UNIVERSITY OF TARTU
Faculty of Science and Technology
Institute of Computer Science
Cybersecurity Curriculum

Magnus Valgre

Evaluating Cybersecurity Capabilities: Organisations' Perspective

Master's Thesis (21 ECTS)

Supervisor: Mari Seeba, MSc

Tartu 2024

Evaluating Cybersecurity Capabilities: Organisations' Perspective

Abstract: To assess their current security posture and pinpoint areas for improvement, cybersecurity capability evaluations serve as crucial tools for organisations. This thesis delves into the landscape of existing methods outlined in the scientific literature, explores practices at the state level, and investigates efforts to aggregate data across multiple countries simultaneously.

Through the selection process, ten relevant methods were identified from the literature, while six countries and five data aggregation methods were chosen for analysis at the state level.

The research places a primary focus on the individual organisation within the broader context, aiming to discern how data-gathering practices within the identified methods consider individual organisations and whether such data reaches higher levels through data aggregation.

The possible challenges and limitations of the described approaches are identified, and possible directions for further work are identified. The intention is to help progress towards a unified evaluation method for organisations, ensuring results that are both comparable and relevant. By addressing these considerations, the research contributes to the ongoing efforts to enhance the efficacy and standardisation of cybersecurity capability evaluations.

Keywords: cybersecurity capability evaluation, organisations' perspective, cybersecurity index

CERCS: T120 - Systems engineering, computer technology

Küberturvalisuse taseme hindamine: organisatsioonide vaade

Lühikokkuvõte: Käesoleva turvapositsiooni hindamiseks ja parandamist vajavate valdkondade leidmiseks on küberturvalisuse taseme hindamised organisatsioonide jaoks üliolulised tööriistad. Käesolev lõputöö uurib teaduskirjanduses välja toodud olemasolevaid meetoid, riigi tasandi praktikaid ja mitme riigi andmete koondamisel järgitavaid praktikaid.

Valikuprotsessi käigus tuvastati kirjandusest kümme asjakohast meetodit, riigi tasandil analüüsimiseks valiti kuus riiki ja viis andmete koondamise meetodit.

Uurimistöö keskendub esmajoones üksikule organisatsioonile laiemas kontekstis, püüdes välja selgitada, kuidas tuvastatud meetodite raames kasutatavad andmete kogumise praktikad arvestavad individuaalsete organisatsioonidega ja kas sellised andmed jõuavad läbi andmete koondamise kõrgemale tasemele.

Selgitatakse välja kirjeldatud lähenemiste võimalikud puudused ning võimalikud suunad edasisteks uurimustöödeks. Eesmärk on aidata liikuda organisatsioonide ühtse hindamismeetodi poole, tagades nii võrreldavad kui ka asjakohased tulemused. Neid küsimusi käsitledes aitab uurimus kaasa käimasolevatele jõupingutustele küberturvalisuse võimekuse hindamiste tõhususe ja ühtlustamise suurendamiseks.

Võtmesõnad:Kübertruvalisuse taseme hindamine, organisatsioonide vaade, küberturbe indeks

CERCS: T120 Süsteemitehnoloogia, arvutitehnoloogia

Acknowledgements

I want to express my gratitude to my supervisor, Mrs. Mari Seeba, whose patience, guidance and collaborative approach made the process all the more enriching.

I also want to thank my wife without whose support I would never have gotten this far.

I am very grateful to the experts at the National Cyber and Information Security Agency of the Czech Republic, the e-Governance Academy in Estonia, and Irina Klementi at the Estonian Ministry of Economic Affairs and Communication for giving me their time and providing valuable input to this thesis.

This work is part of the Cyber-security Excellence Hub in Estonia and South Moravia (CHESS) project funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Abbrevations and Definitions

Abbrevations

- CSIRT - Cybersecurity Incident Response Team
- ECCC - European Cybersecurity Competence Center
- eGA - e-Governance Academy
- ENISA - The European Union Agency for Cybersecurity
- EU - European Union
- G20 - Group of 20. Intergovernmental forum made up of the largest economies of the world.
- GCI - Global Cyber Security Index
- GDPR - General Data Protection Regulation
- ICT - Information and Communication Technologies
- ITU - International Telecommunications Union
- ISACA - Global association of IT professionals focused on governance. Previously known as the Information Systems Audit and Control Association
- ISMS - Information Security Management System
- IOT - Internet of Things
- NCC - National Coordination Center
- NCISA - the National Cyber and Information Security Agency of The Czech Republic (NÚKIB in Czech)
- NCSC - National Cybersecurity Center
- NCSI - National Cyber Security Index
- NIS2 - Network and Information Security Directive
- NIST - National Institute of Standards and Technology
- SETA - Security, Education, Training, Awareness
- SMEs - Small and Medium-Sized Enterprises
- VPN - Virtual Private Network

Contents

1 Introduction

This thesis reviews the current state of cybersecurity capability assessments from various angles, focusing on individual organisations. Mainly how the cybersecurity capability evaluations are performed on individual organisations and how their experience carries over to evaluations conducted on broader domains.

There are several reasons why an organisation might want to evaluate its cybersecurity capabilities. First and foremost, to identify any missed vulnerabilities in the system. If an organisation does not assess the current state, then there is no basis for building improvements. However, even in an organisation with strong preventative measures in place, security incidents can still happen. In such cases, the organisation must be aware of its capability to maintain normal operations and minimise damages in the face of security breaches.

Organisations need to be aware of their cybersecurity posture for their own sake but are also facing regulatory pressures. All EU member states have until October of 2024 to ratify the NIS2 directive [1], which replaces the previously in effect NIS directive [2], in their national law. Article 21 [3], paragraph 1 of the directive states:

> "Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services."

Furthermore, paragraph 2 of the same article specifies that *"policies and procedures to assess the effectiveness of cybersecurity risk-management measures"* are a required part of the measures referred to in paragraph 1. This means that cybersecurity capability evaluations must become a regular part of EU member states' cybersecurity policies.

Furthermore, a robust security posture is not only essential to the organisation itself but also to other connected organisations and the environment as a whole. In December of 2023, Asper Biogene, a company that provides genetic testing services for its customers, fell victim to a data breach [4]. Criminals obtained the personal data of about ten thousand patients, including genetic testing results. The Data Protection Inspectorate claims that in this case, the business clients of Asper Biogene, as the data controllers, are also responsible and could face legal consequences [5]. Reliance on third-party vendors for business operations and services is an increasing source of risk for all organisations [6].

There are several ways to evaluate the cybersecurity capabilities of an organisation. Leszczyna performed a literature review [7] describing the methods available in the scientific literature and assessing their applicability in the real world. He identified six common categories of cybersecurity assessment methods: checklist-based evaluation, compliance checking, vulnerability identification and analysis, penetration testing, simulation or emulation-based testing, and formal analysis and reviews. This thesis mainly looks at methods belonging to the checklist-based evaluation and compliance-checking categories, with some methods similar to formal analysis and reviews.

In addition to single organisations, evaluations are performed on more significant subjects, like whole economic sectors [8] and countries [9]. The end goals of these evaluations are the same. Still, due to the larger scale of the subjects, they can be considered a different kind of system altogether and need another approach method for evaluation [10]. These evaluations rely much more on the environment the subject is in, using a more top-down approach. For example, the legislation and existence of certain agencies are taken as a measurement of cybersecurity capabilities.

The thesis aims to explore the existing approaches to cybersecurity capability evaluations for organisations and investigate how the cybersecurity posture of individual organisations is considered at a broader level.

Measuring, Assessing, Evaluating According to Huitt [11], measuring, assessing, and evaluating are three distinct processes. Measuring is the process of attributing a numerical value to the characteristics of an object or a part of an object. In the context of this thesis, measuring is defined as attaching a numerical value (or a score) to the cybersecurity capabilities, or a single aspect of the capabilities, of a given subject (a country or an organisation). Assessment is the process of collecting data on a subject to make judgements about them. In the context of this thesis, assessment is the process of gathering data about a given subject's cybersecurity capabilities. Evaluation is the process of determining the capabilities of a subject through the data collected during assessment. In the context of this thesis, evaluation is the process of appraising a subject's cybersecurity capabilities according to the data collected during the assessment.

The thesis is structured as follows. The introduction section (Section 1) sets out to give the reader a general introduction to the topic, introduce the research problem, and the author's motivation and contribution. Section 2 details the research methodology and limitations of the thesis. The following three sections each examine cybersecurity capability assessments from three different perspectives. Section 3 explains the current state in scientific literature, looking separately at proposed methods and independent evaluations that have been carried out. Section 5 reviews the methods of practices that aggregate data on several countries in parallel. Section 4 examines how six EU member states (Finland, Estonia, Latvia, Lithuania, Poland, and the Czech Republic) have approached the problem in their respective countries. Following the three sections on findings is Section 6, which describes the validation method and discusses the thesis findings. Section 7 is the thesis's conclusion and final section.

1.1 Motivation

The motivation for the thesis is to support the development of a tool for assessing cybersecurity capabilities named Framework for Security Level Evaluation (F4SLE) [12]. This thesis supports the development of F4SLE by providing background research on capability evaluation methods already available and by describing their strong and weak points. F4SLE is also one of the methods described in Section 3.

Currently, F4SLE is in the pilot study phase. As part of the CHESS[1] project, F4SLE is being tested in organisations from Estonia and the Czech Republic.

1.2 Research Question

The thesis aims to answer what the current approaches for cybersecurity capability evaluations for individual organisations are. Furthermore, the thesis aims to explore what approaches have been taken by countries and initiatives that aggregate data on several countries at once. The primary research question (PRQ) can be worded as follows: **What are the limitations of presently proposed methods and practices of cybersecurity capability evaluations on organisations?** To answer the primary question, the following secondary research questions (SRQ) should be answered:

- **SRQ1**: What methods have been proposed in the scientific literature for conducting cybersecurity capability evaluations on organisations?
- **SRQ2**: What methods have been employed for one-time capability evaluations in the scientific literature?
- **SRQ3**: What are the practices employed at the country level for cybersecurity capability evaluations?
- **SRQ4**: How do data aggregation methods used in cybersecurity capability evaluations consider individual organisations?

1.3 Contribution

The author searched for and reviewed available scientific literature on the topic (Section 3). The scientific literature was divided into two parts: proposed methods and performed assessments. The author also examined how six EU member states (Finland, Estonia, Latvia, Lithuania, Poland, and the Czech Republic) have approached cybersecurity capability assessments in their countries (Section 4). The author also researched relevant cybersecurity evaluation data aggregation practices (Section 5). The author also interviewed experts from the Czech Republic and Estonia. As part of the CHESS program,

[1] https://chess-eu.cs.ut.ee/

the author also took part in a trip to Brno in Czechia to visit colleagues at Masaryk University.

2 Research Method

2.1 Literature Selection Process

The author performed a literature review following the methods outlined by Kitchenham [13] to assess the current state of cybersecurity capability evaluation methods and individual evaluations in the scientific literature.

The author used a previously performed literature review [7] on the topic as a starting point to find relevant research literature. The author was introduced to the review in a course on master thesis writing as recommended reading. Furthermore, snowballing was used to identify more relevant studies in the literature reviews of the methods described by Leszczyna.

