TALLINN UNIVERSITY OF TECHNOLOGY
Faculty of Information Technologies

Alex Bindevald 182497IVCM

Cyber Security at Schools - Challenges, Opportunities and Needs for CTF-Solution

Master's thesis

Supervisor: Birgy Lorenz
PhD

Tallinn 2021

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Alex Bindevald

21.04.2021

Abstract

This study was aimed at teaching cybersecurity in general education. The goals of this study were to find out about what and how is cyber defence taught in general education schools and what kind of extracurricular activities are available for students to learn cyber defence. In addition, the author was curious if cyber defence is possible to be taught with Capture The Flag (CTF) environment and which kind of environment would schools need. To find out if the there is a need for CTF environment, the author needed to get answers on what options there are for creating and using CTF environments and what are school's needs for using such an environment. To reach the goal of this study, the author conducted a survey and interviews with teachers. In addition, data was gathered about extracurricular activities from students in the context of CyberDrill competition. The data gathered from theory and from teacher's study showed that there is a need for CTF environment, but the teachers do not have the skills nor time to set up it. The study showed that currently there is a curriculum for teaching cybersecurity in basic and high school, but since the schools have big autonomy of what they want to teach in their schools, only a few of the schools are teaching it actively. Besides formal education, the students can acquire cybersecurity-related skills from summer camps, training environments and cybersecurity competitions. The study provides information on the needs for creating a CTF environment and recommendations are given to using CTF environments for different focus groups.

This thesis is written in English and is 59 pages long, including 8 chapters, 10 figures and 3 tables.

Annotatsioon

Küberturvalisus koolides - väljakutsed, võimalused ja vajadused CTF-lahenduse järele

Käesolev magistritöö oli suunatud küberturvalisuse õpetamisele üldhariduskoolides. Lõputöö eesmärkideks oli välja selgitada, mida ja kuidas õpetatakse küberkaitse raames üldhariduskoolides ning milliseid õppekaväliseid tegevusi saavad õpilased küberkaitse õppimiseks kasutada. Lisaks oli autoril huvi, kas küberkaitset on võimalik õpetada *Capture The Flag* (CTF) keskkonnaga ja missugust CTF keskkonda koolid vajaksid. Et teada saada, kas koolides on vaja CTF-keskkonda, pidi autor saama vastused selle kohta, milliseid võimalusi on CTF-i keskkonna loomiseks ja kasutamiseks ning millised on koolide vajadused sellise keskkonna kasutamiseks. Selle eesmärgi saavutamiseks viis autor läbi küsitluse ja intervjuu koos õpetajatega. Lisaks kogus autor õpilastelt andmeid õppekavaväliste tegevuste kohta CyberDrilli võistluse kontekstis. Teooriast ja õpetajate seas läbiviidud uuringust kogutud andmed näitasid, et CTF-i keskkond on vajalik, kuid õpetajatel pole oskusi ega aega sellise keskkonna ülesseadmiseks. Uuring näitas, et hetkel on küberturvalisuse õpetamiseks olemas õppekava põhi- ja keskkoolis, aga kuna koolidel on suur autonoomsus, mida nad koolis õpetavad, õpetavad seetõttu vähesed koolid seda aktiivselt. Ametliku hariduse kõrvalt saab õpilane küberturvalisusega seotud oskusi omandada suvelaagritest, treeningkeskkondadest ja küberturvalisuse võistlustelt. Uuringus esitatakse vajadused CTF-keskkonna loomiseks ja antakse soovitused erinevatele fookusgruppidele.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 59 leheküljel, 8 peatükki, 10 joonist, 3 tabelit.

List of abbreviations and terms

CTF	Capture The Flag
RQ	Research question
IT	Information Technology
UT	University of Tartu
Taltech	Tallinn University of Technology
NICE	National Initiative for Cybersecurity Education
ENISA	European Union Agency for Network and Information Security
EU	European Union
WiFi	Wireless Fidelity
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

Table of contents

List of figures

List of tables

1 Introduction

Cybersecurity can be learned in many ways, but when you are younger (for example age 10-16) more gamified possibilities are preferred [1]. In Estonian basic schools, people usually talk and develop student’s common digital literacy including digital safety skills in the informatics subject. The informatics subject is not mandatory for the basic and high schools [2]. In Estonia, digital safety is taught mostly with extracurricular activities (for example the program Smart on the Net) [3]. In 2017, a cyber defence syllabus was created, together with cyber defence materials for high schools, which teaches how to be a good citizen [4]. In the teaching of informatics in high school, students get an overview of what the discipline of informatics means to a university, but in cyber defence, such information is not received because it is not obligatory. Students' understanding of the cybersecurity topics are too low to choose it consciously at the bachelor's level, which often leads choosing cybersecurity career later. At the moment, there is an opportunity to study cyber defence at the university level in TalTech Bachelors program at IT Kolledz [5] or TalTech and UT joint program in Master’s level [6]. At the same time, some young students are eager to learn cybersecurity-related topics and they do it by participating in extracurricular activities. Cybersecurity can mostly be learned in university, official training, or at one’s workplace.

In Estonia there are cybersecurity events for lower-level competitions such as CyberPin [7] for grades of 1-6 and CyberCracker [8] for grades of 4-9, all these events are held once a year. These events are necessary for training students for them to be able to participate in higher-level competitions like local CyberDrill [9] and CyberSpike [10] and international events like Magic CTF [11], European Cyber Security Challenge [12] and others. In addition to those possibilities, there are also gaming events for the cybersecurity community that is called “capture the flag (CTF)” [13] where cybersecurity talents are cracking the puzzles and learning about attack or defence in a safe and legal environment. Some studies even have shown that competition-based learning has shown increase of motivation to learn cybersecurity-related topics [14] [15].

The motivation of the thesis is that:

- universities would have more young people interested in the cybersecurity;
- the military would have more young people to choose for cyber-service;
- companies would have more specialised people in the field;
- the field would progress.

The novelty of this study is:

1) According to the Estonia's cybersecurity strategy for 2019-2022 chapter 3 stipulates that we need to focus more to the cybersecurity awareness among young and improve our talents pool for building up our information society [16].
2) Informatics curricula in Estonia will go into updating soon again (7.-9h graders plans were not executed and 2017-18 developed curriculum for high school needs a facelift). More school should teach cyber security as part of their curriculum. The question is how to engage both teachers and students in cybersecurity learning-teaching, either through formal education or nonformal education. Since in formal education there is no decisions made and seems that then it should be done in nonformal education, but how – as most of schools are in different paths and learning curves.
   a) Challenge with that is that most students have not been exposed to CTF and their teachers do not have enough skills to set up a CTF environment or even direct students to that area;
   b) The problem is that there is no understanding of what is currently taught in the schools, how it is taught and whether they need help;
   c) Also we need to consider that teachers would prefer environments and study materials to be in the Estonian language or would have the support for it, since the education programs are in the Estonian basic and high schools mainly in Estonian language.

3) IT- and Cyber security companies are developing solutions and training platforms that suits adult learners, international high paying learners. Problem with engaging more students in cybersecurity learning through nonformal education is no-mands land as its costly and benefit comes 5-10 year not immediately. Currently cybersecurity companies such as RangeForce, KPMG, CybExer, Clarified Security and TalTech are

looking for talents through organizing more CTF competitions, but CTF are ran 1-5 times in a year and it is not enough to have a permanent effect for the mass's education. How is it possible to get more masses involved to harvest more talents for all the Estonia that cyber security strategy is aiming for? How can we take opportunity and improve the situation for the schools, students that they can manage the competencies in a lower level themselves and still have an impact for the future workforce in the cybersecurity area?

The goal and a scope of this research paper is to find answers to the following questions:

1) According to the curricula in general education schools, how is cyber defence taught and what topics are covered?
2) What extracurricular activities are available for students to learn cyber defence?
3) Is there a need for Capture The Flag (CTF) environment and which kind of CTF environment schools need?
   a) What are the options for creating and using a CTF environment?
   b) What are the school's needs for using such an environment?

2 Strategies in cybersecurity

This chapter will look into cybersecurity strategies from the education, digital safety and digital literacy point of view.

2.1 Education in cybersecurity strategies

Although there is not much material on cyber defence strategies aimed directly at young people, from a national perspective, general cyber defence strategies need to be examined to see if there is a focus on educating people and the rise of cyber defence experts. Some examples of countries strategies that are promoting cybersecurity among young people:

- The United States of America's national cybersecurity strategy says that the National Initiative for Cybersecurity Education (NICE) is prioritising cyber awareness and promoting cybersecurity in education. [17]
- The Japanese government is enhancing cybersecurity by making computer science courses mandatory for elementary schools. Additionally, cybersecurity learning environments should be created, which would prevent cybercrime in youth. These measures come from the Japanese national cybersecurity strategy. [18]
- The Australian government is taking measures to educate all Australians, such as having cybersecurity modules for basic and high schools, and a program for raising cybersecurity awareness called Cyber Security Awareness Week. [19]

In the European Union, an agency called European Union Agency for Network and Information Security (ENISA) helps coordinate cyber defence strategies in europe. ENISA gives an overview and supports countries in their strategies. Their mission is to raise awareness of network and information security. ENISA’s objectives are expertise, policy, capacity, community, and enabling. Expertise’s task is to analyse global cyber issues and help to find out future risks and threats, as well as to give best practices for dealing with cyber problems. The policy task is to promote information security in the

European Union and create guidance and law for it. The capacity task is to help build information security capabilities in European countries. The community task is to strengthen cooperation between Member states, public and private sectors and ENISA related communities. The enabling task is to make sure ENISA is working efficiently. To involve young people in cybersecurity they have initiated The European Cyber Security Challenge. [20]

In the European Union internally, there are exemplary countries that are working towards educating people about cybersecurity:

- In Finland, basic cybersecurity-related topics have to be taught in every level of education and learning cybersecurity has to be mandatory for all levels of education. [21]
- Lithuania's national cybersecurity strategy suggests also that basic cybersecurity topics should be taught in primary, basic and secondary schools. [22]
- In Sweden, security of the Internet topic is part of the teachers' training course, for achieving a more secure Internet environment. [23]

The author investigated education and training parts only in Estonia's cybersecurity strategies since technical parts are not in the focus of this study. In Estonia, the Ministry of Economic Affairs and Communications has created a cybersecurity strategy for the years 2019 to 2022. The main vision of the current strategy is that Estonia is the most cyber-secure digital country in the world. To achieve the vision there are four basic principles. The protection and promotion of fundamental rights and freedom on the Internet are as important as in the physical environment. Cybersecurity should be treated as an enabler and amplifier of Estonia's rapid digital development. Security must support innovation and innovation must support security. We must acknowledge that ensuring the security of cryptographic solutions is as uniquely important for Estonia, as the entire ecosystem of a digital country is based on it. The functioning of the digital state is based on transparency and public trust. To maintain this, they adhere to the principle of open communication by the state. The goals are that Estonia is a sustainable digital society with strong technological resilience and crisis preparedness, is a respectable and strong partner in the international arena, is cyber-conscious and the future of specialists in the field is guaranteed. [16]

The same strategy has been made for the years 2021 to 2024. The future strategy shows that awareness of cybersecurity remains insufficient among public and private leaders as well as in society more broadly, which in turn leads to a lack of ownership, which causes underestimation of cybersecurity in the development of information systems and services. Ensuring cybersecurity is not perceived as personal responsibility or as a risk to the core business of the organization but is predominantly treated as a complex technical issue with which someone else must deal with. From the strategy we found out that the current cybersecurity curricula have not yet sufficiently considered the needs of the Estonian labour market, because there is no clear mapping and ordering of labour needs. The lack of flexible retraining opportunities can also be pointed out as a shortcoming of cybersecurity curricula. [24]

2.2 Strategies in digital safety and digital literacy

Cyber defence strategies focus more on adults, activities aimed at common citizens of European Union are set out in the DigComp model, which applies to both young people and adults [25]. The DigComp model has been implemented differently in each EU country. In Estonia it has been implemented almost one to one. For example, in the digital safety the learner:

- knows how to protect their digital devices and its content;
- understands threatening dangers of a digital device and is able to avoid them;
- implements security measures to protect their personal data and privacy in the digital environment;
- makes sure that the digital service that uses their personal data is in accordance with the service's privacy policy;
- is aware of the mental and physical health risks associated with the use of digital technology and is able to prevent these risks;
- is aware of the impact of digital technology on the natural environment [26].

