyber security. In addition, the website offers an option to see how a country's position in the index has changed over time.

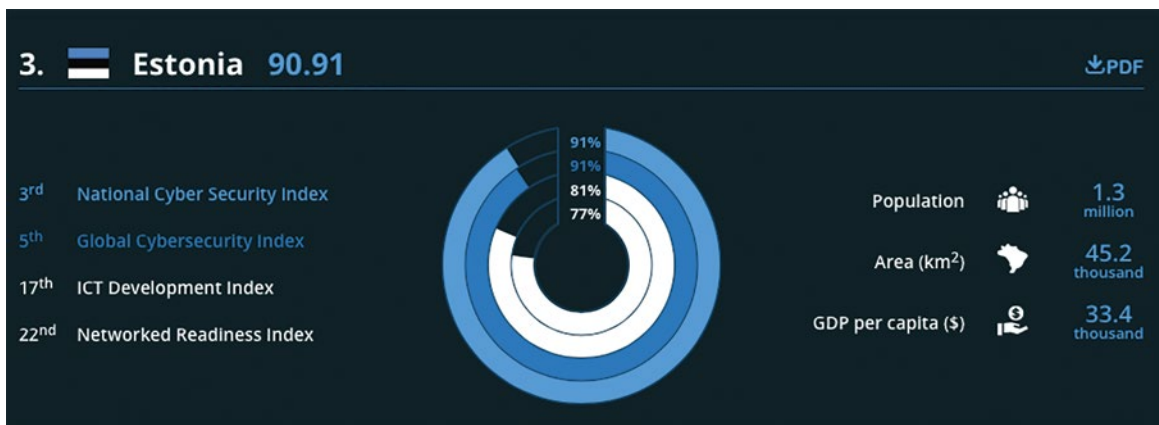


Figure 15. A country's level of cyber security based on four indicators

There are a wide variety of factors to consider when assessing cyber security. In addition to the usual tasks of the state, such as creating legislation or designating responsible institutions, the assessment also surveys activities related to cyber defence, such as in planning curricula at different school stages or in public-private interaction. The existence of a reliable digital identity and a means for its identification are also elements of a country's cyber security, as the use of personalised e-services requires that the services are used only by the person to whom access is granted. Therefore, cyber security can be created through a wide range of activities.

The National Cyber Security Index focuses on activities that can be measured. These measurable activities include:

- (1) the existence of legislation;
- (2) organisations responsible for certain activities;
- (3) forms of cooperation (councils at the national level, working groups and other management structures);
- (4) outcomes of activities, e.g. exercises, policy documents.

Measurable Aspects of Cyber Security

Implemented by the central government

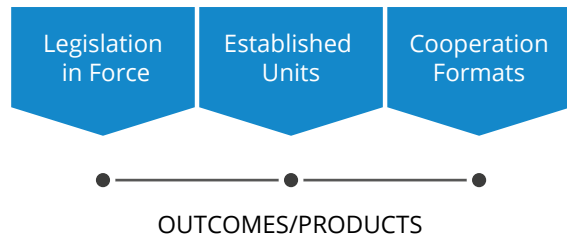


Figure 16. Measurable activities of the National Cyber Security Index

In the National Cyber Security Index, measurable activities are divided into 12 capacities. Each capacity contains multiple indicators. For example, the capacity of cyber security policy includes four indicators that assess whether a country has a cyber security policy unit, formats of cooperation, as well as a cyber security strategy and a plan for its implementation. The other 11 capacities are similarly measurable. The index includes 46 indicators in total.