The author performed a keyword search through the Google Scholar database to cover research published later than the previously mentioned literature review and the papers described in the review. The keywords used to perform the search were cybersecurity, information security, assessment, capability, evaluation, measuring, level, and preparedness. A lower publishing date limit of 2021 was used to limit the results. The Google Scholar search engine returns the search results it deems relevant to any of the inserted keywords, not only those relevant to all. The author also tried to maximise relevant results using search operators and quotation marks. Combining keywords would yield several thousand results even with the date limit and extra parameters. For example, the keyword combination "cybersecurity level evaluation organisation" yielded 17,300 results. The search engine places the most relevant results at the top, so the author sifted through the results until no more relevant papers could be found.

Papers that were not generally applicable or too technical were excluded. General means that the central method proposed in the paper should apply to any organisation to help them evaluate their cybersecurity capabilities regardless of specialisation. Also, methods that relied only on technical measures like network scanning or penetration testing were excluded.

Following these steps, the author identified nine relevant scientific papers. Four were through previous literature reviews, three were through snowballing, and one was through a database search. The nine papers cover eight methods, with two introducing a method and a pilot study. In addition, the author also decided to include the F4SLE [12] method in the analysis. Figure 1 illustrates the initial method search process.

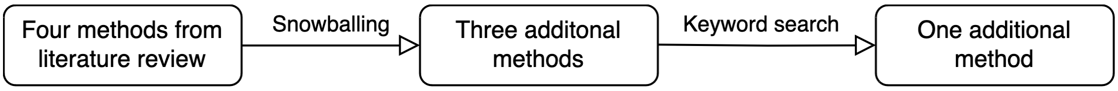


Figure 1. The initial method search process.

The thesis also reviews the methods of one-off cybersecurity capability evaluations found in the scientific literature. To limit the scope of results, the author decided only to review evaluations performed on the countries described in Section 4. A combination of the previously listed keywords and the name of the given country was used to find research literature on specific countries. In the case of the Czech Republic, both currently accepted international names of the country, the Czech Republic and Czechia [14], were used in the search. In the case of countries, the focus was on finding performed evaluations, not methods. Through the database search, the author was able to find seven relevant papers, but none on Latvia or the Czech Republic.

2.2 Data Aggregation Method Selection Process

The most common cybersecurity capability data aggregation methods are cybersecurity indices. There are several different approaches to what an index is. For example, the New York University's Tandon School of Engineering publishes the Index of Cyber Security [15], a single numerical value representing the overall perceived threat level of the current cybersecurity environment. For the purpose of this thesis, the author chose to focus on indices that rank and aggregate data on countries.

Furthermore, many indices rank countries according to different perspectives, like the OECD Better Life Index [16]. In this thesis, the author chose to focus on indices that specifically measure cybersecurity and cyber-related capabilities.

The chosen indices also had to be currently active for a better comparison base and to ensure relevancy. The author excluded any indices that had not been updated or were seemingly inactive for over two years.

Based on these observations, the cybersecurity indices for comparison were chosen based on the following criteria.

- The subjects of the index should be countries.
- The index should be focused on cybersecurity-related capabilities.
- The index has to be active.

Through an Internet search, the author was able to find five indices that align with the specified criteria. These indices are described and compared in Section 5. The author also supplemented Internet searches with an investigation of literature reviews on cybersecurity indices [17], [18], but these did not yield any additional relevant indices.

In the case of the National Cyber Security Index, the e-Governance Academy was contacted directly over email for additional information about the methodology. This has been pointed out specifically in the text.

2.3 Country Selection Process

To compare state-level approaches to cybersecurity capability evaluations, six countries were chosen: Finland, Estonia, Latvia, Lithuania, Poland, and the Czech Republic. These particular countries were selected due to their geographical closeness to and the similarity of their geopolitical situation to that of Estonia. With the main challenge being the proximity of Russia to the East [19], [20]. The countries also provide a broad base of comparison in history, size, and economy.

2.4 Validation

The author validated the findings by conducting two semi-structured expert interviews. The process and results are detailed in Section 6, and the questions can be found in Appendix 1.

2.5 Limitations

As the author is not familiar with the native languages of the covered countries, this is a possible limitation of the research: the author cannot be sure that he was able to find all the related information.

In the case of scientific literature, the author relied on a previous literature review [7] on the topic to find previous research. This could mean that any literature the review's author missed is also missing in this thesis.

Publications by private enterprises specialising in business or cybersecurity consulting have been excluded from the analysis. Although their methodologies would be relevant to this topic, the publications are often vague and are mostly marketing material. These publications aim to attract customers and do not want to reveal their proprietary methods for competitors to see.

Due to time constraints and in the interest of clarity, the author decided to exclude cybersecurity maturity models from this analysis. Although some of the described methods share similarities with maturity models, some are based on one.

The validation was carried out with two expert interviews, and it should be acknowledged that opinions among other professionals might differ. Still, the insights obtained are a valuable contribution to this thesis.

3 Literature Review

3.1 Introduction

The following section aims to address two specific research questions. **SRQ1**: What methods have been proposed in the scientific literature for conducting cybersecurity capability evaluations on organisations? **SRQ2**: What methods have been employed for one-time capability evaluations in the scientific literature? The section is divided into cybersecurity capability evaluation methods and performed evaluations. The first part describes the proposed evaluation methods, and the second part describes the methods of evaluations conducted on specific subjects. The distinction between these two types of literature was made because each focuses on a different part of the process. Methods mainly describe the tools and techniques that could be used to evaluate start to finish. Independent evaluations mainly describe the results of a single evaluation, with the methodology not being the main focus.

3.2 Cybersecurity Capability Evaluation Methods in Scientific Literature

The methods described in this subsection were chosen through the steps described in Section 2. Each approaches the challenge of cybersecurity capability evaluations from a different vantage point, giving a varied overview. Although, as will be discussed in Section 6, there are many issues still left unresolved.

Organisations can vary widely in all their aspects, and what works with one might not work with another. You et al. [21] proposed a cybersecurity capability assessment approach that can be tailored to fit the needs of each individual organisation. According to the methodology, an assessment can be carried out in four stages: the preparation phase, the check phase, the classification phase, and the improvement and review phase. In the preparation phase, officials performing the survey determine the criteria and control items best suited for the assessed organisation. The check phase: The officials compile a survey based on the identified criteria, distribute it, and retrieve it. In the classification phase, the officials divide the criteria identified in the first phase into three levels of importance (mandatory, significant, and recommended). The improvement and review phase: Based on the survey results and the classifications done in the previous phase, the organisation's security level is determined on a scale of 0 to 1. As validation, the authors assessed 15 thermal power plants in South Korea.

Conversely to the previous, the following method has the opposite approach. Bernik and Prislan [22] created a 10 by 10 information security performance model, named ISP 10X10M in short. The model is made up of ten areas and ten key performance indicators under those areas, hence the 10 by 10 name. The authors stress the wide scope and generality of the model. The areas specified in the model are physical information security controls, technical and logical security controls, information resources management, employee management, information risk management and incident handling, organisational culture and top management support, information security policy and compliance, security management maturity, third-party relationships, external environment connections. Each area consists of 10 key performance indicators that the respondents are asked to answer on a scale of one to five, where one means a measure is not adopted and five means fully implemented in practice.

Prislan et al. [23] followed the initial model development with a study applying the model in a real-world scenario. The authors carried out surveys among 20 private enterprises in Slovenia. The authors initially selected 193 enterprises to participate in the study but were only able to get 20 to respond and fill out the questionnaire. Even though 20 might seem small, it is one of the larger sample sizes that can be found in the existing literature where proposed methods have undergone real-world testing.

The combined cybersecurity posture of organisations in a country is an essential indicator of the situation as a whole. Recognising this, Jazri et al. [24] further developed the cybersecurity wellness idea first introduced by ITU [25] with their cyberwellness profiles (also discussed in Section 5). The authors propose a bottom-up assessment technique of assessing the critical infrastructure organisations in a country for an overview of the situation in a whole country. This is opposed to the more typical top-down technique where legislation and government attitudes are used as metrics for the cybersecurity posture of a country. The authors compiled a questionnaire consisting of 114 cybersecurity vital signs based on the NIST framework[2] and ISO/IEC 27001 standard[3]. There is, however, no discussion on how the broader evaluation at the state level should take place. For validation, the authors then conducted interviews among 20 critical infrastructure organisations in Namibia and determined their cybersecurity wellness index value. On average, the whole process took a single working day per organisation.

Seeba et al. [12] proposed the F4SLE (Framework for Security Level Evaluation) method, designed to be universally applicable across diverse organisations. Based on the Estonian Information Security Standard (E-ITS)[4], F4SLE encompasses ten security dimensions, each having four possible levels (Initial, Defined, Basic, and Standard). The dimensions are Information Security Management System, Organisation and Personnel, Concepts, Operation, Detection and Reaction, Applications, IT Systems, Industry IT, Networks and Communication, and Infrastructure. The primary goal is to establish a method that yields comparable results, aiming to evaluate the cybersecurity posture of entire organisational groups, not solely individual entities. Additionally, Seeba et al. [26] presented the MASS (Measurement Application for Self-assessing Security) tool, offering a browser-based environment for organisations to work with F4SLE. While

[2] https://www.nist.gov/cyberframework

[3] hhttps://www.iso.org/standard/27001

[4] https://eits.ria.ee/

F4SLE is currently in the developmental phase and lacks official adoption, pilot study feedback from 54 respondents indicates an average completion time of one to two hours. Responding organisations promptly receive feedback through a spider chart covering the ten security dimensions mentioned earlier.

Organisations are primarily made up of people, and cybersecurity awareness and management processes can be as important as technical security measures. Maleh et al. [27] introduced a capability assessment framework that focuses on improving management processes and human aspects to increase an organisation's cybersecurity capabilities. As validation, a survey was carried out in a large port organisation in Morocco among 104 IT professionals. Responding to the survey took an average of 30-45 minutes for a stakeholder from the organisation to fill it out.

Moreover, evaluating the cybersecurity awareness of the members of an organisation can be a way to get a picture of the organisation's cybersecurity posture as a whole. In their research paper, Goode et al. [28] introduced a way to assess the human aspects of organisational cybersecurity capability. The authors devised a way of measuring the effectiveness of Security, Education, Training, and Awareness (SETA) programs in an organisation. With the help of a panel of experts, the authors composed a questionnaire of vignettes to test the respondent's awareness of security risks and organisational policy. Vignettes describe hypothetical situations employees might encounter during their everyday work lives. For example: *"Sandy's supervisor requested her to leave the office computer unlocked so other employees can use it while she is out to lunch or away from the office."* As initial prototypes, the authors constructed nine vignettes and conducted surveys in 21 SMEs for validation.

Another approach is to combine the technical and human aspects. Rae and Patel [29] developed a cybersecurity rating scheme for small and medium-sized enterprises. The main difference with other schemes is the addition of behavioural and risk propensity questions in addition to questions about technical controls. For example, questions that ask the SME representative if they even consider cyber threats an issue or who they would go to if they needed help with a cyber issue. The authors created a survey with ten questions on both the technical and behavioural aspects.