Estonian Ministry of Education and Research has created Lifelong Learning Strategy for 2014 to 2020. The strategy has five strategic goals:

1) Changed perception of learning - supporting the individual and social development of each learner, learning skills, creativity and the entrepreneurial learning concept has been applied at all levels and types of education.
2) Competent and motivated teachers and school leaders - the evaluation and remuneration of the work of the teacher / lecturer and the head of the school is in accordance with the requirements for these positions and the performance of the work.
3) Compatibility of opportunities for lifelong learning and the needs of the world of work - high-quality, flexible learning opportunities and career services with diverse choices and considering the development needs of the labour market have increased the number of people with professional qualifications in different age groups and different regions of Estonia.
4) The digital revolution in lifelong learning - in learning and teaching, modern digital technology is applied more efficiently and effectively, the digital skills of the entire population have improved and access to the new generation of digital infrastructure has been ensured.
5) Equal opportunities for lifelong learning and increased participation in learning - equal opportunities for lifelong learning have been created for all people. [27]

In order to implement the strategy, the Ministry of Education and Research prepares programs for all levels of education based on the development plan and implementation plan. [27]

The Ministry of Education and Research has created The Education Development plan for 2021–2035, which is a follow-up strategy to the Estonian Lifelong Learning Strategy 2020. The plan has a general goal of Estonian people having the knowledge, skills and attitudes that enable them to fulfil themselves in personal life, work and society and support the promotion of Estonian life and global sustainable development. The general goal is supported by three strategic objectives:

1) Learning opportunities are abundant and accessible, and the education system allows for smooth movement between levels and types of education.

2) Learning is learner-centred and forward-looking, and the future of teachers is guaranteed.
3) Learning opportunities meet the development needs of society and the labour market. [28]

Next step is to find out what kind of education is provided for students in the world and in Estonia.

3 Education

This chapter will give an overview of what kind of formal and non-formal education are in the world and in Estonia. The overview starts from the university level to basic school level.

3.1 Learning theories

In education there are different learning theories. The main learning theories are behaviourism, cognitivism, humanism, social learning theory, constructivism, experiential learning and connectivism. Behavioural theory argues that learning occurs only by making associations or connections between one's experiences or behaviour. According to cognitive learning theory, the central place in learning is the internal processing of information, because of which the internal models necessary for receiving, deciphering information, and solving problems are acquired. Humanism learning theory says that learning is realising your ability. Social learning theory is based on learning from other people and situations, new behaviours are acquired by modelling the surrounding environment. Constructivists say that a learning environment that is rich, varied, motivating and individual is very important in learning. There is a constant emphasis on the social context and other people's contribution to learning, teamwork. Experiential learning theory is based on learning through personal experience, its interpretation and application in new conditions. Finally, connectivism says that knowledge is shared between networked connections and learning is the ability to create, connect and transcend these networks. The author wants to know what learning theories are used in teaching cyber defence and will look teaching cybersecurity from that perspective. [29]

3.2 Formal education

This chapter will give an overview of what kind of cybersecurity and informatics curriculums are in different school levels in the world and in Estonia.

3.2.1 Cybersecurity curriculums around the world

This subchapter will give an overview of cybersecurity curriculums and courses in the world. The curriculums and courses described are top results with a keyword “cybersecurity curriculum”.

Around the world there are a lot of cybersecurity curriculums or courses for students starting from kindergarten to university. Although there is an overview of which universities teach cybersecurity in Australia [30], Europe [31] and United States Of America [32], this information is not available for general education schools.

The topics that are commonly taught in bachelor and masters levels in United States of America and European Union universities can be seen in the Figure 1.

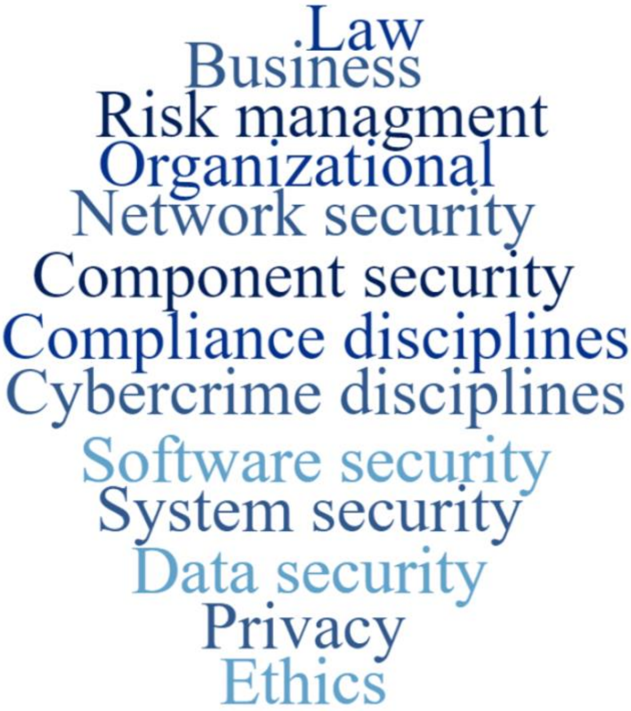


Figure 1. Cybersecurity topics taught in universities

These topics are taught in for example, Technical University of Denmark [33], University of Turku [34], Vilnius Gedmininas Technical University [35], Purdue University

Northwest [36], Georgia Institute of Technology [37] and Maryville University [38] for example.

Estonia is one of the few in Europe, who teaches cybersecurity in vocational schools. For teaching cybersecurity in vocational schools, a project called ITSVET has developed a cybersecurity curriculum, laboratories and other learning materials for Estonia, Latvia and Finland vocational schools [39].

For general education in the United States of America some schools have a cybersecurity curriculum. For example, Lower Dauphin School District offers the curriculum for grades of 10-12 with topics of:

- “ethics and society;
- security principles;
- cryptography;
- physical security;
- malicious software;
- web security;
- computer forensics investigation [40].”

Besides cybersecurity curriculum, the schools have computer science courses through which they teach some of the cybersecurity-related topics such as network security.

The author did not find any schools in Europe that actively have cybersecurity curricula, instead there are computer science courses where schools introduce cybersecurity related topics. For example, Carr Hill Highschool in England has a computer science course for grade 10, where students learn about cyber-attacks, finding and solving system security vulnerabilities [41]. Most of the European countries have digital literacy integrated into the curriculum or have it as a separate subject. Better visualization can be seen in the Figure 2.

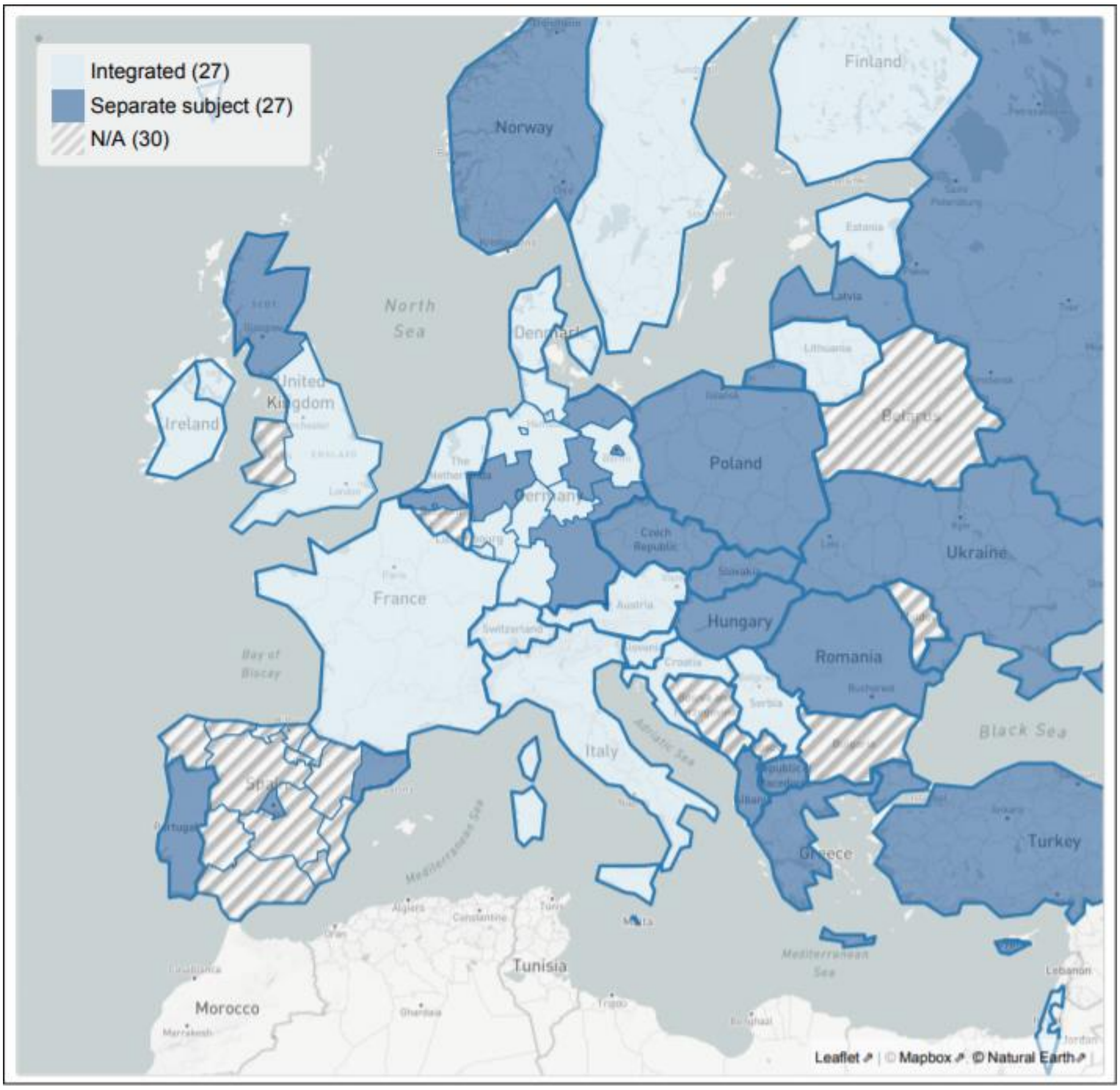


Figure 2. Digital literacy curricula in Europe [42]

Estonia is one of the few countries who has dedicated cybersecurity courses for high schools available. Next step is to find out what Estonian schools are providing for students compared to the rest of the world.

3.2.2 Cybersecurity curriculums in Estonia

This subchapter will give an overview of cybersecurity curriculums and courses in Estonia. The curriculums and courses described are top results with the keywords “cybersecurity curriculum” and “informatics curriculum”.