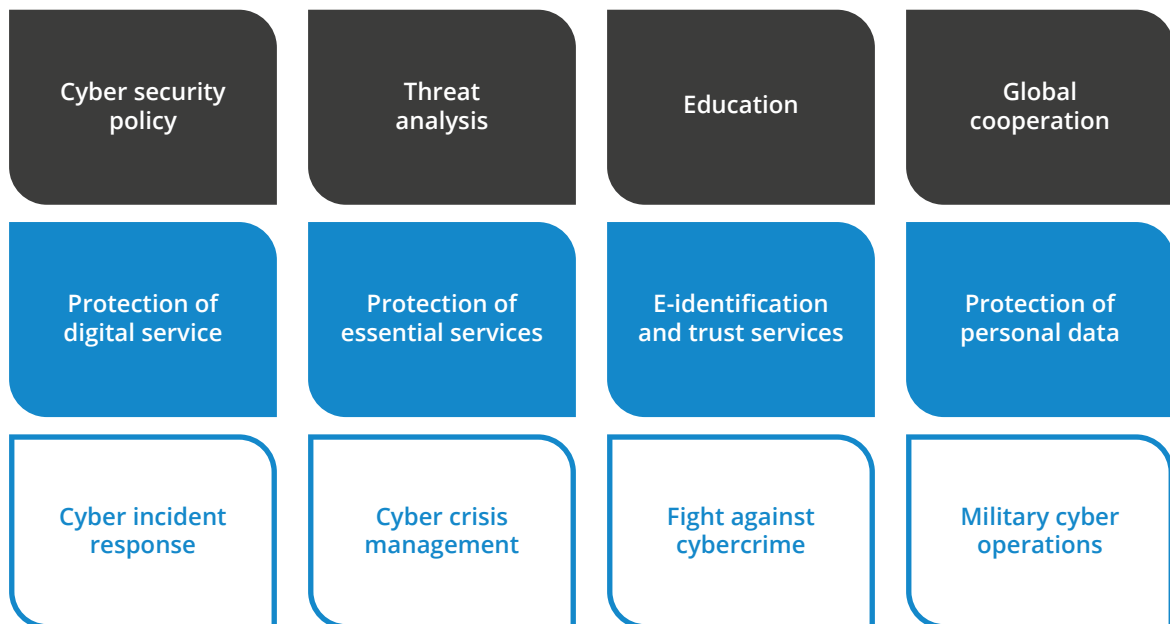


Figure 17. The 12 capacities of the National Cyber Security Index

The page that presents an overview of a country's data provides a more detailed description of all indicators along with the evidence on which the specific scores are based. We consider evidence to be, for example, a link to a law or strategy, to a website of a competent authority, to a news article about a training activity or another relevant document. Therefore, the website of the Cyber Security Index is one large database of references to a country's cyber security documents and activities. Maintaining such a public database and presenting the evidence transparently on the web distinguishes the National Cyber Security Index from other methodologies in the same field.

Submitting data to the National Cyber Security Index is voluntary. National data may be provided by representatives of the state or other competent organisations. In addition, experts from the e-Governance Academy who work on the index on a daily basis collect data from public and official sources. At the same time, our team aims to find partners in each country who are up-to-date on local developments and able to update their country's data on an ongoing basis. The update history and the sources of updates are available on each country's page.

- Would you like to update your country's data in the NCSI?
- Interested in developing your country's cyber security in a comprehensive manner?

Get in touch with the NCSI team
ncsi@ega.ee!

The unique feature of the NCSI is that its data is continuously updated. Unlike other indices, which generally publish assessments once a year, the National Cyber Security Index updates data on a rolling basis – as soon as new country data becomes available and is reviewed by experts.

The National Cyber Security Index is a valuable source of data that each country can use to protect the security of its digital services. Check out the index at ncsi.ega.ee and see what you, as a country, should do to improve the level of your cyber security.

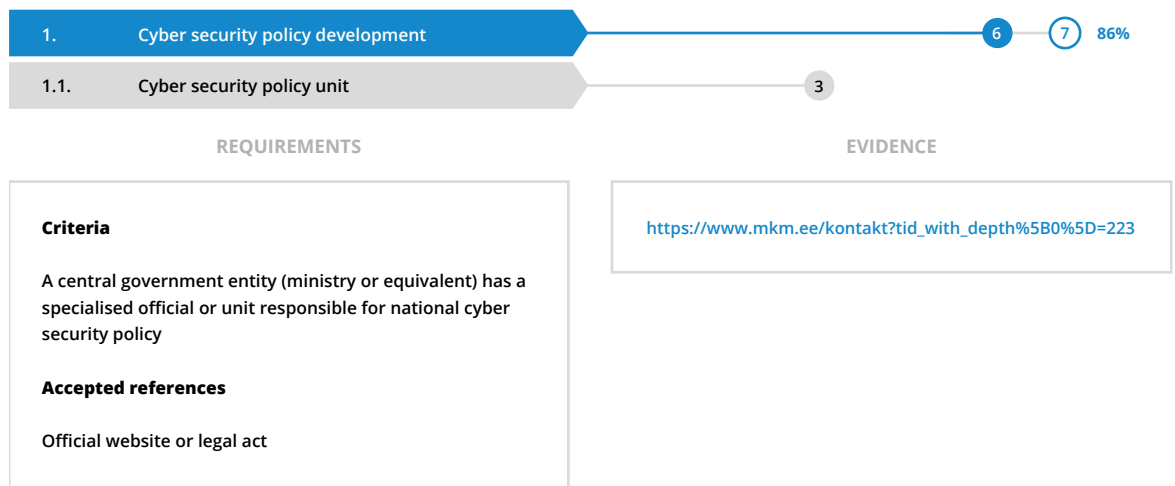


Figure 18. An example of a National Cyber Security Index indicator and the linked evidence

Contributors



Oskar Gross

Oskar Gross has been working as head of the Cybercrime Bureau of the Central Criminal Police at the Police and Border Guard Board since its establishment in 2016. From 2010–2015 he studied at the University of Helsinki focusing on language independent word association analysis, and obtained a PhD in computer science in 2016.