Some authors emphasise producing as little discomfort as possible for the subject organisations. Like Malaivongs et al. [30], who introduced the Cyber Trust Index (CTI) in their paper. The authors emphasise speed, flexibility, adaptability, and minimal effort with their framework. The CTI uses binary question paths and fewer questions to make the assessment process as easy as possible for organisations. The authors conducted a pilot study among 35 organisations from Thailand's critical infrastructure networks.

Following the same ideas, Qiangmin et al. [31] proposed a methodology for optimising survey-based cybersecurity capability assessments. The authors introduced a system by which criteria that duplicate others and are of lesser importance can be removed, thereby reducing the resources needed to fill out the survey and process the results.

3.3 Cybersecurity Capability Evaluations in Scientific Literature

This subsection describes the methods of one-off cybersecurity capability evaluations performed and published in the scientific literature. To limit the scope of papers, the author chose to focus on the countries described in Section 4.

In the case of independent evaluations, the survey is a common method for data gathering, but it is not the only one. Over the years 2016 - 2019, Szczepaniuk et al. [32] performed a longitudinal study on implementing Information Security Management Systems in units of Polish public administration. One part of the research defined the conditions needed to implement an ISMS, and the second part assessed the efficiency of information security management in public administration. The second part of the research was conducted through surveys with 50 public administration units participating. The authors found that there has been a steady uptake in implementing information security management systems in public administration over the years covered. The authors credit this advancement to increased legal pressure from European Union legislation, including the GDPR.

With a similar approach as the previously described paper, Chodakowska et al. [33] performed another research on local government administrators of Poland in 2022. The study aimed to determine if local municipalities have a cybersecurity policy in place and if it is actually being applied in practice as well. The research was conducted through online surveys, and a request to participate was sent to all the municipalities of Poland. From the 2477 total municipalities invited, 1787 responded, making the response rate 72.1%. This study supports the conclusions reached by Szczepaniuk et al. in the previously described study by stating that the majority of municipalities have an information security management system in place. However, there is still a lot left to do. On the negative side, the authors list the following: lack of a security policy, lack of a habit of reporting security-related incidents, lack of security audits, lack of insurance against the risk of cyber-attacks, and lack of appropriate staff training. The authors also bring out an interesting paradox concerning evaluating cybersecurity capabilities and monitoring in general. Those municipalities that have their cybersecurity infrastructure set up correctly tend to report more incidents than those whose capabilities are lacking in comparison. This is explained with better capabilities in general, meaning better capabilities in incident detection, but at first sight, this finding can cause confusion.

As an example of an evaluation performed on a whole economic sector, Gavenaite-Sirvydiene and Miecinskiene [8] studied the significance of cybersecurity in Lithuania's financial sector. Although the authors' main goal was to get an idea of the significance of cybersecurity for the financial sector, they also identified relevant risks and assessed the preparedness of the sector.

The multi-criteria expert decision analysis method, TOPSIS [34], was selected as the research method. The experts interviewed belonged to financial institutions such as banks and non-life insurance companies. Furthermore, the experts were required to have at least ten years of experience in the financial field and work in leading positions in either IT security, data protection or risk management. The experts were asked to rank their institution's preparedness to face different cyber events for the capability assessment part. The specified cyber events were listed as malware, insider threats, denial of service, account takeover and credential abuse attacks, phishing, web application attacks, and ransomware. As such, the data-gathering method can be categorised as one based on surveys. In the results of the analysis, the authors state that, in general, the Lithuanian financial sector is aware of its weak points regarding cybersecurity and is constantly investing in fixing them.

There are also examples where a survey-based solution is used to evaluate not only the organisations in a country but the whole country. In 2017, Bada and Weisser-Harris [9] conducted a cybersecurity capacity review of Lithuania. From April 24 to 26, 2017, the researchers from the Global Cyber Security Capacity Centre (GCSCC)[5] interviewed stakeholders from the public and private sectors. The stakeholders primarily belonged to different state government institutions, but some participants were also from the police agencies, finance sector, academia, and the private sector. No further details are provided on who exactly participated from the private sector. Lithuania was the 17th country reviewed by the GCSCC. As of August 2023, the GCSCC has coordinated and facilitated over 130 reviews worldwide, mostly in countries belonging to the global south.

The researchers used their own GCSCC Cybersecurity Capacity Maturity Model [35] to perform the analysis. The model specifies five dimensions (Cybersecurity Policy and Strategy; Cyber Culture and Society; Cybersecurity Education; Training and Skills; Legal and Regulatory Frameworks; Standards, Organisations and Technologies), which all consist of more specific sets of factors. The maturity dimensions are assessed along the following scale: Start-up, formative, established, strategic, and dynamic.

As a result of the analysis, the authors determined that in 2017, Lithuania was in the process of building up its cybersecurity capabilities, with legal and regulatory aspects being the most advanced.

Lehto and Limnéll [36] conducted research into the importance of strategic leadership in cybersecurity. The study was conducted through manual data collection and expert interviews, emphasising the interviews more significantly. The interviews were carried out in a semi-structured way with 40 employees in managerial roles in public and private organisations.

The paper concludes that Finland needs a more centralised approach to cybersecurity management, with the Prime Minister's Office being the most likely point of concentration. According to interviewed experts, the lack of a sufficiently strong central authority has also been a detriment to the Cyber Security Strategy Implementation Programme.

As can be seen in Section 5, another source of data for evaluations is public records. This is usually the case when the evaluation is performed on a whole country. In 2017,

[5] https://gcscc.ox.ac.uk/home-page

Wong et al. [37] benchmarked Estonia's cybersecurity capabilities and compared them to those of the USA by reviewing policy changes implemented after the 2007 Bronze Night cyberattacks. The authors used the cybersecurity strategies of the respective countries as the primary sources for their study. The authors determined that the USA could benefit from rapid resource investments in cybersecurity awareness programmes and public-private cooperation.

3.4 Summary

While there is literature available, it's worth noting that the scope of existing research in this area is relatively narrow.

Table 1 compares the described cybersecurity capability evaluation methods. The column headers are explained as follows:

- **Authors** states who the authors of the method are.
- **Year Published** states when the study or studies if there are several papers, were published.
- **Number of Questions** details how many questions the survey questionnaire contains.
- **Answer Scale** details the exact answer scale used for the questionnaire.
- **Data Collection** shows the data collection approach for the method.
- **Activity After Study** details what further work has been done on the method after the initial study.
- **Time Investment for Subject** details the amount of time an evaluation is expected to take from the subject.
- **Feedback for the Subject** details the feedback the subject can expect.
- **Possible to Implement** shows if it is possible to implement the given method using the information provided in the paper.
- **Tool Used** details what tool is used to facilitate data collection.
- **Updating Cycle** details the time period after which the method and its components are reviewed.

Some patterns emerge from the table. The number of questions can vary significantly between the methods. From 20 to 200, and some do not specify the amount at all.

The question of time investment for subjects is not a big concern for the authors. Of the three that specified the possible time investment, it varies from half an hour to a working day.

Feedback for the subjects is another point of interest. Most authors only specify a single score the subjects receive back without further discussing how this can benefit the subject. Three of the methods specify that the subject gets back a separate score for each aspect of the evaluation, which can be more beneficial.

Only one of the authors considered the updating cycle of the method in their study, but only in the sense that the survey should be tailored to each evaluation separately. It should be acknowledged that Seeba et al. later published a separate study specifically on this issue [38].

Answers to Research Questions To answer **SRQ1**: The methods described here gather information from organisations through surveys and interviews using a checklist-based approach to evaluations. The methods deal with organisations directly, and the product of the process is an evaluation of a single organisation.

To answer **SRQ2**: The methods here gather information through interviews or from public sources. The subjects of the single evaluations are not organisations but local governments, economic sectors, or countries.

Table 1. Scientific Literature. '—' means that no information is provided. '●' means 'Yes'. ○ means 'No'.

Authors	Qiangmin et al. [31]	Jazri et al. [24]	You et al. [21]	Bernik and Prislan [22], [23]	Maleh et al. [27]	Goode et al. [28]	A. Rae and A. Patel [29]	Malaivongs et al. [30]	Seeba et al. [12], [26]
Year Published	2007	2011	2016	2016, 2020	2017	2018	2019	2022	2021, 2022, 2024
Number of Questions	—	114	—	100	100	—	20	70 Maximum	Around 200
Answer Scale								Binary	0 - 4
Data Collection	—	Survey	Survey	Survey	Survey	Survey	Survey	Survey	Survey
Activity After Study	—	—	—	Validation Study	—	Thesis	—	—	Work Ongoing
Time investment for subject	—	Less than a day	—	—	30 - 45 minutes	—	—	—	1 - 2 hours
Feedback for subject	N/A	Score	Score	Score for each factor	Level for each aspect	—	Score	Grade	Level for each dimension
Possible to implement	●	○	●	●	○	○	○	○	●
Tool Used	—	Interview	Decided case-by-case	—	—	—	—	Interview	Web Interface
Updating Cycle	—	—	Every evaluation	—	—	—	—	—	—

4 Country Practices

4.1 Introduction

The following section aims to answer **SRQ3**: What are the practices employed at the country level for cybersecurity capability evaluations? To answer this question, six EU member states were chosen for comparison: Finland, Estonia, Latvia, Lithuania, Poland, and the Czech Republic. In addition to the findings here, Section 3.3 describes independent evaluations published in the scientific literature on these same countries.

4.2 Finland

In February of 2022, the Finnish Ministry of the Interior and the Ministry of Defense started a project to assess Finnish cybersecurity capabilities. The project evaluated the national ability to defend against serious cyber threats and identified areas needing further development. The workgroup also proposed legislative improvements. In April of 2023, a preliminary report [39] of the results was published.

The report concludes that Finland is unprepared for serious cyber threats, emphasising the need for better cooperation between authorities. Unfortunately, the report's methodology section does not specify how the data was gathered. It is stated that a survey was conducted, but there is no further explanation of who participated and what the questions were.

As an example of an official tool that helps organisations in the country assess their cybersecurity capabilities, The National Cybersecurity Centre of Finland is developing the Cybermeter [40] (Kybermittari in Finnish). The tool uses the NIST's C2M2 maturity model as its base for the evaluation, with some adjustments made to fit the Finnish environment better. One of the primary motivations for developing the tool is the current fragmented state of capability measurements. Different organisations use different methods that are not compatible with each other and which produce results that are not comparable. With Cybermeter, NCSC-FIN aims to create a unified tool that sets a common language for cybersecurity capability assessments among the organisations in Finland [41]. In addition to self-assessment, organisations can voluntarily share their results with NCSC-FIN for statistics and analysis.

Regarding raw data-gathering, Statistics Finland, the Finnish state data agency, gathers and publishes data on the use of information technologies in enterprises [42]. Statistics have been collected on many metrics, but only one is related to cybersecurity: the percentage of enterprises that use cloud-based security software.