After graduating high school, students have an option to study cybersecurity technologies curricula at bachelor level in the Tallinn University of Technology. Graduating from this curriculum, the students should understand the nature of the information system life cycle, the basics of information system management, including development and test environments. The graduate should be able to program, test and implement an information system from the point of view of its security and manageability, perform information system security testing based on standards and best practices, implement processes that ensure the security of the information system, participate in their development and improvement and should be able to follow ethical standards in their professional activities. [5]

Additionally, if students have acquired a bachelor's degree, then they have an option to study in the joint curriculum of Cyber Defence master’s level in the Tallinn University of Technology or in the Tartu University. In the curricula the student has to choose speciality from three choices: Cyber Defence, Digital Expertise or Cryptography. [6]

Students who choose vocational training centres instead of high schools have an option to go to Pärnumaa Kutsehariduskeskus where they are offering vocational training for IT-specialists. The curriculum gives a base for cybersecurity, teaches about web applications security, cyber hygiene, and network security. Completing the curriculum gives students an opportunity to work as a cybersecurity specialist or cybersecurity consultant for example. The length of this curriculum is one year, and school takes place on two to three days a week. [43]

The ministry of education and research has developed four national curriculums for vocational training centres. The first curriculum through which students achieve Junior IT systems specialist status contains a cybersecurity module which is about four percent of the whole curriculum. The second curriculum through which students achieve Junior Software developer status and the third curriculum through which students achieve Software developer status does not contain cybersecurity modules at all. The last curriculum through which students achieve IT systems specialist status contains a cybersecurity module which is about three percent from the whole curriculum. [44]

In addition to cybersecurity or informatics curricula, which can be used also in the vocational school, there is a project called CyVET, which objective is to lower missing parts in cybersecurity competence. The project created a cybersecurity curriculum that has four different profiles depending on how technical or cybersecurity-based it is. The first profile is more developed towards cyber hygiene, the second more towards data security and secure data transport. The third and fourth profiles teach cybersecurity more deeply and are useful for workers that work in the same field. The first profile is suitable for all vocational training and curriculums. Other profiles are not relevant in this thesis. [45]

Estonia's general education has a national curriculum for basic schools [2] and high schools [46]. For basic schools there is an elective subject called Informatics, through which students in second level will learn about the following topics:

- introduction to word processing;
- file management;
- searching for information on the Internet and working with media files;
- working with data;
- creation of presentation;
- formatting of a school paper;
- In the third level, students will acquire knowledge about these topics:
- Internet as a communication and work environment;
- Estonian e-government and e-services;
- creating a personal learning environment;
- content production and reuse, licenses;
- participation in a virtual community of practice;
- completion of the development project [47].

In addition to informatics courses, students in grades one to nine have digital safety course options. The topics that are taught in the first, second and third level of school are generally similar. The topics are about:

- safe use of smart devices and other digital equipment;
- information systems and environments;
- virtual identity management;
- public and private communication;
- health risks;

- technical problems [48].

The first school level has a course called Digital Safety, the second school level has a course called Digital Hygiene and the third school level has a course called Cyber Hygiene [48]. Tartu University has developed a book for the first and second school level, which is called Digital Textbook. No materials have been created for Cyber Hygiene course and the development activities have been stopped now.[49]

For high schools there is an elective course called Cyber Defence [50]. For teaching the course, there is a cybersecurity book for high schools called Cybersecurity. The subject gives an overview of cyber defence and discipline and gives its reader an opportunity to gain basic knowledge in the field. The subject consists of three main topics, which are information society, risks and danger, and work opportunities and career. [4]

Under the information society topics student will acquire knowledge about these subtopics:

- information space and society and cyber defence;
- digital society on the example of Estonia;
- culture and ethics of digital society;
- laws and regulations;
- development and future of the information society [4].

Under the risks and danger topics student will learn about these subtopics:

- data and identity;
- fraud and scams;
- effects on mental and physical health;
- attacks and threats;
- infrastructure, network and its security;
- web attacks, network logs;
- smart security and home security audits [4].

Under the opportunities and career topics there are following subtopics:

- examples and anti-examples;

- cyber defence competencies;
- studying and career in cyber defence;
- talent hunt [4].

As the curricula are voluntary and each school can implement them as it wishes or has the opportunity, different schools use cyber defence study days or discuss the topic in the computer science lesson. There are less than 10 schools teaching cybersecurity in Estonia in high school level as a course. There are more schools who have taken use of the modules from the materials.

The following are some examples from schools. The schools were chosen with the keyword "informaatika õppekava". Total of 13 schools were found in the first four pages of the search.

In some of the basic and middle schools there are informatics courses where students learn how:

- to join and use web-based environment purposefully and safely;
- to distinguish between security levels of environments such as HTTP and HTTPS;
- to use virtual identity securely and ethically and distinguish real virtual identity from a fake one [51] [52].

In Viimsi basic school, they teach computer security and how to defend computers from viruses and malwares. [53]

In Vasalemma basic school the Informatics curriculum additionally offers a career module. The career module develops students' readiness to enter the labour market and achieve better employability, to develop independent decision-making skills, to fulfil different life roles. Career education helps to ensure that the new generation is not constrained by the stereotypical gender roles that have developed in traditional culture and time period. [54]

Instead of special cybersecurity curriculum, the Vastseliina Gümnaasium is offering optional course called Multimedia and Cyber Defence for students in the 3rd grade, which focuse more on multimedia than cyber defence. After completing the course, the student is aware of the most common dangers associated with smart devices and ways to avoid them. In addition, the student can prevent and remove malware from smart devices, prevent common security flaws using smart devices, distinguish between insecure and secure WiFi networks, can assemble a computer, knows the role of antivirus and firewall with the Windows operating system in the computer, knows how to use their Windows computer more securely, can use Linux at a basic level and gains first experience with the competitive side of cybersecurity. [55]

Põltsamaa Ühisgümnaasium offers a field of study called Cyber Defence, which has four main courses called information society, fundamentals of secure networking, digital security and cryptography and introduction to mechatronics. Upon completing the syllabus of high school cyber defence, students have acquired cybersecurity theory fundamentals and hands-on experience to make their daily digital environment safer. The school also offers field of study called Cyber Defence - Information Technology (IT), which has the four main courses called cyber protection and digital services, basics of secure networking, mechatronics and software development. Upon completing the study, students have acquired cybersecurity theory fundamentals and hands-on experience to make their daily digital environment safer. [56] [57]

Rocca Al Mare school offers students a cybersecurity course, after which the student will have acquired wider knowledge about cybersecurity for the average user, in order to make their daily activities in cyberspace more secure. Additionally, they will be able to help their family and community with problems in day-to-day activities on the Internet, from the cyber hygiene and safety point of view. [58] In addition to Rocca al Mare, students from Jõhvi Gümnaasium also have an option to choose an elective course in cybersecurity. Specifically, Jõhvi Gümnaasium offers an Infotechnology module, which is suitable for students who are interested in the digital world and wish to have an overview of the various areas related to information technology. In addition to programming and creating websites and applications, the optional module provides an opportunity to get acquainted with both cyber defence and robotics. Additionally, they offer an Accurate Science module, which also has courses about cyber defence and robotics. [59]

3.2.3 Analysis of Estonian school curriculum examples

For analysing the curriculum and courses, the author chose schools that were different from each other to see the big picture of what is currently being taught. 10 school’s curricula were selected and compared. The curricula were chosen by two criteria's, which were curriculum that contained cybersecurity-related topics and non-repetitive curricula. The curricula were compared by the cybersecurity-related topics, the volume of curricula and by grades in which these topics are taught. To get better knowledge about what topics are being taught in basic schools and high schools, the author compares different Informatics and cybersecurity curriculums. The author is more interested in the topics that are taught in the seventh to twelfth grades. The goal of the comparison is to find what cybersecurity topics are missing from the curricula. It should be mentioned again that schools have the autonomy to make their own curricula and syllabus. There is a sample national curriculum from which schools choose the modules that suit them. The topics that were found have been divided into two main categories which are digital safety and cybersecurity-related topics.

The author investigated the curricula and found a lot of informatics competencies such as:

- basics of spreadsheet programs such as Excel;
- photo editing programs;
- word processing skills;
- prepare hypertext documents in Wikipedia;
- creation of a personal learning environment;
- create new web content and reuse web content created by others, based on good practices in intellectual property protection;
- basic programming language
- reflect on their learning experience using a blog [51] [60] [61] [62].

In addition to informatics competencies, schools teach digital safety, some also call it cyber hygiene. For example, in Vasalemma basic school's informatics syllabus for 7th grade, they have a topic about how students can:

- protect their virtual identity and distinguish real virtual identity from a fake one;
- use information systems provided by schools, local governments, and the state, and youth e-services [54].

In addition to these topics, Viimsi school students learn about smart device safety and how to understand the damage caused by computer viruses and malware, and the importance of anti-virus protection [53]. In Tartu Kristjan Jaak Petersoni Gümnaasium the student will learn about components and operations of digital services through IT-module [63]. Students in Järveküla School have opportunity to learn about online communication and cyberbullying and have ability to perform a personal security audit and resolve security issues identified by the result of the audit [64].

The author searched for cybersecurity-related topics from the curricula and found that one common topic schools are teaching is to distinguish between security levels of environments such as HTTP and HTTPS. Other cybersecurity related topics were more school specific.

For example, In Põltsamaa Ühisgümnaasium they have a Cyber Defence curriculum for 10th to 12th grades. The curriculum consists of four core courses: information society, the basics of secure networking, digital security and cryptography, and introduction to mechatronics. Upon completing all four courses, the student will:

- know common cyber attack types and how to deal with them;
- know what is privacy and is able to protect their data with everyday tools and opportunities;
- have the knowledge on how to protect IT equipment from simple cyberattacks, prevent and avoid malware infection of equipment and systems;
- know the principles of secure use of network and cloud services;
- be guided by good practices of intellectual property protection;
- know and generally follow the regulations related to Information and Communications Technology (ICT),
- be aware of the framework of the common part of technology and legal ethics and knows the main terms and concepts used in the field;
- have an overview of the possibilities, security and operating principles of e-Estonia services;
- have an overview of cryptography and will be able to use the most common everyday encryption options;
- know the possibilities of using robotics today;

- be able to advise the community on day-to-day cyber defence issues related to privacy;
- be able to secure data transmission and behaviour on social networks. [56]

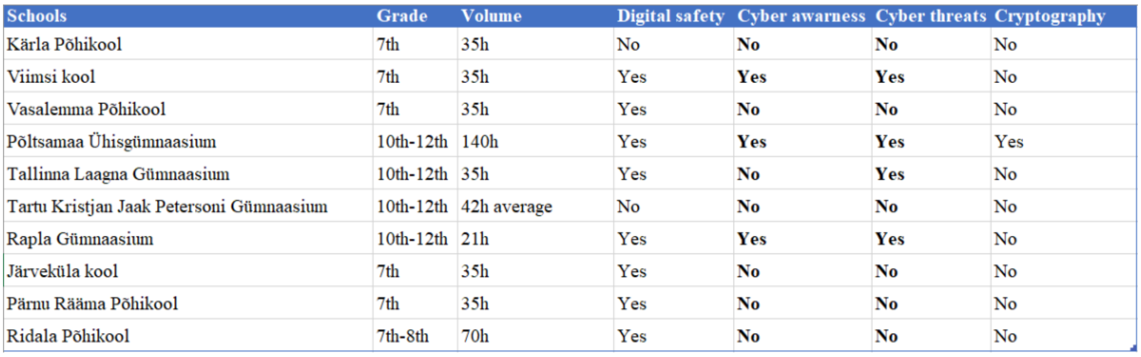
Rapla Gümnaasium has a unique teaching system, where the students can choose courses, they want to learn, due to which they have a lot of elective courses. One of the elective courses is cybersecurity. Upon completing the cybersecurity course, the student will learn the history of information security, get an overview of the most important cyber-attack types and the writing of the first virus circumstances. The students will know, be able to explain and implement cyber defence and cybercrime basic concepts, acquire basic skills in home IT networks and consumer security to ensure and protect against the most common cybersecurity incidents, are able to describe and document a cyber incident and compile an appropriate notification to the competent authority. [65]

The schools' syllabuses that author found by the criteria were:

- Kärla basic school;
- Viimsi school;
- Vasalemma basic school;
- Põltsamaa Ühisgümnaasium;
- Tallinna Laagna Gümnaasium;
- Tartu Kristjan Jaak Petersoni Gümnaasium;
- Rapla Gümnaasium;
- Järveküla school;
- Pärnu Rääma basic school;
- Ridala basic school.

From the 10 analysed syllabuses, only one school had a course solely focused on cybersecurity, others were mostly named "informatics" and had some cybersecurity or digital safety topics in the course. The following table shows which schools, and in which grade cyber-related topics are taught (see Table 1).