Lauri Luht

Lauri Luht has led the National Situation Centre at the Estonian Government Office since January 2020. Between 2018 and 2019 he worked at the NATO Cooperative Cyber Defence Centre of Excellence as head of Cyber Exercises. Before that he was head of the Crisis Management Department at the Estonian Information System Authority, where his main responsibility was for national cyber security policy and legal issues, cyber emergency preparedness and situational awareness development at the national level. As part of his job Luht has been responsible for planning national and international cyber exercises, plans and procedures for emergency preparedness and international cooperation. Between 2007 and 2013, Luht worked in the Estonian Ministry of the Interior, where he was responsible for supporting the Government Crisis Committee, organising national emergency preparedness and response planning as well as international co-operation issues in the field of civil protection. He is one of the authors of the first Estonian Emergency Act in 2009, and the first Estonian Cyber Security Act in 2018. Luht has carried out capacity building for enhancing digital societies, cyber security and critical information infrastructure protection in Ukraine and Georgia, but also in Central and South America and African countries.



Epp Maaten

Epp Maaten is Programme Director of National Cyber Security at the e-Governance Academy.

Maaten has 20 years of experience from Estonian public sector institutions. She worked as Advisor and Deputy Head of the Electronic Voting Committee. She has advised the President of Estonia and the Chancellor of Justice on information society related matters. Previously, Maaten served at the Estonian Information System Authority and managed government policy and projects concerning critical infrastructure protection and IT risk management. Epp has also been an auditor at Eesti Energia and the National Audit Office. Until 2007, she coordinated the IT projects of the National Electoral Committee, including Internet voting. She is a certified IT auditor (CISA).



Elsa Neeme

Elsa Neeme is a Legal Advisor at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) based in Estonia since October 2018. Prior to joining the CCDCOE she worked at the Cyber Security Branch of Estonia's Information System Authority (RIA) providing in-house legal advice and supporting the execution of RIA's tasks in ensuring cyber security, ranging from incident response to cooperation with private sector service providers. Neeme has been a member of Estonia's Network and Information Systems Directive (EU) 2016/1148 transposition working group and one of the co-authors of Estonia's Cyber Security Act.



Kimmo Rousku

Kimmo Rousku has been working for the Finnish Public Sector Digital Security Management Board (VAHTI) as an expert since 2004, and as General Secretary since 2015. From 2020, he works as Chief Special Expert at the Finnish Digital Agency. Rousku has worked in the ICT sector since 1985 and has exceptionally wide ranging expertise in ICT and security. He has broad work experience as CIO, CISO and CRO in the Finnish government administration. Over the last 10 years, he has specialised in developing information, digital and cyber security, risk management and data protection and developing and utilizing the potential of digitalisation in the public sector. Rousku was nominated as the Chief Information Security Officer of the year 2015 by The Association of Information Security in Finland. He has been listed in the TOP 100 ICT influencers by Finnish TiVi Magazine every year since 2011.



Toomas Vaks

Toomas Vaks has worked in security and risk management positions in the public and private sector for over 25 years. In 2011, he transferred from the position of Chief Risk Officer of Bank Cards in the Swedbank Group to the position of Deputy Director-General at the National Information System Authority (RIA) and began to lead the cyber security unit. The unit performed the tasks of the national CERT, coordinated the cyber security of the state information system and essential services, and monitored the compliance with security requirements. Since the end of 2017, he has worked in the private sector, but continues to contribute to the development of the country's cyber security sector. He actively participates in the work of the State Cyber Security Council and various professional associations. He holds a Master's degree in Social Sciences from Tallinn University of Technology. He is also a graduate of the London Business School and the University of Iceland. Vaks has examined strategic planning and crisis management of cyber safety, and has participated as an expert in various research and development projects.



NCSI National Cyber
Security Index

ncsi.ega.ee | ncsi@ega.ee