4.3 Estonia

In 2020, the Center for Security Studies in Zürich published a report [43] on the state of cybersecurity in Estonia. The report is one in a series of reports on the cybersecurity capabilities of various nations. For example, some other nations assessed by the competence centre are Japan [44] and Romania [45]. The report on Estonia is the latest in the series, and none have been published since, nor have there been any updates to the reports published thus far. The report recounts some of the most essential cybersecurity-related events in Estonian history. It overviews the then-current state of Estonian cyber capabilities by covering policy, strategy, and international cooperation. The report brings out the following positive aspects of Estonia's approach: coherence of strategic planning, the "just do it" attitude of Estonian bureaucracy, and a commitment to international cooperation and alliances, including a total commitment to NATO even through limited resources. The author relied on publicly available sources, including legislation and official government publications, when writing the report.

The National Audit Office of Estonia [46] has published three audits on the topic of cybersecurity since 2018. In 2021, the office published an audit on the administration and reliability of the X-Road[6] data exchange platform [47]. In 2018, the office published two audits: one on the security and preservation of critical state databases [48] and one on implementing ICT security measures in local governments [49].

The Estonian Statistics Board gathers data on ICT integration among enterprises, including several metrics about cybersecurity. For example, data about the different cybersecurity measures implemented in the enterprises (user authentication, patch management, off-site backups) and recent cybersecurity incidents. But also about employee training and who carries out cybersecurity-related tasks in the enterprise [50]. According to the methodology [51], the survey takes 67 minutes on average to fill out. It should be noted that the survey is a lot wider and has many other ICT-related questions that are not covered here.

In an interview with the author, the cyber risk management leader at the Estonian Ministry of Economic Affairs and Communication stated that the ministry conducts a simple survey among some of the ministries, the constitutional institutions and the most significant local governments. The survey aims to identify weak points and determine who might need additional help.

4.4 Latvia

The Central Statistics Bureau of Latvia conducts surveys among the country's enterprises and individual citizens, and some are related to cybersecurity topics. For example, enterprises that provide employees with information on ICT security requirements, ICT

[6] https://www.x-tee.ee/home

specialists in enterprises, and individuals who have experienced security-related incidents using the Internet. For individual persons, the data is gathered through surveys, either done face-to-face or on the phone. For enterprises, the data is collected either through surveys or through the enterprise's tax declarations. Each database does not mean an individual survey. Instead, a single survey covers several topics, separating the answers into different categories for clarity[52], [53], [54].

In 2022, the State Audit Office of the Republic of Latvia performed an audit [55] to answer the question: are access to information systems and the receipt of e-services reliable? The audit concludes that it is impossible to answer this question unambiguously due to several issues in how the data is gathered and inadequacies in the associated law. The audit was conducted on-site through interviews and data collection in the Ministry of Defence and Environmental Protection and Regional Development.

4.5 Lithuania

In 2015, an audit [56] was performed by the National Audit Office of Lithuania. The audit aimed to determine if an adequate cybersecurity infrastructure has been set up and if cybersecurity is ensured in public establishments in Lithuania. The audit analysed the then-current regulations, strategies, management practices, and fund allocations. The audit was conducted on-site at eighteen public establishments, mainly the Ministry of Interior and the Ministry of National Defence. The audit covered data from 2011 to the first half of 2015.

Statistics Lithuania, the State Data Agency, gathers information on various ICT topics [57], among some cybersecurity metrics. Data on the following metrics is collected: ICT security tools used by enterprises, methods of cybersecurity training, the performance of security-related tasks in an enterprise, documentation on different security measures, enterprises that have suffered cybersecurity-related incidents, and enterprises that have insurance against cybersecurity-related issues. The data is gathered through a survey sent out to enterprises in a random sample. In the latest iteration, the survey sample covered 3100 enterprises with at least ten employees. This represents about 22% of the total number of enterprises in Lithuania. Filling out the survey took an average of 69 minutes. It should be noted that the survey covers a wide range of ICT topics, but only those related to cybersecurity are mentioned here [57].

4.6 Poland

Statistics Poland, the Polish Statistics Office, gathers data on several ICT topics, but only a few related to cybersecurity [58]. In its latest publication on ICT use in the enterprise, the following metrics related to cybersecurity were measured: enterprises using artificial intelligence for ICT security purposes and public administration units carrying out information system security audits.

The Supreme Audit Office of Poland has conducted audits in the cybersecurity area, but these have not been published in English, so they are out of reach for the author of this thesis.

4.7 The Czech Republic

The Czech Statistical Office gathers data on many topics, including cybersecurity [59]. The statistics office records the following statistics related to cybersecurity: enterprises in the Czech Republic that experienced ICT-related security incidents, enterprises that experienced unavailability of ICT services, enterprises that experienced destruction or corruption of data, Selected ICT security measures used in enterprises to ensure the security of their ICT systems (for example data backup to a separate location, management of user rights, VPN usage, encryption of data ICT security monitoring systems, multi-factor authentication, biometric authentication). The statistics office gathers the data from a survey conducted among a sample of 8000 enterprises with at least ten employees. The chosen enterprises are also from a variety of industries.

The Czech Supreme Audit Board published an audit in 2020 of the National Cyber and Information Security Agency and the Ministry of Interior. The audit aimed to determine how well these entities had performed their task of implementing the National Cyber Security Strategy of the Czech Republic. The audit was performed through on-site interviews and data gathering but also relied substantially on surveys conducted by NCISA. The statistics board conducted the surveys referenced here over the years 2018 and 2019. The survey aimed to determine the budget polled state agencies have for cybersecurity and the estimated actual budget they need. The author could not find any further information about the survey from other sources [60].

NÚKIB, the National Cyber and Information Security Agency of The Czech Republic, publishes an annual report [61] on the state of cybersecurity in the country. One part of the report is a survey of the country's administrators of essential information systems and critical information infrastructure. According to one of the authors of the report, the survey is carried out among several hundred organisations. It can take 2 - 6 hours to complete, depending on the organisation's size. The survey is central to the report, and results from a given year are compared with previous years for analysis. The survey is also a lot of work for NÚKIB, possibly taking several months to complete for one employee. However, the burden has recently been shared among several employees.

4.8 Summary

This section describes the approaches to cybersecurity capability evaluations of five EU member-states: Finland, Estonia, Latvia, Lithuania, Poland, and the Czech Republic. The most common pattern among the described countries is the presence of official statistics.

The other common practice is one-off reports and audits. The reports can be done by either interested parties from outside the country or inside, but the audits are all done by the officially sanctioned state body. The reports' authors have to rely on public information and interviews, while the officials performing audits have much more power and possibilities for gathering information.

Of the reviewed countries, currently, only Finland provides an official tool for self-assessment to its organisations, and only the Czech Republic performs a yearly evaluation of its critical infrastructure organisations.

Answers to Research Questions To answer **SRQ3**: There are several practices in place on the country level: official statistics gathered by the state statistics authority, and official tools provided by the state. Surveys carried out by state agencies. The statistics offices collect information directly from organisations but do not provide any analysis. The survey conducted by NÚKIB is the only broad periodic effort to evaluate the cybersecurity capabilities of critical infrastructure organisations that the author was able to find. The only available tool that directly helps evaluate the cybersecurity posture of an organisation is the Finnish Cybermeter.

5 Data Aggregation

5.1 Introduction

The following section aims to answer SRQ4: How do data aggregation methods used in cybersecurity capability evaluations consider individual organisations? The most common method for data aggregation for cybersecurity capabilities are cybersecurity indices. Cybersecurity indices measure and compare countries' readiness to face cyber threats and respond to incidents. Currently, several different indices are active around the world. Due to the differences in methodology and sources, a country's ranking may differ significantly in separate indices. This section describes and compares five indices: the National Cyber Security Index (NCSI), the Global Cybersecurity Index (GCI), the National Cyber Power Index (NCPI), the Cyber Defense Index, and the EU Cybersecurity Index. The main aim of the analysis is to determine if and how individual organisations contribute to the score of an entire country.

5.2 National Cyber Security Index

The National Cyber Security Index (NCSI) [62] evaluates and ranks the countries of the world according to their cyber capabilities. The NCSI was created and is managed by the e-Governance Agency[7] in Estonia. One of the more significant differences between this index and others is that it is not published periodically but is updated when new information is made available.

According to experts at the e-Governance Academy, whom the author contacted over email, the data is gathered from three sources: public sources, government officials, or cooperative partners. The first refers to data provided by their team or colleagues (including interns) at the e-Governance Academy. The second one refers to government employees whom their governments have designated to be country contributors. The third term refers to private individuals, civil society organisations or private sector organisations that have been accepted as contributors. The data gathered might differ from contributor to contributor based on how they interpret the criteria of the indicators. Any inconsistencies are mitigated by having two experts review the data and accept or decline based on predetermined criteria.

Figure 2 illustrates the data-gathering process for the NCSI.

As of November 2023, the methodology of the NCSI was updated [63], and scores are being updated and added back into the index monthly. As of February 2024, 31 countries have been reintroduced and aligned with the updated methodology. Of the countries described in Section 4, only Estonia and Latvia are currently present, ranked 3rd and 5th, respectively.

[7] https://ega.ee/

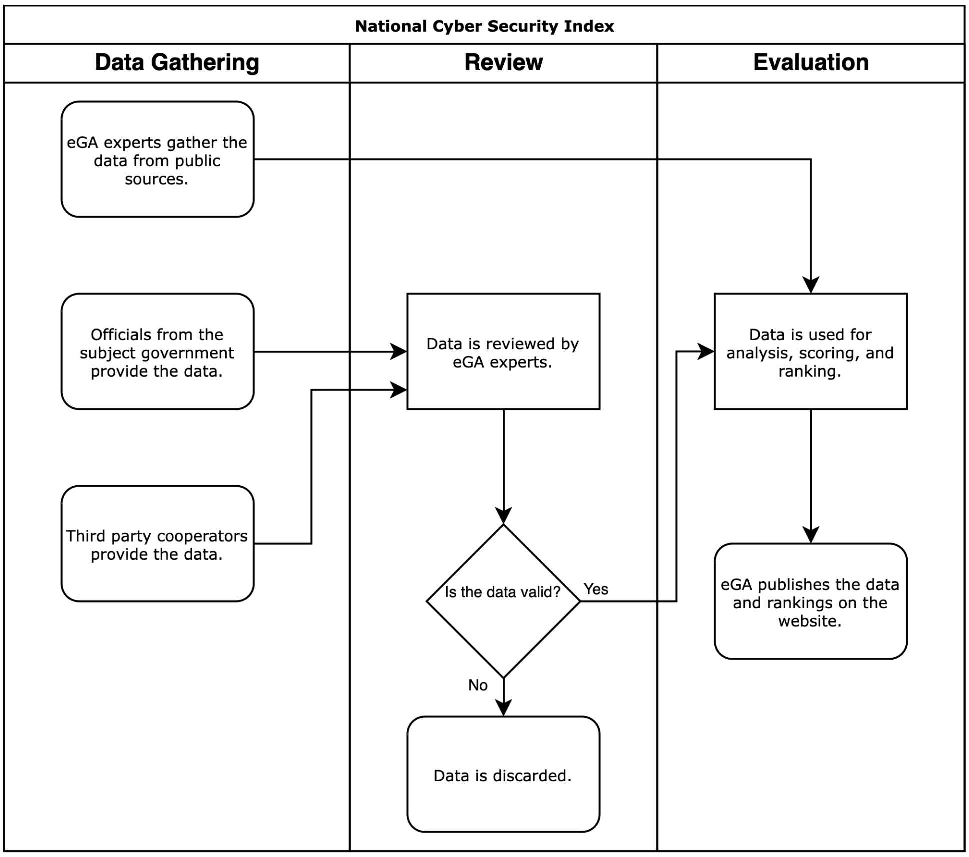

National Cyber Security Index
Data Gathering
Review
Evaluation
eGA experts gather the data from public sources.
Officials from the subject government provide the data.
Third party cooperators provide the data.
Data is reviewed by eGA experts.
Is the data valid?
Yes
No
Data is discarded.
Data is used for analysis, scoring, and ranking.
eGA publishes the data and rankings on the website.