Table 1. Schools teaching cyber-related topics



Schools	Grade	Volume	Digital safety	Cyber awarness	Cyber threats	Cryptography
Kärla Põhikool	7th	35h	No	No	No	No
Viimsi kool	7th	35h	Yes	Yes	Yes	No
Vasalemma Põhikool	7th	35h	Yes	No	No	No
Põltsamaa Ühisgümnaasium	10th-12th	140h	Yes	Yes	Yes	Yes
Tallinna Laagna Gümnaasium	10th-12th	35h	Yes	No	Yes	No
Tartu Kristjan Jaak Petersoni Gümnaasium	10th-12th	42h average	No	No	No	No
Rapla Gümnaasium	10th-12th	21h	Yes	Yes	Yes	No
Järveküla kool	7th	35h	Yes	No	No	No
Pärnu Rääma Põhikool	7th	35h	Yes	No	No	No
Ridala Põhikool	7th-8th	70h	Yes	No	No	No

It can be seen from Table 1 that digital safety is the most popular topic to be covered in the syllabuses that were analysed in this thesis. Although digital safety is taught only on a basic level, such as protecting one's virtual identity, user creation and choosing secure passwords is an important topic to teach students. Cyber awareness and cyber threat topics on the other hand are taught in only a few schools, mostly in high schools, and cryptography is taught only in one school. The most common knowledge a 7th-grade student acquires is how to use word and photo processing tools and how to search for information on the Internet.

In the author’s opinion, the schools should contribute more to teaching cybersecurity and create more courses in the field, since our current society is more computer-driven. Especially in COVID-19 times, when everything students do is online, it is crucial for them to have knowledge on how to properly act on the Internet, how to protect themselves and their personal information and how not to fall victim to cybercrimes. It can also be noted that none of the analysed courses were mandatory, they were mostly elective courses. In the author’s opinion, cybersecurity should be mandatory for students at least on a basic level, since more of our lives are online and this is a developing field, so raising awareness might also get some students interested in pursuing a career in it. In order to gain more insight into why schools are not more focused on cybersecurity and if they are, what topics are they more focused on, the author has conducted a survey and carried out interviews.

From the learning theory point of view from the chapter 3.1, formal education tends to be more cognitive, where the teacher role is structuring learning activities and sharing knowledge with students. The student role is to be active and adaptive learner.

3.3 Non-formal cybersecurity education

There are other ways than cybersecurity curriculums to teach cybersecurity to younger students. Other ways to have a bigger impact on cybersecurity knowledge in students are summer camps, online courses, hackathons, and cybersecurity competitions/events. Educating students through workshops and competitions has shown to be an effective way to teach the cybersecurity related topics to students. [66] Additionally, learning through video games have shown a good way to gain experience about the cybersecurity profession and has potential to make a difference in choosing a profession. [67]

3.3.1 Non-formal cybersecurity education in the world

In addition to schools, there are also separate projects to teach cybersecurity, for example Hacker Highschool [68], National Initiative For Cybersecurity Careers And Studies [69] and Virginia Cyber Range [70].

There are different non-formal cybersecurity related programs in the world. For example, there are different summer camps that focus on the topic. The GenGyber camp in the United States, which is organised by the National Security Agency and the National Science Foundation, focuses on increasing interest in cybersecurity careers [71]. Computer Science for Cyber Security is a summer camp organised by New York University, which introduces the fundamentals of cybersecurity, this program’s target group is girls from high schools [72]. CyberSTEM organised by Denmark Technical College has separate camps for middle and high school students, where computer forensics, different programming languages are learned and students have the opportunity to participate in different projects [73]. In the United States of America there is a program called CyperPatriot, which offers different levels of cybercamps and competitions [74].

Secondly, there are different events such as hacking events and conferences. Major League Hacking helps create big hackathon events in North America, Europe, and Asia. They have an event called Local Hack Day which is worldwide and local communities can participate in that. [75] Additionally, there is an annual hacking conference that takes place in Las Vegas called DEF CON. This conference targets different age groups and offers participants the opportunity to sharpen their skills in DEF CON villages, different announcements, talks and workshops and presents tools that people have created. [76]

Thirdly, there are different competitions for cybersecurity enthusiasts. In Europe there is a big cybersecurity competition called European Cyber Security Challenge which gathers all young cybersecurity talents who can compete for the win. The participants must solve complex challenges related to web security, mobile security, crypto, and more. [12] Additionally they have their own cybersecurity curriculum for high schools and universities. [77]

Another cybersecurity competition is called picoCTF which was created by Carnegie Mellon University. This competition focuses on middle and high school students and consists of challenges around a storyline. [78] There is a website that has archived different CTF competitions, some of which have ratings from teams that have competed. It gives a good overview of how many CTF events there are worldwide. [79]

There are also some courses which students can take to educate themselves in their own time. CodeHS offers a web-based curriculum Introduction to Cybersecurity (Vigenere), which teaches cryptography, software security, cyber hygiene, and networking security. The curriculum is made for students from grades nine to ten. The topics are learned by videos, quizzes, and simulations. [80]

There are of course lot more cybersecurity competitions such as The Cyberlympics [81], National Collegiate Cyber Defense Competition [82], National Cyber League [83], Cyber Quests [84], U.S Cyber Challenge [85], NetWars: DFIR Tournament [86], Panoply [87], CyberPatriot’s National Youth Cyber Defense Competition [88], PacketWars [89], International Collegiate Cyber Defense Invitational [90], Digital Forensics Security Treasure Hunt [91], The International Capture The Flag [92], National Cyber Analyst Challenge [93], The National TSA Conference competition [94], CyberForce Competition [95] and many more.

3.3.2 Non-formal cybersecurity education in Estonia

In Estonia, there are different extracurricular activity groups and competitions in the cybersecurity field. Küberring is an extracurricular activity group for children aged five to seven. In the 2017/2018 study program, they were teaching basic knowledge about dangers and malware for smart devices, such as mobile phones, and how to remove them. Additionally, they teach about secure and unsecured WiFi networks, what purpose anti-virus programs have and cyber hygiene. The same topics are taught in the 2019/2020 study program but by different people. [96] Enterprise called Noored Progejad offers an extracurricular activity group for children aged between seven and sixteen. They have developed a curriculum that teaches homepage development, creation of a mobile application, game development, cybersecurity, graphic design and modelling, and hacking methods. From the cybersecurity side, it teaches the basics of cybersecurity, cyber hygiene, cyber threats, and cyber technologies. Additionally, it gives an overview of basic hacking methods and how to protect yourself from them. [97]

The biggest cyber competitions that are held in Estonia are CyberSpike [10](Estonian: Kübernaaskel) and CyberCracker [8] (Estonian: Küberpähkel) and CyberDrill [9] (Estonian: Küberpuuring). All of these competitions are organized by the Tallinn University of Technology. The CyberSpike is a cyber defence competition for ages 14-24 years, where participants show skills in completing different problems and acquire the flag. The competition is held in Capture the Flag style [10]. The CyberCracker competition is a research and testing project for students in basic, upper secondary, and vocational schools. The survey focuses on different digital safety and cyber defence knowledge, such as privacy and safety, cyber hygiene, problem-solving, and technical binding. In 2019 there were about 2660 participants in the school round and 202 in the final round, overall, there were around 8700 participants. [8] CyberDrill is a cyber defence competition for ages 14-19 years. In 2020 the competition had a preliminary and a main round. In the preliminary round there were sixteen background questions and 30 competition questions. The competition was held in both Estonian and Russian languages and was participated by 1791 boys and 1397 girls. The main round was based on CTF and there was a total of 41 challenges with different levels of difficulty. The participation of the main round was team based, where every school could put out 2 teams of girls and 2 teams of boys. CyberDrill's main round competition research showed that schools that focus on IT learning and student creativity development activities have stronger participants than other schools. [9]

For young people in Europe there is a cybersecurity program called Better Internet for Kids. The goal of the program is to provide high-quality online content for children and young people, more effective awareness raising and empowerment in digital safety, creating a safe internet environment for children and fight against sexual abuse and sexual exploitation of children online. [98]

In Estonia, the program is implemented by Safer Internet Centre who also organizes:

- Safer Internet Day, which has different themes every year and each country has different activities.
- Conferences for teachers where they discussed cyber ethics and fake information on the web in 2021.
- Development of materials for teaching digital safety.
- Helpline and hotline to help and protect young people and other awareness raising activities. [99]

From the learning theory point of view from the chapter 3.1, nonformal education tends to be more humanistic learning theory, where the teacher role is to be creator of learning preconditions, opportunities and involve student’s to the process. The student role is to self-conducting learner, creative and spiritual growth aspiring.

4 Cybersecurity learning environments

This chapter describes CTF and other cybersecurity learning environments. At the end of the chapter the author analyses five CTF environments that he tried to set up. To understand what a cyber defence competition is like, the author will look at CTFs, because when a teacher, who is in the focus group, reads this master's thesis, it is more understandable to them what young talents often encounter in their non-formal education. Similarly, one of the research questions is whether CTF competitive environments could be used more in formal education.

4.1 Laboratories and training environments

For learning cybersecurity there are other training platforms than CTF such as Moodle, Google Drive, RangeForce [100] and for example, Hack the Box, which is an online platform, where you can learn penetration testing skills. It offers different labs for individuals, companies, and universities. Every lab has different challenges to complete. [101] [101] These environments are more academic and serve their purpose, but they do not create a competitive spirit and do not always encourage cyber defence talent who want to challenge others to find out who is the best in Estonia or Europe, for example. Similarly, the simulation game used in competitions allows you to deal with problems that are under time pressure and where you must work with others at the same time, for example Locked Shields [102]

From the learning theory point of view from the chapter 3.1, learning cybersecurity through laboratories and training environments tends to be more connectivism learning theory, where the teacher role is to be instructor, advisor and give guidance. The student role is to be active communicative learner.

4.2 Capture the Flag environments and tools

This chapter gives an overview of Capture the Flag environments and tools. Additionally, gives and overview of Capture the Flag.

4.2.1 Overview of CTF

There is a widely known cybersecurity training called CTF competitions. CTF is an abbreviation of Capture the Flag, which in gamification means that both teams have flags that they have to defend or attack. In cybersecurity, it is a contest, which purpose is to challenge participants to solve computer security problems. There are three common types of CTF competitions. [103] [104]

The first type is Jeopardy-style, which means that the competition has a range of different questions and the questions must be answered in correct order in a specific time frame. The questions start from the simpler questions and become more difficult after each question. The harder the question the more points you will get. When you answer the questions correctly, you get a flag that is in a hash format. Then the participant enters the flag and collects points for his team. The winner of this type of competition is the team with the biggest number of points at the end of the time frame. [105] [107]

The second type is the attack-defence style. Each team has its own network or system with vulnerable services. At the start of the competition, you are given a time frame where you can patch your vulnerable services or create traps for the attackers. When the time frame ends, the organizer connects the teams and then the game starts. The idea of this type of CTF competition is that you protect your own system while attacking the other team’s system. For every successful protection, you get defence points and for every successful attack, you get attack points. [106] [107]

The third type is a mix of Jeopardy-style and attack-defence styles. The idea is to solve computer security questions while hacking into other team systems and maintaining your own network. [105]

There are many different types of CTF tools in Github and on the Internet. Some of them offer their own servers, some require setting up a server, or the environments are web applications or simulations which do not need servers to be set up. CTF tools contents are also different, some of the tools can create a CTF competition itself or are a learning tool to practice cybersecurity, or both. For practicing CTF, there is a tool called SecGen which teaches security penetration testing, which creates a virtual machine (VM) based on scenarios to solve [108]. A toolkit to exploit network vulnerabilities called Pwntools has libraries for normal use and for CTF competitions to create challenges [109]. Some of the tools are still in development such as Librectf which, offers the user the ability to create CTF competitions, to insert challenges and it has a built-in grader [110]. Additionally, there are tools that help to maintain cybersecurity competitions by offering a scoring server. For example, Hack The Arch, which has been built by the Military Cyber Professionals Association and is free to use [111].

There are CTF tools that have built-in challenges that you cannot modify, but you can modify the scoring, customization, and penalties. Such tool is for example RootTheBox [112], which has a very graphical user interface.

The most common type of CTF tools are ones that can create challenges, score them, and set up different solving environments automatically, only the tasks must be created by the teacher. Such tools are mkCTF [113], which was used in INS'hAck 2017 competition, Mellivora [114], NightShade which offers setting up different types of CTF competitions [115], Facebook CTF [116] which offers setting up Jeopardy or King of the Hill types of capture the flag competitions.