Figure 2. Diagram of the data gathering process of the National Cyber Security Index

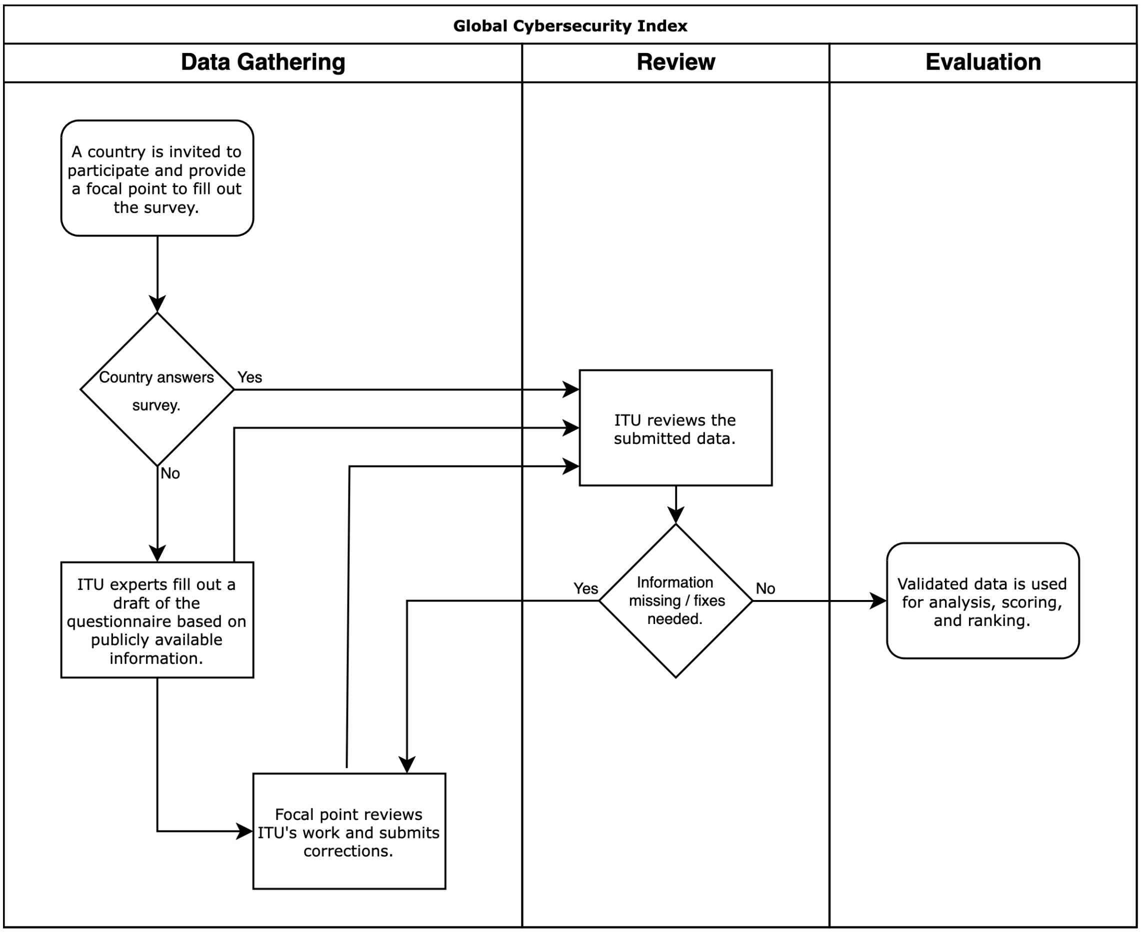
5.3 Global Cybersecurity Index

The Global Cybersecurity Index [64] ranks most of the world's countries on their commitment to cybersecurity and helps them identify areas for improvement. The information presented here is gathered from the methodology document of the Global Cybersecurity Index [65]. The index is composed by the International Telecommunication Union, a United Nations agency specialising in information and communication technologies. The index comprises five pillars: legal, technical, organisational, capacity development, and cooperation.

The data is gathered from a combination of self-assessment by the countries, information available to the public, and expert research. Figure 3 illustrates the data-gathering process.

In 2015, along with the first edition of the GCI, ITU also published a compilation of cybersecurity wellness profiles [25]. They provided a holistic overview of each country's cyber wellness and included the indicators used to compose the index. However, the wellness profiles were discontinued in the subsequent editions.

Figure 3 illustrates the data-gathering process for the GCI.



Global Cybersecurity Index
Data Gathering
Review
Evaluation
A country is invited to participate and provide a focal point to fill out the survey.
Country answers survey.
Yes
No
ITU reviews the submitted data.
ITU experts fill out a draft of the questionnaire based on publicly available information.
Yes
Information missing / fixes needed.
No
Validated data is used for analysis, scoring, and ranking.
Focal point reviews ITU's work and submits corrections.

Figure 3. Diagram of the data gathering process of the Global Cybersecurity Index

5.4 National Cyber Power Index

The National Cyber Power Index ranks countries according to their cyber power capabilities and publishes the top thirty. The index is composed by Harvard University's Belfer Center and was first published in 2020. The information presented here is gathered from the National Cyber Power Index 2020 [66] and 2022 [67] reports. At the centre of the index are eight objectives that a country might have in the cyber realm: amassing and protecting wealth, controlling and manipulating the information environment, defining international cyber norms and technical standards, destroying or disabling an adversary's infrastructure and capabilities, foreign intelligence collection for national security, growing national cyber and commercial technology competence, strengthening and enhancing cyber defences, surveilling and monitoring domestic groups. The objectives are also separately viewed from the angles of capability and intent to fulfil them.

The index is based on publicly available information and thus can suffer from incomplete data. Several of the measured objectives concern offensive and intelligence capabilities on which states generally want to remain as opaque as possible. Especially those states that are more closed to the outside world in general, like Iran and North Korea. The data for the index is gathered from countries' websites, public strategy and policy documents, and comments made by senior government figures. No primary data collection or surveys are done, and no information is gathered on individual organisations.

Of the countries described in Section 4, only Estonia is present in the NCPI, ranked 25th.

5.5 Cyber Defense Index

The Cyber Defence Index [68] ranks the largest twenty economies of the world in their cybersecurity capabilities. A nation's score is given on a scale of 1-10 and is an aggregate of four pillars: critical infrastructure, cybersecurity resources, organisational capacity, and policy commitment. The chosen countries also mostly overlap with G20[8] countries. The index is developed by MIT (Massachusetts Institute of Technology) Technology Review, a media company connected to MIT, and sponsored by Code42[9], a cybersecurity software company. The information presented here is based on the description of the index taken from the official report for 2022/23 [69], which is also the first year the index was published.

The methodology of the Cyber Defense Index states that the data is collected in two ways. Secondary source data is collected from publicly available sources, including other indexes, such as the Global Cybersecurity Index composed by the International Telecommunications Union. Other public sources include popular data aggregators organisations such as the Data Center Map[10] and Worldometer[11]. Primary source data is collected through surveys conducted with around a thousand senior executives from organisations from the ranked countries, with an equal number from each country. The respondents were asked to rate their country's policy and regulations and their own organisation's cybersecurity activities and discuss the priorities for the next few years. The questionnaire and responses are not public and are unavailable to the author. Due to this, the author can't determine how much the survey asks about the organisation's cybersecurity posture and the overall cybersecurity environment in the country. This, in turn, means that the author cannot determine how much of the organisation's perspective makes it into the final data. In determining the score, all of the four pillars of the index take the survey data into account. On the negative side, the report says very little about

[8] https://www.g20.org/en

[9] www.code42.com

[10] www.datacentermap.com

[11] www.worldometer.com

the surveyed organisations themselves. It is not stated if they are public or private, their size, or their area of activity.

5.6 EU Cybersecurity Index

The European Union Cybersecurity Index is a new initiative by ENISA, the EU Agency for Cybersecurity. As of this writing, the index is in the pilot phase and has not yet published its first report. The first report is expected to be published in the summer of 2024. The methodology of the index is also not yet available for review, and the information presented here has been obtained from interviews with a member of the index workgroup.

The EU Cybersecurity Index ranks all the EU member-states. The data for the index is collected through surveys filled out by stakeholders from subject countries. In addition to the survey, ENISA also gathers information from public sources like Eurostat and Eurobarometer. The results of the index help the EU make informed decisions and identify challenges and gaps in its cybersecurity capabilities.

Figure 4 illustrates the data-gathering process for the EU Cybersecurity Index.

5.7 Other Methods

Several private companies worldwide are working on their own cybersecurity index or performing ratings in another way. These companies mainly work in the consultancy field, either as a cybersecurity consultancy [70] or, more widely, as a general business consultancy [71], [72]. But there are also large technology companies that publish reports on the cybersecurity capabilities of their customers like Microsoft [73] and Cisco Systems [74]. Private enterprises and organisations use proprietary methods and data sources to create their ratings and reports. The methodologies and gathered data remain largely unpublished; only a report and its conclusions are available. For example, the methodology section of the aforementioned Data Security Index report published by Microsoft mentions that a survey was conducted to gather data for the whitepaper. Still, the questionnaire and exact results are not available to the reader.

Several companies provide security ratings as a service. For example, BitSight [75] is one such company. BitSight analyses individual organisations like companies, government agencies, and educational institutions. Organisations pay a yearly subscription fee in exchange for their rating and feedback on improvement and risk management. According to official documentation published by the company [76],[77], the data used to calculate the ratings is largely telemetry gathered from the Internet and from partners.