In addition to tools, there are games that have been developed to teach cybersecurity through gaming, for example framework IPAR, which teaches forensics. The framework is module-based and can be used as a separate Windows application or web application. [117]

The biggest concern of CTF competitions is that they are organized by a university or a company and are not required to be available to schools at any time like traditional teaching materials. Next, the author compares 5 different CTF environments that teachers could set up in their own school to organize CTF competitions.

From the learning theory point of view from the chapter 3.1, learning cybersecurity through CTF environments tends to be mix of experiential learning theory and humanism learning theory, where the teacher role is to be instructor, advisor and give guidance and students. The student role is to be active communicative and self-conducting learner, creative and spiritual growth aspiring.

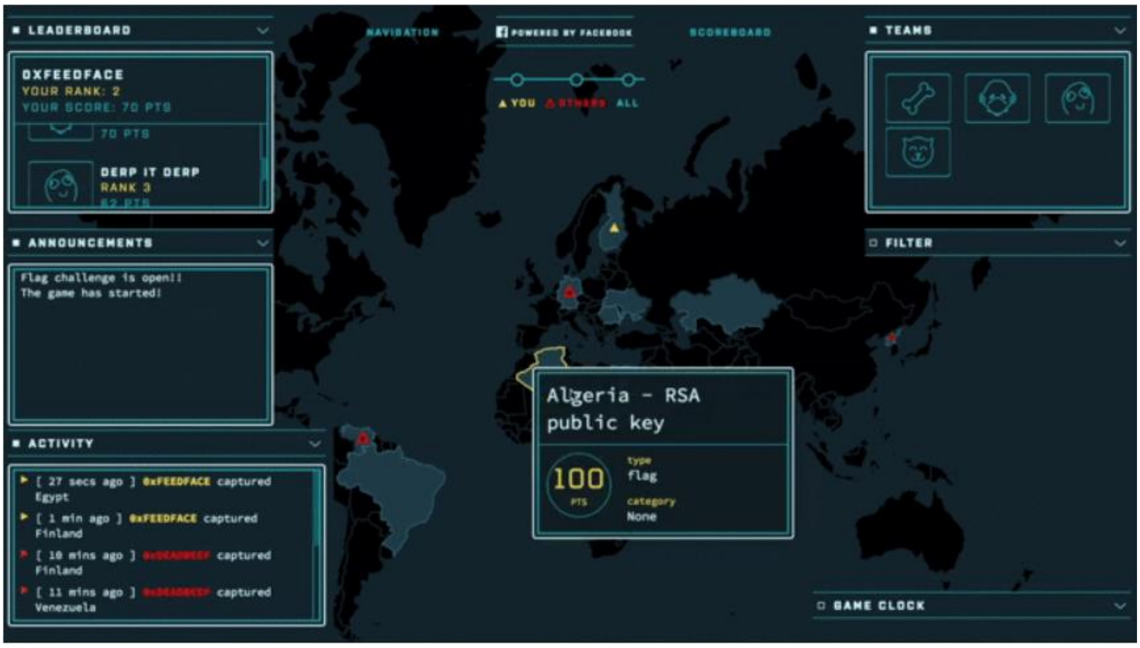
4.2.2 Analysis of selected CTF environments

Five selected CTF environments were chosen for analysis to narrow down the best in order to suggest them to interviewees. The environments were selected from the GitHub and the criterion was that the environment is CTF and there was open access to its code - there were a total of 8 environments, of which 5 were open access.

The five selected CTF environments were FCBCTF [116], Mellivora [114], CTFd [118], PicoCT [119], ctfspace [120].

The environments were compared by three criteria, which were environment setup time, usability and data gathering options.

- First environment that the author tried to set up locally was FCBCTF. After numerous attempts, the author failed to set up the CTF environment, because the environment uses an old version of python module and installs other modules through it. Additionally, installing the environment required a setup of Ubuntu 16.04. Although, author managed to find a small demo of the environment. The environment was very interactive and interesting to use. From all the CTF environments that were tried to set up, this environment had the most interesting visuals, which would invite more students to play. From a data gathering perspective, besides a simple scoreboard there were no other options. The main view of the environment has a basic leader board module, an announcements module, a latest activity module, a team’s module, and challenges/questions as countries. The main view resembles a video game the most from all the environments and can be a bit overwhelming. The main view can be seen in the following image (see Figure 3).



```
Flag challenge is open!!
The game has started!
```

```
[ 27 secs ago ] 0xFEEDFACE captured Egypt
[ 1 min ago ] 0xFEEDFACE captured Finland
[ 10 mins ago ] 0xDEADBEEF captured Finland
[ 11 mins ago ] 0xDEADBEEF captured Venezuela
```

Figure 3. Main view of the FCBCTF environment [116]

- Second environment that the author tried to set up was Mellivora. After numerous attempts, the author failed to set up the CTF environment. Unfortunately, there were no demo versions on the Internet and because of that the author cannot describe nor analyse the environment on usability and gathering criteria. The reason for failure was that the environment code had errors, which the author was unable to fix. It is probable that an average teacher who faces the same error is also unable to set up the environment.
- Third environment that the author tried to set up was CTFd. From all the environments that the author tried to install, CTFd took the least time. It took around 20 minutes to set up the basic environment. The environment was installed with Docker tools and can be restarted in a couple of clicks. CTFd offers a lot of functionality, such as user management, team management, notices, creation and solving the challenges, scoreboard, statistics and solving logs. Every functionality can be managed with an admin role inside the web application. The overall appearance of the environment compared to FBCTF is clean and not overwhelming. Additionally, there is an option to change the design of the web application. Following picture shows the challenge page in the environment (see Figure 4).

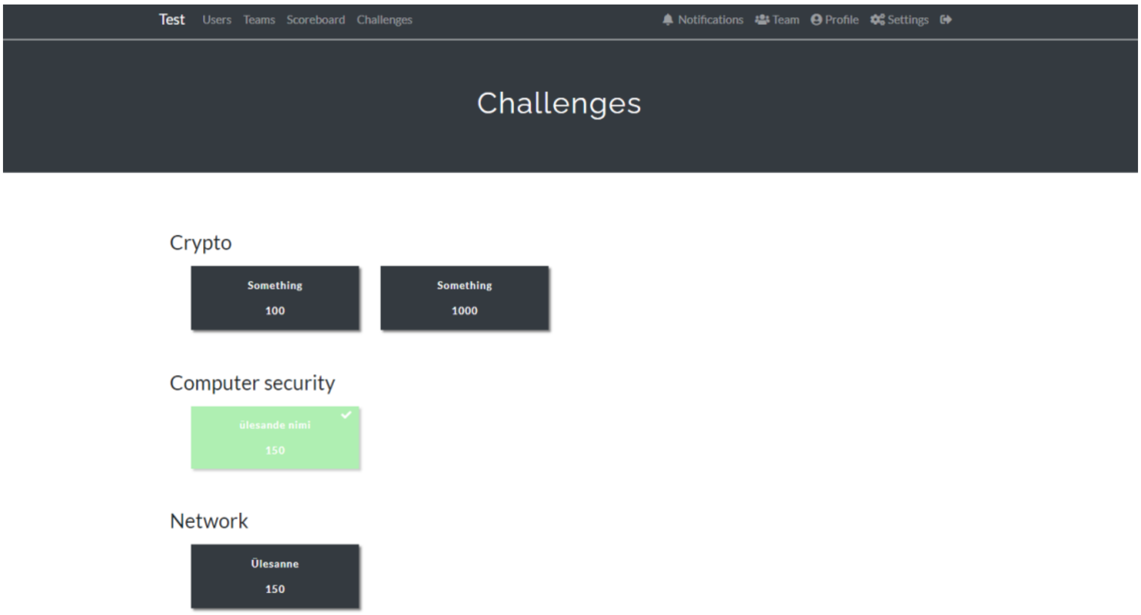
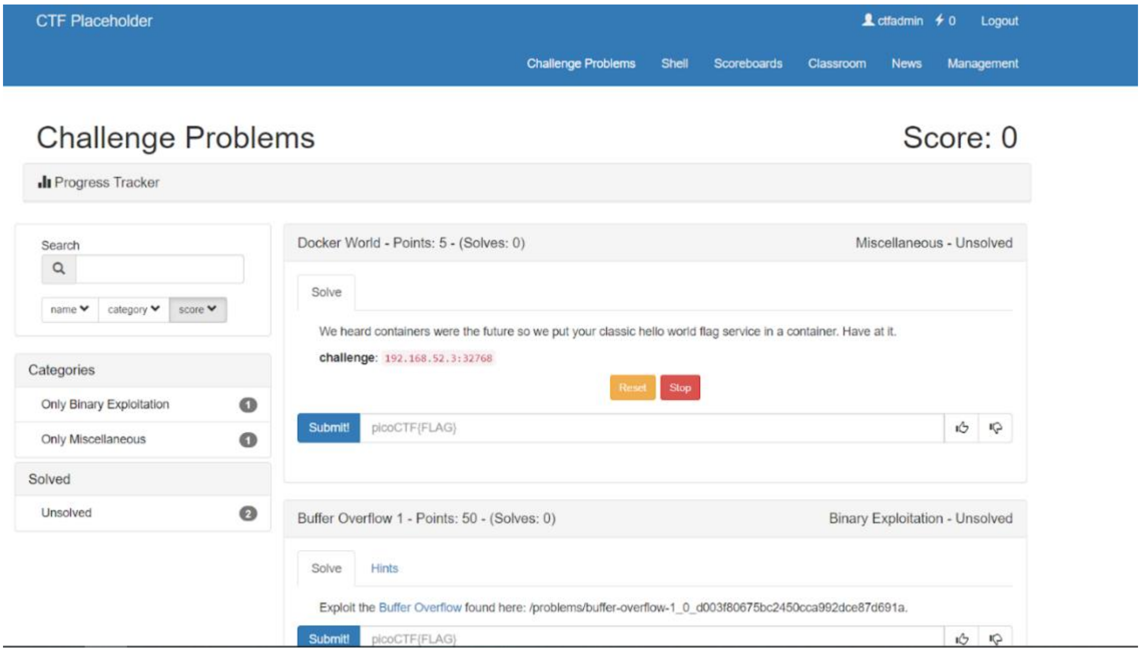


Figure 4. Challenge view of the CTFd environment [118]

- Fourth environment that the author set up was picoCTF. This environment had the longest setup time from the environments that the author succeeded setting up. The long setup time was due to an error that the author managed to solve. Setting up the environment needed some changes in the deployment configuration, since one of the modules' install link was outdated. The environment itself runs in two virtual machines, one of them is picoCTF web, which is the environment for web application and picoCTF shell, which is a Linux environment, where users can complete challenges. PicoCTF offers users management, solving and managing challenges, notices, classroom, and scoreboard functionality. The challenges themselves need to be created in Python language. The challenge creator needs to write a Python file and JSON file and place it in the correct folder of the server directory. This environment is used in the picoCTF competition [78], from the age of thirteen. This environment is unique from other environments by having a shell environment for solving challenges. The main view of the environment is simple and not overwhelming as can be seen in the following picture (see Figure 5).



Challenge Problems

Score: 0

Progress Tracker

Search

Categories

Only Binary Exploitation 1

Only Miscellaneous 1

Solved

Unsolved 2

Docker World - Points: 5 - (Solves: 0) — Miscellaneous - Unsolved

We heard containers were the future so we put your classic hello world flag service in a container. Have at it.