This data includes:

- DNS queries and responses

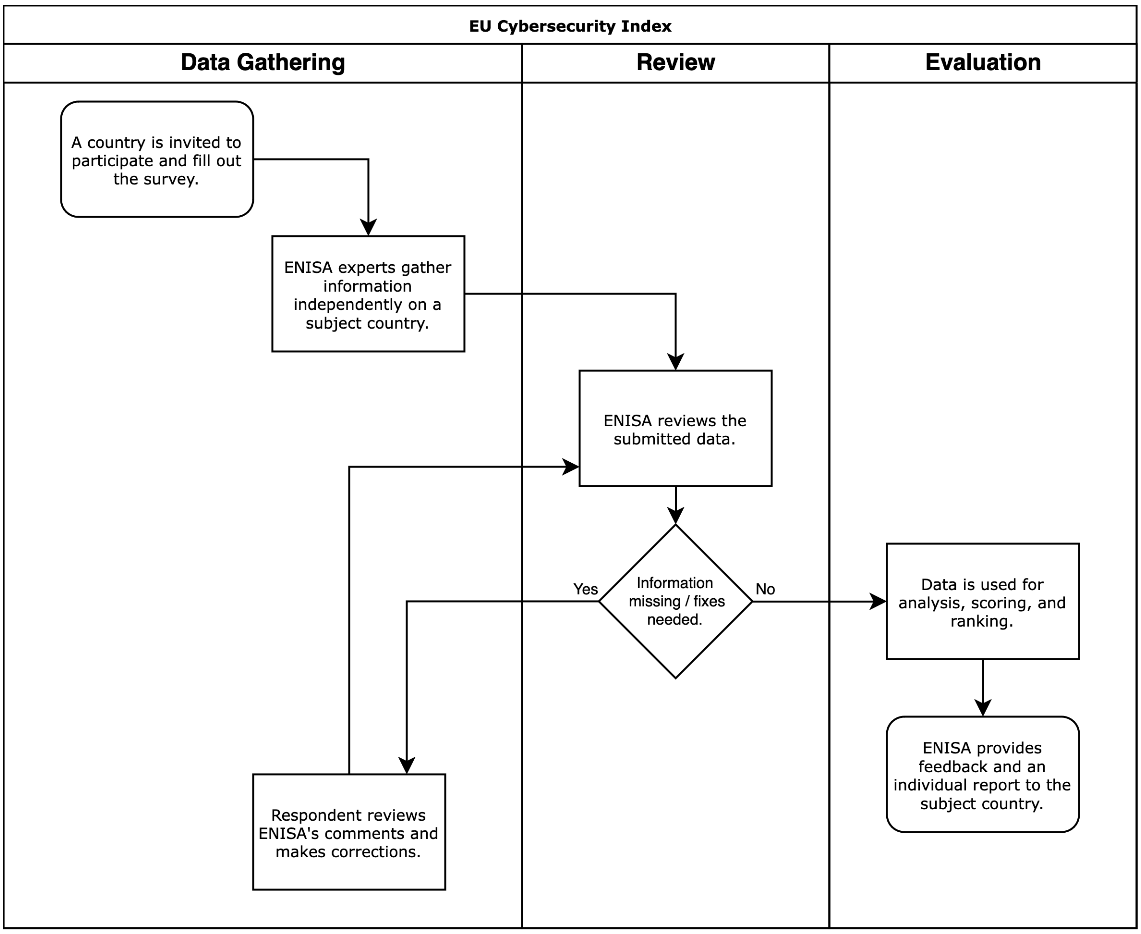

EU Cybersecurity Index
Data Gathering
Review
Evaluation
A country is invited to participate and fill out the survey.
ENISA experts gather information independently on a subject country.
ENISA reviews the submitted data.
Yes
Information missing / fixes needed.
No
Data is used for analysis, scoring, and ranking.
ENISA provides feedback and an individual report to the subject country.
Respondent reviews ENISA's comments and makes corrections.

Figure 4. Diagram of the data gathering process of the ENISA Cybersecurity Index

- Malicious traffic like DDOS attacks
- Attempts at brute force attacks
- Open ports
- Software configuration and versions
- Traffic from IOT devices
- Known vulnerabilities

The exact process and algorithm are proprietary and not public knowledge.

Some companies publish more thorough reports and assessments that might be more valuable to cybersecurity experts in general like the Finnish cybersecurity consultation company Nixu and their annual cybersecurity index [78]. Nixu's index was first published in 2022. The data was gathered through in-person and online interviews. The interviewees were mainly from the Nordic countries (Finland, Sweden, Denmark, and Norway), with 12% of respondents being from other countries. In addition to questions about their organisation's cybersecurity capabilities, the respondents were asked more open-ended questions. For example, what are the topics they feel have been increasing in importance in the past year and what will matter in the coming year?

While these reports may not have the same level of authority and recognition as government or international indices like those by the ITU, they can still provide valuable insights and assessments for decision-making in the cybersecurity domain. Due to their proprietary nature, it is difficult to rely on them for official strategies by governmental decision-makers.

5.8 Summary

In summary, this section describes five cybersecurity indices: the National Cyber Security Index, the Global Cybersecurity Index, the National Cyber Power Index, the Cyber Defense Index, and the EU Cybersecurity Index. The data-gathering practices of the indices involve several sources that can be divided into three categories: surveys, public sources, and evidence provided by the subject. With the exception of the National Cyber Power Index, which relies exclusively on public data, the indices use a combination of sources. Table 5 compares the indices and their data-gathering practices. The column headers are explained as follows:

- **organisation** is the organisation's name that manages the index.
- **Published Since** is the year the first edition of the index was published.
- **Publishing Period** is the period after which a new ranking is published.
- **Iterations** is how many rankings have been published.
- **Updating Cycle** is the period the methodology of the index is updated.
- **Subjects** are the ranked countries.
- **Survey** indicates if one of the data-gathering instruments is a survey.
- **Public Sources** indicates if data is gathered from public sources.
- **Individual Organisations** indicates if data from individual organisations is reflected in the index.

- **Time Investment for Subject** indicates how much time the survey or information gathering takes for the respondents.
- **Feedback for Subject** indicates if the respondents receive anything back.
- **Number of Questions** indicates how many questions there are on the questionnaire.
- **Answers Scale** indicates the answer scales of the questionnaire questions.

Some patterns emerge from the table. The updating cycle of the methodologies of the indices is varied. The NCSI does not have a set update schedule, but this is due to its rolling nature. It is worth noting that the methodology was only recently updated, and countries are currently slowly being added back in. The EU Cybersecurity Index and CDI probably do not have a schedule because they are very new and are still figuring out their processes.

All of the indices rely on public sources for information in one way or another. The NCSI and NCPI rely only on public information, while the other indices also collect data from surveys. The public information includes legislation, official government announcements and the existence of certain agencies in the country. This approach is probably due to the high level of abstraction that evaluating large entities requires. This is perhaps the reason why data on individual organisations seemingly do not propagate up to the index level. Evaluating the cybersecurity posture of an entire country by assessing its numerous individual organisations is too resource-intensive.

Answers to Research Questions To answer **SRQ4**: The methods described here use public sources and surveys as data-gathering tools. With the exception of the Cyber Defense Index, the experience of individual organisations in a country does not directly figure in the indices. The Cyber Defense Index surveys organisations from subject countries. Still, the survey contents are not publicly available, which means that the answer remains ambiguous.

This section concludes the three sections describing the different approaches to cybersecurity capability evaluations on different levels. The following section will discuss the findings and emerging patterns in the preceding research.

Table 2. Cybersecurity Indices. ’—’ means that no information is provided. ’●’ means ’Yes’. ○ means ’No’. ’N/A’ means that the row is not applicable to the given index.

	National Cyber Security Index	Global Cyber Security Index	National Cyber Power Index	Cyber Defense Index	EU Cybersecurity Index
Organisation	e-Governance Academy	International Telecommunications Union	Harvard University’s Belfast Center	MIT Technology Review	ENISA
Published Since	2016	2014	2020	2023	2024
Publishing Period	Rolling	—	—	—	—
Iterations	3	4	2	1	1
Updating Cycle	—	Updated with each iteration	Updated with each iteration	—	—
Subjects	All the countries of the world	United Nations member states plus the state of Palestine	40 countries	G20 countries, excluding Russia and including Poland	EU member states
Survey	○	●	○	●	●
Public Sources	●	●	●	●	●
Individual Organisations	○	○	○	●	○
Time Investment For Subject	—	—	○	—	—
Feedback For Subject	No immediate feedback	—	No immediate feedback	No immediate feedback	Personalised report
Number of Questions	N/A	83	N/A	—	174
Answer Scale	N/A	Ternary (yes, partial, no)	N/A	—	Varies

6 Validation

In sections 3, 4, and 5, the author described the various methods and practices that have been proposed or used to perform cybersecurity capability evaluations. The author described the current state on three levels: scientific literature on the organisational level, country-level practices by the example of five EU member-states, and cybersecurity indices that simultaneously aggregate data on many countries. This section describes the validation process and the observations from analysing the methods and practices from the previous three sections. The author considers the observations from the perspective of possible issues and limitations. As the main focus of the thesis is on the individual organisation, this section also looks at the described methods mainly from that perspective.

Validation of the findings in this thesis was done through two expert interviews with stakeholders from Estonia and the Czech Republic. The experts were chosen based on their knowledge and experience in cybersecurity capability evaluations among organisations and their familiarity with related issues. The expert from Estonia is the cyber risk management leader at the Estonian Ministry of Economic Affairs and Communication. The other is the author of the yearly report on the state of cybersecurity in the Czech Republic [61] at the National Cyber and Information Security Agency of the Czech Republic (abbreviated as NÚKIB in Czech). The report is more closely described in Section 4.

The interview with the Estonian expert was conducted in a semi-formal fashion. The talking points revolved around the current experience governmental agencies have with cybersecurity capability evaluations and the requirements for any future methods. The interview with the Czech expert was a formal interview conducted over email. The questions were about the survey NÚKIB conducts among the critical infrastructure organisations in the Czech Republic every year for the aforementioned report. The questions used as the basis of both interviews can be found in Appendix 1.

The validation process aimed to provide reflection on the author's findings and to help identify commonalities and disparities between the described literature and other methods and the interviewees' experiences.

Organisational Demands Recurring throughout emphasises the importance of providing organisations with a minimally disruptive evaluation process. Of the methods described in Section 3, two of the described methods [31], [30] explicitly bring out the need for time efficiency and comfort as key motivators for their creation. In an interview, the cyber risk management leader at the Estonian Ministry of Economic Affairs and Communication reflected similar sentiments by highlighting the critical aspect of time commitment in evaluations. She emphasised that the time commitment extends beyond just filling out the survey, encompassing preparatory work to provide accurate responses and subsequent time investments in result analysis. Furthermore, the interviewee observed that surveys perceived as burdensome by participating organisations might be hastily completed without due consideration, a phenomenon known as survey fatigue [79]. This can cause issues with the integrity of the provided data. Recognised as a known issue with surveys as a data-gathering tool, it emphasises the importance of creating evaluation methods that lessen the strain on organisations. NÚKIB, however, does not explicitly track the time it takes for respondents to fill out the survey, saying only that it can take anywhere from two to six hours, depending on the size of the organisation. Only one of the methods described in Section 3 included the average time to complete the survey. Furthermore, none of the methods discussed in Sections 4 and 5 included any information on probable time investment for subjects.

Additionally, little is discussed about organisations' fears about sharing sensitive data, which information on their cybersecurity capabilities definitely is.

Real-world Application The common issue with the methods covered in Section 3 is that only one [22] of them has seen real-world application beyond the initial validation done as part of the study. Furthermore, the reader can implement only a few of the methods using the information provided. Most notably, none include the survey questionnaire used to validate the methods. This severely limits the applicability of the proposed methods. Additionally, none of the methods describe any tools to help with the evaluation process, either conducting the survey or analysing the results. In the case of one method [24], it can be seen from the figures in the paper that an Excel spreadsheet was used to gather the answers.

Evolving Threat Landscape The cybersecurity threat landscape is dynamic, and new threats and technologies are continuously emerging. This means that evaluation methods must also be updated to consider changing circumstances. According to NÚKIB, the survey questions have evolved since they began the survey. Seeba et al. have recognised this issue and addressed it with their MUSE [38] tool. Of the other methods reviewed in this thesis, only the cybersecurity indices explicitly stated that methodology is reviewed periodically to ensure the measures are relevant.