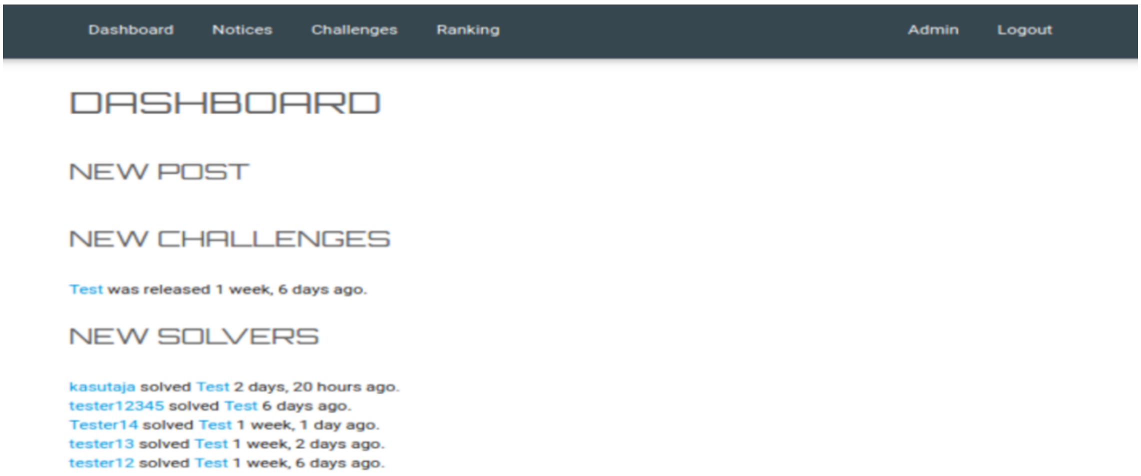
challenge: `192.168.52.3:32768`

Buffer Overflow 1 - Points: 50 - (Solves: 0) — Binary Exploitation - Unsolved

Exploit the Buffer Overflow found here: /problems/buffer-overflow-1_0_d003f80675bc2450cca992dce87d691a.

Figure 5. Challenge view of the picoCTF environment [119]

- Fifth environment that the author tried to set up was ctfspace. This environment was the second fastest setup time environment. Ctfspace is easier to set up in the Linux operating system, since it uses a virtual environment (virtualenv) from Python. The environment is very similar to the CTFd but has less functionality. Additionally, the whole environment is not in one language and displays some information in an Asian language in very important places, such as account registration and challenge creation. Ctfspace offers users and their rights functionality, creating and solving challenges functionality, solving logs and notices functionality. The main view of the environment is very simple as can be seen in the following picture (see Figure 6).



DASHBOARD

NEW POST

NEW CHALLENGES

Test was released 1 week, 6 days ago.

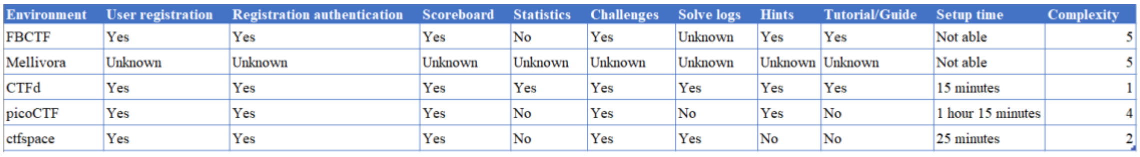
NEW SOLVERS

kasutaja solved Test 2 days, 20 hours ago.
tester12345 solved Test 6 days ago.
Tester14 solved Test 1 week, 1 day ago.
tester13 solved Test 1 week, 2 days ago.
tester12 solved Test 1 week, 6 days ago.

Figure 6. Dashboard view of ctfspace [120]

Author compared all the installed environments and created the following table (see Table 2). The time spent on acquiring all necessary tools was not taken into account for the environment's setup time, since download speed of installers may vary.

Table 2. Overview of CTF environment analysis



Environment	User registration	Registration authentication	Scoreboard	Statistics	Challenges	Solve logs	Hints	Tutorial/Guide	Setup time	Complexity
FBCTF	Yes	Yes	Yes	No	Yes	Unknown	Yes	Yes	Not able	5
Mellivora	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Not able	5
CTFd	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	15 minutes	1
picoCTF	Yes	Yes	Yes	No	Yes	No	Yes	No	1 hour 15 minutes	4
ctfspace	Yes	Yes	Yes	No	Yes	Yes	No	No	25 minutes	2

Registration authentication column shows if the environment has strong authentication, in other words password and email address requirements. Under statistics column author means statistics of solved challenges for acquiring knowledge, what challenges are popular, and which are not. The author rated the complexity of the environment from 1 to 5, where 1 means very easy to use and 5 means very hard or unusable. According to the table and the analysis, CTFd environment would be most suitable for teachers to use in their classrooms and Mellivora the worst. CTFd has all the basic needs and can be set up fast. Additionally, it has plugins to make the environment more complex and have new functionalities such as the first solver of the challenge will get the most points and next ones will get less.

Overall if you have all necessary tools, the setup time of the environments is relatively short for CTFd and ctfspace. Unfortunately, it is very probable that a teacher can run into an error while setting up the environments, which can take a long time to solve. It can be concluded that if these environments had detailed tutorials or setup guides with possible errors that could be faced during setup and what to do to solve them, then it could be an even quicker process. Most of the environments have a registration, scoreboard, and challenges module and only one (CTFd) has a graphic statistics module. From the five selected environments CTFd, ctfspace and picoCTF will be used in the interview with the teachers, since the author thinks that teachers could handle the set-up process.

5 Research Method

In this chapter the author is describing the methods he used to collect and analyse the data. Additionally, an overview is given on limitations of the research.

5.1 Research plan

The goal of this research paper is to find answers to the following questions:

1. According to the curricula in general education schools, how is cyber defence taught and what topics are covered? (Phase 2 and 3)
2. What extracurricular activities are available for students to lean cyber defence? (Phase 1 and 2)
3. Is there a need for Capture The Flag (CTF) environment and which kind of CTF environment schools need?
   a. What are the options for creating and using CTF environment? (Phase 2 and 3)
   b. What are the school's needs for using such an environment? (Phase 2 and 3)

For answering the goals of this study, the author used the following research plan for gathering data, which can be seen in Figure 7.

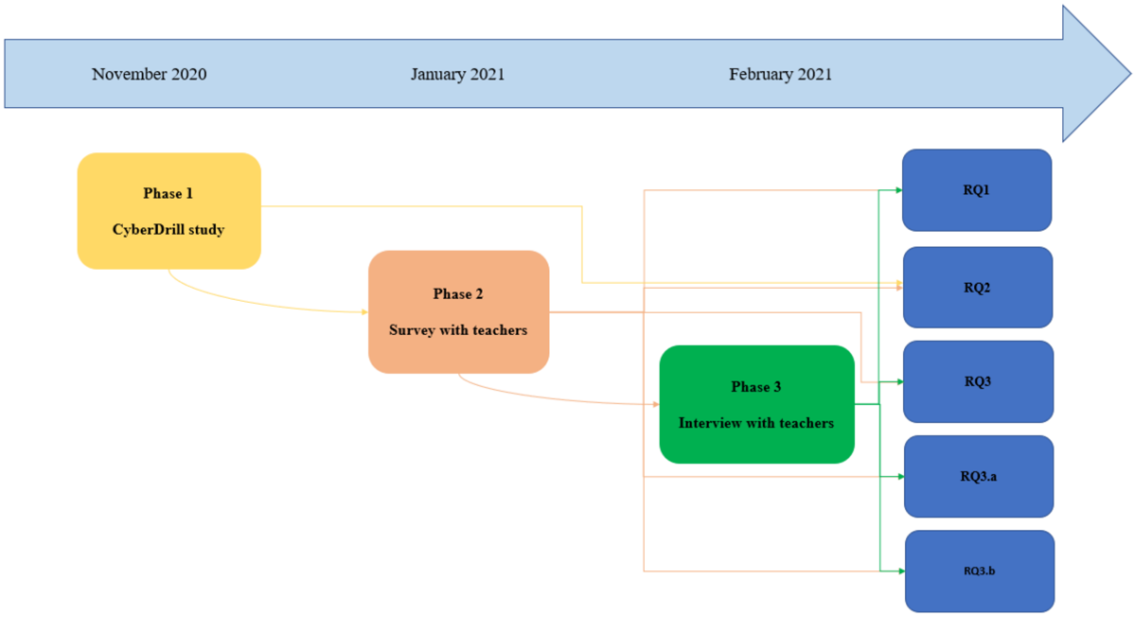


Figure 7. Research plan

The data results and analysis are divided into two parts:

1. Students study: CyberDrill competition background data study about 7.-12 grade students
2. Teachers study
    a. Survey with teachers
    b. Interview with teachers

5.1.1 Students study

Data was gathered from CyberDrill 2020 preliminary round to obtain a student's perspective about their interest and needs to study cybersecurity topics at schools. CyberDrill is a competition for 7.-12th graders and vocational school students that had two rounds:

1) preliminary round was held on 1.10-15.11.2020 and was an individual round;
2) the main round was held on 8.12.2020 and was a team round.

In this study the author is analysing background questions in the preliminary round where 3188 students attended, from which 1791 were boys and 1397 were girls.

CyberDrill 2020 preliminary round consisted of sixteen background questions and thirty main challenges (Appendix 1. Questions for the students). The main topics that background questions covered were about the age, and a language group where they participate. Background questions were divided into three parts:

1. Students' previous experience of IT and cyber defence learning and competitions (2 questions)
2. Self-assessment to solve complex problems (1 question)
3. Interests in cybersecurity and IT issues and field (2 questions)

All the questions were closed-ended questions with combinations of Likert scale [121] and list of options with multiple answers. The survey method provides a good way to gather large amounts of information from a large sample of people. The students study gives an overview of what activities are done with students to teach cybersecurity.

5.1.2 Teacher’s study

Teacher’s study is divided into two data gathering methods: survey and interview. The survey gives a possibility to gather a large amount of data from a large sample of teachers. The interview provides a deeper understanding of the teacher’s point of view about CTF environments and teaching cybersecurity in general education schools.

- Survey (Appendix 2. Survey questions) was held 2021 January and was shared in social media groups (i.e Eesti Informaatikaõpetajad, Küberkaitse teadlikkused tõstmine, Haridustehnoloogid, Nutitund igasse kooli) and sent to all representatives of schools that participated in the CyberDrill 2020 preliminary round and a network of schools that teach cybersecurity and to representatives of national defence schools who participated in the summer school on cyber defence in August 2020. This method gave the possibility to compare results of interested teachers' views whose students were participating on CyberDrill 2020, but also include those opinions and ideas who were not. The survey was conducted from 06.01.2021 - 31.01.2021 with Google Forms platform. The survey contained eight questions about the school’s background, sixteen questions about teaching informatics in schools and twelve questions about cybersecurity competitions and the future. There was a combination of open-ended and closed-ended questions in the survey. The closed-ended questions were combinations of binary answer, scales, list of options with single answer available and list of options with multiple answers, in order to find patterns in how schools are teaching students on cybersecurity related topics. The overall estimated time for completing the survey was 25-30 minutes. The author gave the respondents the opportunity to supplement their answers on several questions. The survey results give an overview of what is taught about cybersecurity in general education schools according to curricula.

- Interviews were conducted with the survey participants, who shared their interest and contacts at the end of the survey. The interviews were held after the survey in March on the dates that were most suitable for the participants. Interviews were performed in Skype conference calls and were recorded for the analysis purpose. The interview (Appendix 3. Questions for the interviews) consisted of three background questions, three questions raised from the preliminary study that needed confirmation and explanations, eleven questions about the CTF environment and a showcase of three environments that the author managed to set up. Additionally, a question about whether the shown environments should be different, if yes, what should be different. The interview questions were mostly open-ended to obtain teachers' opinions about CTF environments. The interview results give an overview of what the school’s needs are for using CTF environments.

The data gathered from CyberDrill 2020 was analysed with a cross-tabulation method, by comparing the question answers by students' gender, age and nationality. For analysing the survey data gathered from the teachers, the author is using percentages and frequency descriptive statistics methods. Most important questions were selected for the analysis. The interviews were analysed using a coding method for the qualitative data, specifically a combination of deductive and inductive coding [122]. For the deductive coding the author used keywords such as “easily accessible”, “simple to use”, “reduction of work for teachers”, “scoreboards” and “statistics”. These predefined sets of codes were the result of the survey analysis, with these predefined codes the author can find answers to the research question “*What are the school's needs for using the environment, for example?*”

5.2 Limitations

This chapter discusses limitations in internal and external validity, reliability and sample profile.

Internal validity - This study relates to those students, schools and teachers who participated in it. It does not give understanding of other schools, students, and teachers. As there were 89 schools, 3188 students, 50 teachers participating that are usually active on CyberDrill, it gives an overview of ideas that schools and teachers who are already more motivated than others to participate in cybersecurity events. Probably the results show a bit nicer image of the challenge, but from that we can see trends also for the other schools as well, who are for now not being active on cybersecurity.

Reliability - The quality of the data from CyberDrill depends on the work that the study group worked out. As the study has been made with different experts, the author is relying on the quality of that. The issue is how to make connections to this data to teachers' data and proposed solutions with CTF use. As students in this study and half of the teachers were participating in the CyberDrill then students and teacher’s data is connected, also as CyberDrill used one of the CTF solutions then this is the second connection to showcase that the data is connected.

Sample profile - Additionally, there is a limitation in choosing respondents for the survey. The survey focus groups were the schools that are consistently participating in the cybersecurity competitions, because that way the author can make connections between CyberDrill results. To showcase different schools' views, connections were made on social media and mailing lists where teachers usually get their IT related information. It is not the ideal channel, but for the teachers they feel comfortable to attend the studies and share their opinions when they are approached via their preferred social network.

External validity - The questions for the survey and interviews were improved by having a test participant complete the survey and give their opinion where improvements were needed.

6 Results and analysis

This chapter gives the results of the students's study, teachers survey and interview. The data gathered is needed for all the research questions. The results are provided in the order of execution.

6.1 Results of the students' study

This chapter gives an overview of data gathered for the second research question (RQ2). The results of the student's study was needed for creating a survey with teachers. During the CyberDrill competition the participants were asked about their opinion and activities towards cybersecurity to get a better overview of what students are doing to learn more about cybersecurity and prepare themselves for participation in cybersecurity competitions

Basic school students were mostly participating in basic computer lessons, IT activities, courses, in extracurricular activity groups and competitions. Only 7% of the Estonian and 4% of the Russian boys who participated in the survey have participated in digital safety or cybersecurity competitions before the CyberDrill. Same goes for the girls, only 9% of the Estonian and 4% of the Russian girls were participating in digital safety or cybersecurity competitions. So, the participants were newcomers to the field.

High School students are mostly participating in basic computer lessons or other IT and robotics extracurricular activity groups. Only 7% of the Estonian and 1% of the Russian boys have participated in digital safety or cybersecurity related competitions in the last two years. Same goes for the girls, only 6% of the Estonian and 2% of the Russian girls have participated in digital safety or cybersecurity related competitions in the last two years. Since digital safety or cybersecurity lessons are not compulsory in basic and high schools, the participation percentages are low.

Besides participating in cybersecurity competitions and computer lessons, the author was also interested in what they are doing in their free time to educate themselves more in cybersecurity related topics. The results show that the basic schools and high school some students stated that they are actively using nonformal ways to educate themselves:

- watching cybersecurity themed videos and lectures online;
- watching cybersecurity themed communities or online channels;
- talking with friends on cybersecurity topics;
- searching for websites to read and news on cybersecurity topics;
- reading cybersecurity-related books;
- participating in cybersecurity e-courses;
- participating in cybersecurity related competitions that are not from the school.

The students show interest in learning more about networking, Windows and Linux servers, Wireshark, Nmap and HoneyPot technologies. Most of the boys see themselves as a normal user or programmer/developer/tester in their future jobs. At the same time girls do not see themselves working in IT related jobs in the future. In addition, it turns out that there is a big difference between the interests of girls and boys. Girls get IT knowledge from school, boys more from their own leisure activities and non-formal education.

In schools, students tend to highlight IT-related activities, with cyber defence only mentioned by participation in competitions. As competitions are held only once a year, as outlined in theory in Chapter 3.2.2, problems in learning the main topics of cyber defence are lack of schools support and formal education versus nonformal education.

It is the responsibility of schools and teachers to guide students into cybersecurity-related activities since they have the power to reach many students at once. However, if they themselves do not provide these activities in the formal education, only a few of the talents who are consistent will be able to do so.

6.2 Results of the teacher's survey

6.2.1 Background of the respondents

The respondents (50) were asked a few introductory questions about the school they represented, to understand the coverage of locations and school levels in Estonia. From the respondents, 16 basic schools from all 306 basic schools (5%), 30 high schools from all 157 high schools (19%) and 4 vocational training centres from all 9 (44%) in Estonia were represented. [123]

Teachers who answered the study were IT teachers and educational technologists with some cybersecurity interest. School teachers rated their technology interest level (example take part in IT projects, do extra work with students etc) - 54% of the schools responded that their interest is on a medium level and 42% on high level, only 4% of the schools were not interested. The survey showed that most of the schools only have one or two IT specialised teachers, one school did not have any fully specialised teachers. In the list one school stated that they have 11 specialised teachers as they have 3000+students. The lack of specialised teaching staff could also explain the relatively low interest levels in IT or cybersecurity related topics and why many school's do not have such courses available in their syllabus. Also, only 16% of teachers ever had experience of CTF competitions themselves as participants and out of all participants 84% schools had experience of students participating on the CTFs (CyberDrill or other). So, the study tells a story of schools that are already open to cybersecurity competitions.

6.2.2 Schools - formal and non-formal education possibilities

In the second part of the survey, the respondents were asked how, to whom, and what topics are taught in the school's computer science lessons. About 62% of the schools have computer science lessons only for selected classes and 30% of the schools have computer science lessons for all the classes. Remaining 8% of the schools do not have any computer science classes but have other activities or lessons. Respondents also report that schools participating in the survey are:

- offering robotics for those who are interested (80%);
- having other IT extracurricular activity groups (40%);
- organizing IT events (44%);

- doing information work in digital safety (60%);
- participating in IT competitions (58%);
- participating in cyber defence competitions (80%).

The survey involved rather digitally active schools, who are participating in the CyberDrill competition. The results give an overview about the situation of the IT oriented schools, not so much about the average Estonian school. The situation is different in the average Estonian school. The good sign is that 80% of these schools have set themselves the goal of participating in cyber defence issues.

Most of the schools teach cybersecurity-related topics in informatics class or in other topics related classes or extracurricular activity groups, which show that currently, schools do not have dedicated classes or extracurricular activity groups for teaching cybersecurity. Only 14% of the schools that participated in the survey have separate cybersecurity related theme classes or extracurricular activity groups and 9% of the schools only teach cybersecurity through participating in special events or competitions. 26% of the schools say that teaching cybersecurity-related topics is common and shared responsibility of all schoolteachers. About 8% of the respondents say that they are not teaching cybersecurity topics in their school.

The most common topics that are taught in schools related to cybersecurity are how to behave safely on the Internet, how to solve a variety of behavioural IT security issues, how to use smart devices and computers safely and how to behave technically safely on the network. The least taught topics were how to technically secure a computer network, how to conduct an entry-level security audit of its operations and equipment and how to solve various technical IT security problems.

6.2.3 Learning environments and materials

Currently, there is a problem that students are interested in cybersecurity topics, but the schools lack resources for preparing the students for the competitions and teach cybersecurity. There is a lack of materials, time, and teachers who have the knowledge and are willing to teach cybersecurity to students. The survey confirms it because these were the most common answers for what are the challenges for schools for participating in IT competitions.

The most common resources are Targalt Internetis [3], Digiõpik [49]and various videos, such as Netilambad and other used resources were cybersecurity-related books, different role games, or their own creations. Some of the vocational schools were using cybersecurity specialized environments such as Rangeforce [100] study environment, Cisco-s network academy cybersecurity course and ITSVET-project [39].

6.2.4 Students' preparation and participation on the CTF-competitions

The survey results show that most of the participant's schools say that their students are interested and would participate again in the CTF competitions. The reasons that were brought out were that the competitions develop students' skills, out-of-the-box thinking, offer a challenge for them, give them positive emotions, and cybersecurity and hacking topics are very interesting for them. The most common reason was that the cybersecurity topic is very vital in current timing.

About 84% of the respondent's schools' students participate in CTF competitions, from which the author concludes that most of the students like to participate in CTF competitions and a lot of them are actively participating in CTF competitions.

At the same time, schools do not prepare students for IT or CTF competitions, instead, they provide students web links and guides so students can prepare themselves independently or they have additional extracurricular activity groups. To keep students interested in IT or cybersecurity topics, schools have additional extracurricular activity groups, they give additional assignments for interested students, offer additional courses such as robotics, or do not have any special activities to support students' interest in IT.

6.2.5 Issues raised

From the data some extra issues were found. First is the gender equality issue: the data in the background shows that girls are contributing themselves to technologies less than boys, and they are also less involved in cybersecurity related activities, so the author asked respondents whether and what specific activities they are doing to involve more girls in IT and cybersecurity. Currently, most schools are doing nothing extra for involving girls in IT and cybersecurity topics because they do not see the need for it. Some respondents even pointed out that girls are interested in these topics, but nothing extra needs to be done. The schools that do, mostly create separate extracurricular activity groups, or organise competitions between girls and boys.

Second is the fraud issue, schools are facing a problem for in-school competitions, which are how to ensure honesty (fair game) and detection of fraud. The survey shows that currently, schools are handling it by having a teacher as an observer and using computers provided by the school.

Third is that the teachers do not have personal experience of the CTFs - most of the respondents said that their most students have participated in CTF competitions, but only 14% of teachers have done so and only 6% of the teachers have set up a CTF competition environment themselves in their school. In the author's opinion, this shows that either the teacher does not have time or needed skills for it. To improve this, the teachers would need a training course for using and setting up CTF environment, which university could provide.

6.2.6 Need for the future materials

Schools need more materials, practical assignments, labs, challenges are needed for teaching cybersecurity in their school. The responses show that most of the schools expect that the informatics curriculum and materials from grades 1-6 and 10-12 will have the cybersecurity module updated, and the cybersecurity module for informatics curriculum from grades 7 to 9 will be created in 5 years. New topics for the curriculum would be a. human aspects b. technical aspects.

For supporting teachers in teaching cybersecurity topics in the next five years, the schools are expecting that there will be:

- supportive reading material created for teachers/parents on talent preparation in cybersecurity topics;
- a separate e-course, the central theme of which is preparation for cyber defence competitions, usable for both teachers and students;

- more assignments added to the central exercise's web page Targalt Internetis [3];
- recommendations for a CTF solution that schools can use themselves, e.g. on their own server;
- a central Estonian CTF solution, which will be available online with the task bank or with the possibility to add new tasks to the application by everyone.

6.2.7 Sustainability of the competitions

Respondents' expectations for the CyberDrill (KüberPuuring) competition for the next 5 years were, the schools:

- would like the preliminary rounds questions and challenges to be created by the universities, while conducting the preliminary round would be the school's responsibility;
- think that the final round should always be conducted online, but some say that having the final round not online would be a very exciting and unique experience;
- suggest that the prizes for the event should remain educational such as experience, pieces of training, but there should also be some little prizes;
- state that they probably will not have a separate cybersecurity course due to lack of time and there is no place for it in the curricula.

The schools agree that in the next five years the topics of cybersecurity importance is growing, and they keep participating in cybersecurity-related competitions. Some schools are even using their resources to participate in various local activities such as Cyberscouts. The survey shows that the schools would keep using national/university solutions for teaching the cybersecurity topics such as exercise portals, study materials and online courses.

6.2.8 Need for the CTF-environment

Most of the schools think that there is a need for a central CTF solution for all schools in Estonia as a central service (see Figure 8).