Furthermore, single evaluation results are not very useful in a vacuum. Good cybersecurity is not a one-time effort, and making sure weak points are addressed needs periodic evaluations and analysis.

Data Gathering for Aggregation Three main data-gathering methods for cybersecurity capability assessments can be differentiated based on the methods reviewed in Section 4 and5. These methods are surveys, analysis of public records, or a combination of the two. Public records usually mean legislation and official government statements. The existence of specific institutions in a given country can also be used to assess the state of cybersecurity. If a country implements a CERT as an institution, some thought has probably been put into cyber issues. For example, in Estonia, the CERT-EE constantly monitors cyberspace as one of its duties. CERT-EE provides daily updates on significant events and incidents [80], and without it, there would not be anyone to provide this service. Surveys usually mean questionnaires answered over the Internet or interviews in person. Depending on the focus, scope, and resources available, the number of respondents can vary from a few to several hundred.

Bottom-Up or Top-Down Expanding on the previous point, resource constraints affect not only the subjects of the evaluations but also the ones performing them. Similarly, performing an evaluation takes time to prepare and analyse the results. NÚKIB states that in previous years, it has taken several months for a single person to gather and analyse the results of the survey for *"several hundred participants"*. Now, they have begun to spread out the responsibility among several people to ease the workload and *"eliminate quite a critical single point of failure"*. On the other hand, Estonia lacks experience in conducting extensive surveys on organisations. In the case of data aggregation, this issue is mitigated by choosing a top-down approach instead of a bottom-up one. Top-down means to make generalisations based on the country's environment to determine its cybersecurity capabilities. For example, the National Cyber Security Index [62] uses legislation and policy, among other metrics, but does not use the experience of individual organisations. Bottom-up means evaluating the respective organisations in a country to make generalisations about the country's overall capability. Like the method proposed by Jazri et al. [24]. This creates a problem where increasing abstraction causes the cybersecurity capabilities of the grassroots level to get lost in the bigger picture.

Country Perspective All countries reviewed in Section 4 have a cybersecurity strategy in place, meaning they all have developmental goals. The strategies include a short section on how reporting on the progress should be done. Generally, once a year, stakeholders from all areas report to the person in charge of cybersecurity on a state level, who in turn reports to the appropriate ministry. For example, the current strategies for both Estonia [81] and Poland [82] follow this pattern. From this, it could be assumed that a periodic monitoring and evaluation practice is in place. Still, there is no further elaboration on how exactly this is done.

Another issue for governments is data gathering and analysis. This was highlighted by the audit conducted in Latvia [55], the cyber risk management leader at the Estonian Ministry of Economic Affairs and Communication, and also brought out as one of the motivations for creating the Cybermetre by the National Cybersecurity Centre of Finland [40]. There are currently no reasonable solutions for a central authority to gather data from many organisations. Furthermore, no solution would ensure that the collected data is comparable and can be used for analysis.

Of the countries analysed, only Czechia has a process in place to periodically evaluate critical infrastructure organisations in their country. NUKIB concedes that this is a resource-intensive undertaking, taking several months to complete.

7 Conclusion

In conclusion, this thesis describes the various approaches to cybersecurity capability evaluations currently proposed in the scientific literature, both as methods and independent evaluations. Furthermore, to get a more comprehensive view of current practices, state-level experiences and cybersecurity indices are also explored. The thesis aims to analyse the perspective of individual organisations in the context of these methods.

Answers to The Research Questions The primary research question (**PRQ**): What are the limitations of presently proposed methods and practices of cybersecurity capability evaluations on organisations?

> **Answer**: The limitations the author discovered are described in Section 6.

Answers to the subquestions:

- **SRQ1**: What methods have been proposed in the scientific literature for conducting cybersecurity capability evaluations on organisations?

  > **Answer**: Section 3.2 provides an overview of the methods currently proposed in the scientific literature.

- **SRQ2**: What methods have been employed for one-time capability evaluations on organisations in the scientific literature?

  > **Answer**: Section 3.3 provides an overview of the methods used for one-time evaluations in the scientific literature.

- **SRQ3**: What are the practices employed at the country level for cybersecurity capability evaluations?

  > **Answer**: Section 4 provides an overview of the methods currently proposed on the country level.

- **SRQ4**: How do data aggregation methods used in cybersecurity capability evaluations consider individual organisations?

Answer: Section 5 provides an overview of the methods used for data aggregation and their consideration of individual organisations.

Several gaps were identified during the analysis:

Future Work The issues discussed in Section 6 reveal several directions for future research.

- How to lessen the time commitment for organisations participating in cybersecurity capability evaluations?
- What are the possibilities for automating cybersecurity capability evaluations?
- What methods could be employed to perform evaluations on many organisations in parallel and bring the results together for analysis?

Suggestions for Method Developers Finally, some suggestions can be gathered from the previous discussion for developers and owners of future methods:

- Consider the organisation's perspective and the strain the evaluation might put on them.
- Consider how the method can be updated to ensure the timeliness of questions and results.
- Consider how updating the method affects the comparability of results.
- Consider the feedback the organisation gets. Does it motivate the organisation to participate in the evaluation sincerely?

References

[1] European Parliament, "The nis2 directive: A high common level of cybersecurity in the eu." https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf. Accessed: 2023-11-15.

[2] "Directive (eu) 2016/1148 of the european parliament and of the council of 6 july 2016 concerning measures for a high common level of security of network and information systems across the union." http://data.europa.eu/eli/dir/2016/1148/oj, 2022.

[3] "Directive (eu) 2022/2555 of the european parliament and of the council of 14 december 2022 on measures for a high common level of cybersecurity across the union, amending regulation (eu) no 910/2014 and directive (eu) 2018/1972, and repealing directive (eu) 2016/1148 (nis 2 directive) (text with eea relevance)." https://eur-lex.europa.eu/eli/dir/2022/2555, 2022.

[4] Information System Authority of the Republic of Estonia, "Cyber security in estonia 2023." https://www.ria.ee/en/media/3760/download. Accessed: 2024-03-01.

[5] Estonian Public Broadcasting, "10,000 people's data stolen in genetic testing company asper biogene leak." https://news.err.ee/1609194952/10-000-people-s-data-stolen-in-genetic-testing-company-asper-biogene-leak. Accessed: 2024-03-01.

[6] J. VanHoy, "Third party risk management," *Available at SSRN 3763399*, 2021.

[7] R. Leszczyna, "Review of cybersecurity assessment methods: Applicability perspective," *Computers & Security*, vol. 108, p. 102376, 2021.

[8] J. Gavenaite-Sirvydiene and A. Miecinskiene, "The assessment of cyber security's significance in the financial sector of lithuania," *Journal of Cyber Security and Mobility*, pp. 497–518, 2023.

[9] M. Bada and C. Weisser Harris, "Cybersecurity capacity review republic of lithuania," 2017.

[10] S. Pfleeger and R. Cunningham, "Why measuring security is hard," *IEEE Security & Privacy*, vol. 8, no. 4, pp. 46–54, 2010.

[11] W. Huitt, "Assessment, measurement, and evaluation: Overview," *Educational Psychology Interactive*, 2007.

[12] M. Seeba, S. Mäses, and R. Matulevičius, "Method for evaluating information security level in organisations," in *International Conference on Research Challenges in Information Science*, pp. 644–652, Springer, 2022.

[13] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," vol. 2, 01 2007.

[14] Ministry of Foreign Affairs of the Czech Republic, "Official name of the country extended by its short form 'czechia'." `https://mzv.gov.cz/athens/en/about_the_embassy/official_name_of_the_country_extended_by.html`. Accessed: 2023-12-12.

[15] NYU Tandon School of Engineering, "The index of cybersecurity." `https://wp.nyu.edu/awm1/`. Accessed: 2023-02-12.

[16] OECD, "Oecd better life index." `https://www.oecdbetterlifeindex.org/`. Accessed: 2024-02-12.

[17] V. Kravets, "Comparative analysis of the cybersecurity indices and their applications," *Theoretical and Applied Cybersecurity*, vol. 1, no. 1, 2019.

[18] H. Çifci, "Comparison of national-level cybersecurity and cyber power indices: A conceptual framework," 2022.

[19] P. Sharikov, "Contemporary cybersecurity challenges," in *The Implications of Emerging Technologies in the Euro-Atlantic Space: Views from the Younger Generation Leaders Network*, pp. 143–157, Springer, 2023.

[20] J. Limnéll and K. Geers, "Northern european cyber security in light of the ukraine war," *NATO CCD COE Publications, Tallinn*, pp. 145–151, 2015.

[21] Y. You, I. Cho, and K. Lee, "An advanced approach to security measurement system," *The Journal of Supercomputing*, vol. 72, pp. 3443–3454, 2016.

[22] I. Bernik and K. Prislan, "Measuring information security performance with 10 by 10 model for holistic state evaluation," *PloS one*, vol. 11, no. 9, p. e0163050, 2016.

[23] K. Prislan, A. Mihelič, and I. Bernik, "A real-world information security performance assessment using a multidimensional socio-technical approach," *PloS one*, vol. 15, no. 9, p. e0238739, 2020.

[24] H. Jazri, O. Zakaria, and E. Chikohora, "Measuring cybersecurity wellness index of critical organisations," in *2018 IST-Africa Week Conference (IST-Africa)*, pp. Page–1, IEEE, 2018.

[25] International Telecommunications Union, "Global cybersecurity index cyberwellness profiles." https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf, 2015.

[26] M. Seeba, T. Oja, M. P. Murumaa, and V. Stupka, "Security level evaluation with f4sle," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, pp. 1–8, 2023.

[27] Y. Maleh, A. Ezzati, A. Sahid, and M. Belaissaoui, "Towards a capability assessment framework for information security governance in organization," *Journal of Information Assurance and Security*, vol. 12, no. 21, pp. 209–217, 2017.

[28] J. Goode, Y. Levy, A. Hovav, and J. Smith, "Expert assessment of organizational cybersecurity programs and development of vignettes to measure cybersecurity countermeasures awareness," *Online Journal of Applied Knowledge Management (OJAKM)*, vol. 6, no. 1, pp. 54–66, 2018.

[29] A. Rae and A. Patel, "Defining a new composite cybersecurity rating scheme for smes in the uk," in *International Conference on Information Security Practice and Experience*, pp. 362–380, Springer, 2019.

[30] S. Malaivongs, S. Kiattisin, and P. Chatjuthamard, "Cyber trust index: A framework for rating and improving cybersecurity performance," *Applied Sciences*, vol. 12, no. 21, p. 11174, 2022.

[31] W. Qiangmin, L. Mengquan, and L. Jianhua, "Method on network information system security assessment based on rough set," in *2007 Third International IEEE Conference on Signal-Image Technologies and Internet-Based System*, pp. 1041–1046, IEEE, 2007.

[32] E. K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, and B. Klepacki, "Information security assessment in public administration," *Computers & Security*, vol. 90, p. 101709, 2020.

[33] A. Chodakowska, S. Kańduła, and J. Przybylska, "Cybersecurity in the local government sector in poland: More work needs to be done," *Lex localis-journal of local self-government*, vol. 20, no. 1, pp. 161–192, 2022.

[34] C.-L. Hwang, K. Yoon, C.-L. Hwang, and K. Yoon, "Methods for multiple attribute decision making," *Multiple attribute decision making: methods and applications a state-of-the-art survey*, pp. 58–191, 1981.

[35] The Global Cyber Security Capacity Centre, "The cmm." https://gcscc.ox.ac.uk/the-cmm. Accessed: 2024-02-18.

[36] M. Lehto and J. Limnéll, “Strategic leadership in cyber security, case finland,” *Information Security Journal: A Global Perspective*, vol. 30, no. 3, pp. 139–148, 2021.

[37] E. Wong, N. Porter, M. Hokanson, and B. B. Xie, “Benchmarking estonia’s cyber security: An on-ramping methodology for rapid adoption and implementation,” 2017.

[38] M. Seeba, A.-a. O. Affia, S. Mäses, and R. Matulevičius, “Create your own MUSE: A method for updating security level evaluation instruments,” *Computer Standards & Interfaces*, vol. 87, p. 103776, 2024.

[39] Finnsh Government, “Report: Finland’s cyber security must be developed systematically – cooperation of the authorities and processes require further improvement.” https://valtioneuvosto.fi/en/-/1410869/report-finland-s-cyber-security-must-be-developed-systematically-cooperation-of- Accessed: 2024-02-13.

[40] Finnsh Transport and Communication Agency National Cyber Security Centre, “Cybermeter.” https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari. Accessed: 2024-02-13.

[41] NCSC-FI, “Cybermeter: National framework for the assessment of cybersecurity capabilites.” https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_Cybermeter_User_Guide_V1.pdf. Accessed: 2023-12-07.

[42] Statistics Finland, “Official statistics of finland (osf): Use of information technology in enterprises.” https://stat.fi/en/statistics/icte. Accessed: 2023-12-14.

[43] Center for Security Studies (CSS), ETH Zürich, “Estonia’s national cybersecurity and cyberdefense posture.” t. Accessed: 2023-12-14.

[44] Center for Security Studies (CSS), ETH Zürich, “Japan’s national cybersecurity and cyberdefense posture.” https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-08-Japans-national-cybersecurity-defense-posture.pdf. Accessed: 2023-12-14.

[45] Center for Security Studies (CSS), ETH Zürich, “Romania’s national cybersecurity and cyberdefense posture.” https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-10-Romania.pdf. Accessed: 2023-12-14.

[46] National Audit Office of Estonia, "Riigikontroll." https://www.riigikontroll.ee/Avaleht/tabid/36/language/en-US/Default.aspx. Accessed: 2024-02-13.

[47] National Audit Office of Estonia, "Administration and reliability of X-road." https://www.riigikontroll.ee/DesktopModules/DigiDetail/FileDownloader.aspx?FileId=14778&AuditId=2520. Accessed: 2023-12-15.

[48] National Audit Office of Estonia, "Guaranteeing security and preservation of critical state databases of estonia." https://www.riigikontroll.ee/DesktopModules/DigiDetail/FileDownloader.aspx?FileId=14218&AuditId=2462. Accessed: 2023-12-15.

[49] National Audit Office of Estonia, "Implementation of system of IT security measures in local governments." https://www.riigikontroll.ee/DesktopModules/DigiDetail/FileDownloader.aspx?FileId=14270&AuditId=2466. Accessed: 2023-12-15.

[50] Statistics Estonia, "It147: ICT security in enterprises using robots by economic activity and numbers or persons employed." https://andmed.stat.ee/en/stat/majandus__infotehnoloogia__infotehnoloogia-ettevettes/IT147. Accessed: 2023-12-14.

[51] Statistics Estonia, "Community survey on ICT usage and e-commerce in enterprises." https://www.stat.ee/en/find-statistics/methodology-and-quality/esms-metadata/20505. Accessed: 2023-12-14.

[52] Central Statistics Bureau of Latvia, "Enterprises that provide employees with information on ICT security requirements." https://stat.gov.lv/en/statistics-themes/information-technologies/ict-enterprises/tables/epd050-enterprises-provide, 2022. Accessed: 2023-11-01.

[53] Central Statistics Bureau of Latvia, "Ict specialists in enterprises." https://stat.gov.lv/en/statistics-themes/information-technologies/ict-enterprises/tables/epd010-ict-specialists, 2022. Accessed: 2023-11-01.

[54] Central Statistics Bureau of Latvia, "Individuals who experienced security related incidents through using the internet." https://stat.gov.lv/en/statistics-themes/information-technologies/ict-houeseholds/tables/epi010-individuals-who, 2019. Accessed: 2023-11-01.

[55] T. S. A. O. of the Republic of Latvia, “Can we rely on the access to information systems and the receipt of e-services?.” https://www.lrvk.gov.lv/en/getrevisionfile/29525-5Aio6j7MwYsuSG4nKlzFVmCMG0JZircA.pdf, 2022.

[56] National Audit Office of Lithuania, “The cyber security environment in lithuania.” https://www.valstybeskontrole.lt/EN/Product/Download/3366. Accessed: 2024-02-13.

[57] Statistics Lithuania, “Information society in figures - 2023.” https://osp.stat.gov.lt/en_GB/informacines-technologijos. Accessed: 2023-12-12.

[58] Statistics Poland, “Information society in poland - 2023.” https://stat.gov.pl/download/gfx/portalinformacyjny/en/defaultaktualnosci/3417/1/10/1/information_society_in_poland_in_2023.pdf. Accessed: 2023-12-14.

[59] The Czech Statistical Office, “Information society in figures - 2023.” https://www.czso.cz/documents/10180/191186765/06100523.pdf/61bee3a3-1e67-4aad-91eb-0e5c4146493e?version=1.3. Accessed: 2023-12-12.

[60] Czech Republic Supreme Audit Office, “Building the national cyber security of the czech republic.” https://nku.cz/assets/kon-zavery/K19026_en.pdf, 2020.

[61] National Cyber and Information Security Agency of the Czech Republic, “2022 report on the state of cybersecurity in the czech republic.” https://nukib.gov.cz/download/publications_en/2022_Report_on_the_State_of_Cybersecurity_in_the_Czech_Republic.pdf. Accessed: 2023-11-08.

[62] e-Governance Academy, “National cyber security index.” https://ncsi.ega.ee/. Accessed: 2024-02-12.

[63] e-Governance Academy, “Ncsi methodology updated - first countries introduced.” https://ncsi.ega.ee/99/ncsi-methodology-updated-first-countries-introduced/. Accessed: 2024-02-12.

[64] International Telecommunications Index, “Global cybersecurity index.” https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. Accessed: 2024-02-12.

[65] International Telecommunication Union, “Global cybersecurity index 2020.” https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx, 2020.

[66] University of Harvard Belfer Center, “National cyber power index 2020.” https://www.belfercenter.org/publication/national-cyber-power-index-2022, 2020.

[67] J. Voo, I. Hemani, and D. Cassidy, “National cyber power index 2022,” tech. rep., University of Harvard Belfer Center, 2022.

[68] MIT Technology Review Insights, “Cyber defense index.” https://www.technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23/. Accessed: 2024-02-12.

[69] I. T. R. Insights, “The cyber defense index: A benchmark of the digital security preparedness of enterprises across the threat landscapes of the world’s top economies.” https://www.technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23/, 2022.

[70] Bridewell, “Cyber security consultancy.” https://www.bridewell.com/cyber-security-consultancy. Accessed: 2024-02-12.

[71] KPMG, “Cyber security services.” https://kpmg.com/xx/en/home/services/advisory/risk-consulting/cyber-security-services.html. Accessed: 2024-02-12.

[72] KPMG, “Global cyber solutions.” https://www.deloitte.com/global/en/services/risk-advisory/services/cyber-risk.html. Accessed: 2024-02-12.

[73] Microsoft, “Microsoft data security index.” https://www.microsoft.com/en-us/security/blog/2023/10/25/top-insights-and-best-practices-from-the-new-microsoft-data-security-index-repor
Accessed: 2024-02-12.

[74] Cisco Systems, Inc., “Cybersecurity readiness index.” https://www.cisco.com/c/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index.html. Accessed: 2024-02-12.

[75] Bitsight, “Cyber risk management solutions.” https://www.bitsight.com/. Accessed: 2024-02-12.

[76] BitSight, “What is a security rating?.” https://www.bitsight.com/blog/what-is-a-security-rating. Accessed: 2023-11-02.

[77] BitSight, “How bitsight calculates security ratings.” https://www.bitsight.com/sites/default/files/2023-04/How%20Bitsight%20Calculates%20Security%20Ratings.pdf. Accessed: 2023-11-02.

[78] "Cybersecurity index report 2023," tech. rep., Nixu, 2023.

[79] A. Field, "Survey fatigue and the tragedy of the commons: Are we undermining our evaluation practice," *Evaluation Matters—He Take Tō Te Aromatawai*, vol. 6, pp. 1–11, 2020.

[80] Information System Authority of the Republic of Estonia, "Situation in the cyberspace." https://www.ria.ee/en/cyber-security/cyberspace-analysis-and-prevention/situation-cyberspace. Accessed: 2024-03-01.

[81] The Ministry of Economic Affairs and Communications of Estonia, "Cybersecurity strategy 2019 - 2022." https://www.mkm.ee/media/703/download. Accessed: 2024-02-13.

[82] The Ministry of Digital Affairs, "Cybersecurity strategy of the republic of poland for 2019 - 2024." https://www.gov.pl/attachment/6a4aafc6-e339-4cd5-a8e6-cd47257f02d8. Accessed: 2024-02-13.

Appendix

I. Interview Questions

The in-person conversation with the cyber risk management leader at the Estonian Ministry of Economic Affairs and Communication revolved mainly around the following questions:

- What cybersecurity evaluation methods are currently in place?
- What is the purpose of the currently in place cybersecurity evaluation methods?
- What are the requirements for any future cybersecurity evaluation methods?

The interview with the author of the yearly survey at NÚKIB was conducted over email and thus was more structured. The questions were mainly about the survey that is a part of the yearly report:

- How important is the survey in the context of the annual report? How much do the results of the report depend on the survey?
- Do the organisations participating in the survey receive anything back for answering the survey (e.g. results, individual report, feedback, statistics, recommendations)?
- How much time does an organisation take on average to complete the survey?
- Are the results from different years comparable with each other? Do you use the data to analyse how things have changed over the years?
- Are there any notable issues you are currently facing with conducting the survey?
- Have you made any significant changes to how you conduct the survey since you first began?
- A wider question. Do you know the general situation regarding cybersecurity capability assessments in Czechia? Are any other such surveys being conducted among organisations, or are any other approaches implemented?
- Do the results of the survey also shape policies in some way? Or, are the results presented to decision-makers who then consider them when making future policy decisions?

II. Licence

Non-exclusive licence to reproduce thesis and make thesis public

I, **Magnus Valgre**,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

   reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   Evaluating Cybersecurity Capabilities: Organisations' Perspective,

   supervised by Mari Seeba.

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Magnus Valgre
07/03/2024