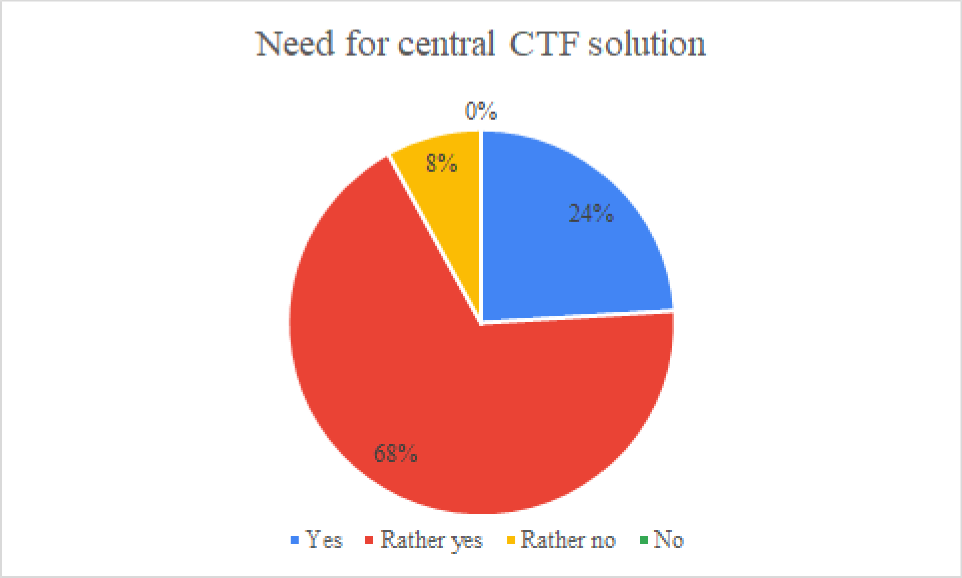


Figure 8. Respondents' opinion on the need for central CTF solution

Since the need is so high, the author is interested in the composition of the central CTF service. The respondents say that the service should:

- be online and the school should not have to deal with the technical side;
- have a possibility to create permanent accounts, which teachers can use;
- the environment should have a leader board.

Additionally, the environment should have an assignment bank with the possibility to add more challenges/questions by teachers and students. Creating a questions packet for competitions should be active for not more than three months, after that it would expire. As the result of completing all the assignments, teachers expect to have the answers sent by email or have access to a result table in the environment.

Overall, the survey shows that schools are interested in having a central CTF solution, so they could have different teaching methods. To get a better overview of teacher's needs the author has conducted interviews with teachers who were interested. In that interview, the author will introduce 3 CTF environments to teachers that would potentially mostly cover their needs that were pointed out in this survey.

6.3 Results and analysis of the teacher’s interview

This chapter gives an overview of data gathered for RQ2, RQ3 and its sub questions.

The interviewees were Informatics teachers (2), educational technologists (3) or other IT related professions (3), who teach students from the age of seven to the age of eighteen. Most of the interviewees agreed with the statement that “cybersecurity related topics are not taught for grades 7.-12., only in extracurricular activity groups” and said that these topics are taught more in vocational training centres or specific courses like part of National Defence studies. In smaller schools there is a problem that the cybersecurity courses will be opened only if there are at least twelve participants, which means that schools that have for example eight or nine interested students in the following topic, they must study it independently or through extracurricular activity groups.

As the survey with teachers showed that students are interested in cybersecurity related topics, but the assortment of the resources is small, for example CTF environments. The participants of the interview agreed that there is a deficit in continuously available CTF environments (a lot of environments have time limits or needs to be set up first) where to practise and said that since this field of study is relatively new, most of the teachers have not looked into it. The reason why teachers are not using CTF environments in their classrooms is that they do not have the skills to set up the environment nor do they have the time to manage the environment. This means that the central CTF environment should be online, and teachers even suggested that the universities should provide the solution for the schools.

6.3.1 Schools needs about the CTF-environment

The CTF environment should have:

- different levels of challenges, easier ones for younger students such as answering questions by searching for the answers from the Internet and harder ones for older students, such as solving problems through command line and having more technical questions;

- cover various topics (shown in Figure 9). The most common topics that teachers pointed out were cryptography, computer security, networking systems and fake data/news;
- contain automatic answer checker and feedback for correct and incorrect answers and have maximum attempt functionality. Results of the challenges should be shown in scoreboard and in diagram form with the possibility to export as a CSV file;
- at least three roles: administrator, teacher, students and one optional role: guest. The role of administrator could manage the whole environment, hand out teacher roles and have the same rights as the teacher role. The role of the teacher could create questions, view students' answers, overall and students' statistics of solving challenges, to have an overview of how their students are doing and what topics they should focus more on. The role of the student could complete the challenges, view notices and their own statistics;
- the possibility to upload and download images, videos and files that are critical for solving the challenge;
- registration of users authenticated and the opportunity to connect with a google account or through a link;
- the possibility that the questions could be easily exported and imported for the teachers, because that would give the teacher an overview of what has been already done and possibility to use ready-made challenges. This functionality would give other researchers an opportunity to gather statistics on what topics are being taught.

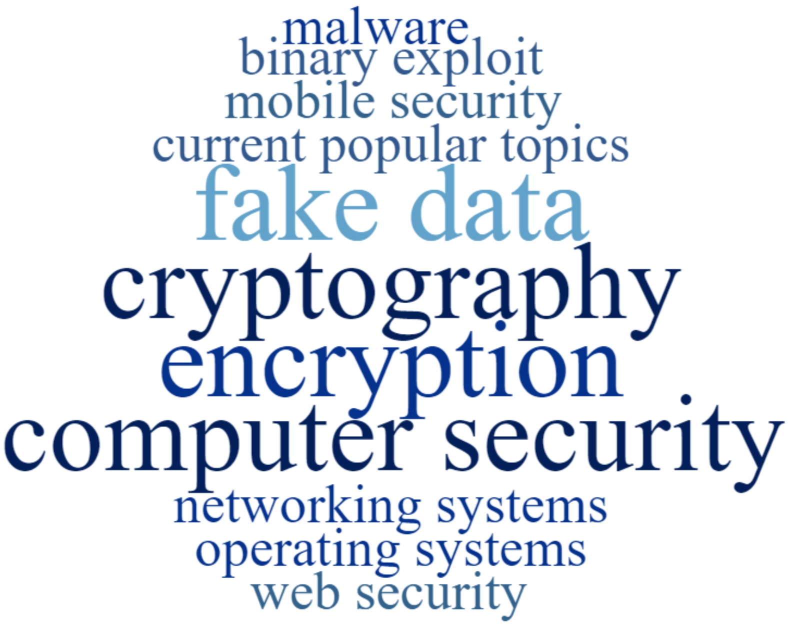


Figure 9. Word cloud of topics a CTF environment should cover

Additionally, not only teachers should have the privilege to create the challenges, but students as well, under the guidance of the teacher. Biggest downside of the current solutions is that there is no information on how to solve the challenges when one wants to learn how to do it - they are missing guidance functionality for solving the challenges.

Some of the interviewees proposed that there should also be a Moodle type of environment as well, where every school would have their own CTF environment and should have the possibility to change the user interface language.

6.3.2 Feedback about the three selected CTF-environment

The feedback for environment named "CTFd" was more positive from the other two environments. Teachers pointed out that the environment was relatively easy to understand, and they would use it as a working tool in their classes. Teachers liked that it was possible to create the challenges inside the environment and there was an opportunity to export and import ready-made challenges. Additionally, the environment showed students results independently.

The feedback for an environment named "picoCTF" showed that the creation of challenges would be too hard for some teachers, because the challenges had to be created in the Python language. Additionally, ready-made challenges were too advanced for the basic and high school students. To solve the example challenges command line skills in Linux were needed.

The feedback for an environment named “ctfspace” showed that some parts of the environments were not understandable, because they were in languages other than English, for example user registration. Some teachers said that the need for a Linux operating system would be a problem in their school. Other than that, they liked the environment because it had only basic features, such as challenge creation, management, and scoreboard.

From the environments that were presented to interview participants “CTFd” was the most popular, since the environment is intuitive and included most of the key requirements that teachers needed, such as students’ statistics and creation of challenges with the environment.

Most CTFs presented were missing challenge guidance functionality, language change functionality and challenges export/import functionality, what was mentioned should be part of the environment. Overall problem that teachers are currently facing is that they do not know how to use available CTF environments.

The solution for the problems would be that the environment should:

- have a guide book;
- have a training course how to set it up (to get hands-on experience and learn how to use and set up the environment correctly);
- spend minimal teachers time on technical side;
- be run by someone else like university or company, that would take that responsibility and take constant care of the environment;
- consider data protection law and necessary measures for it.

Interviews showed that there should be more awareness about CTF amongst the teachers because the teachers have interest in it but lack guidance. Some teachers even asked links to the environments, so they could try to set up and use it themselves.

7 Discussions and recommendations

7.1 Cybersecurity taught in the schools

This chapter discusses research questions number one and two. From the theory we acquired the knowledge that the formal education in Estonia and in the world have only a few cybersecurity curricula in general education, and students are taught more about digital safety. Cybersecurity is being taught mostly in the universities at bachelors and master's level. In Estonia, there is digital safety courses for general education and cybersecurity curricula for high schools, but these are not compulsory, only a few schools are teaching it currently. For non-formal education, the big picture is better. There are a lot of different extracurricular activities for students such as summer camps, cybersecurity events, extracurricular activity groups and cybersecurity competitions. In Estonia, we have different extracurricular activity groups and cybersecurity competitions at least once a year for different education levels. In the students' the results show that cyber defence is taught more through extracurricular activities than through formal general education. Cybersecurity is learned through cybersecurity competitions, hackathons, and materials on the Internet that is nonformal education. The teachers study confirms that they teach cybersecurity more through extracurricular activity groups or send students study materials that they should self-study.

The topics that are taught in general education in the world and in Estonia are:

- digital safety;
- ethics, society and how to be behave correctly;
- basic knowledge of using computer as a student(office tools);
- what are threats and viruses.

The topics that are taught are cryptography, computer forensics and mobile security, but only in vocational schools. These topics are not taught in Estonia's general education because these topics are very specific to cybersecurity and because cybersecurity curricula are optional for schools and students. Nowadays, these topics should be taught because we are moving towards using more smart devices. If these topics are not taught to students, then they cannot do well enough in the information society. Which means the curricula needs content changes, for achieving the goal.

In teaching cybersecurity, the teachers are in the role of structuring learning activities, transferring knowledge and creating learning preconditions and opportunities for students. The students should be active experiencers, interpreters, adapters, and self-directed learners, creative and striving for intellectual growth, self-activity and able to self-evaluate. These properties are part of humanism and cognitivism learning theories. Learning cybersecurity through formal education and laboratories relates to more cognitivism learning theory and learning through CTF competitions more on humanism learning theory.

The situation regarding the acquisition of cybersecurity skills depends on the mandatory nature of the topic. Few deals with it voluntarily, and when they do, it is rather superficial. There are good examples of materials and interested schools in Estonia, but the interested schools are still in a minority.

When we are creating more material for teaching cybersecurity-related topics, we can see problem that the teachers do not have the time and if we create more materials, since they have not worked through available materials, then they would not use them in their classes. On the other hand, if we do no create new materials then the teachers who would take cybersecurity module, would not have enough time and materials to teach cybersecurity-related topics. Currently, teachers mostly teach topics through cognitive learning theory, which is good for acquiring basic knowledge of cybersecurity. But, if we want to move on so that student can could also solve something on their own, we need to teach humanistic values. Which means that student would understand the problem, solve the problem, search solutions for the problem and would discuss it with the teacher. Our teachers probably are not ready for this, although the teachers who participated in the interview showed that they themselves have the initiative and would be willing to cooperate with students.

7.2 Need for CTF environment in schools

This chapter discusses research question number three. The data gathered from the teacher's study shows that there is a need for a central CTF environment, because from theory we could see that learning through gamification or competitions has shown better results than learning by heart. The theory showed that there are some CTF environments that teachers could use in their teachings, but the survey and interview with teachers showed that teachers are lacking the time and skills to set up the environment by themselves. The analysis of the CTF environments and interviews with teachers showed that an environment named "CTFd" would meet their needs for such an environment. But the environment should be set up by the university or other companies since that way the time consumption of teachers could be reduced. Both survey with teachers and interview with teachers showed the environment should have the tools to create challenges, scoreboard, and solutions table. The tools to create challenges should be available for both teachers and students. These environment needs show that teachers are interested in using the central CTF environment and the less they must deal with the technical side the better.

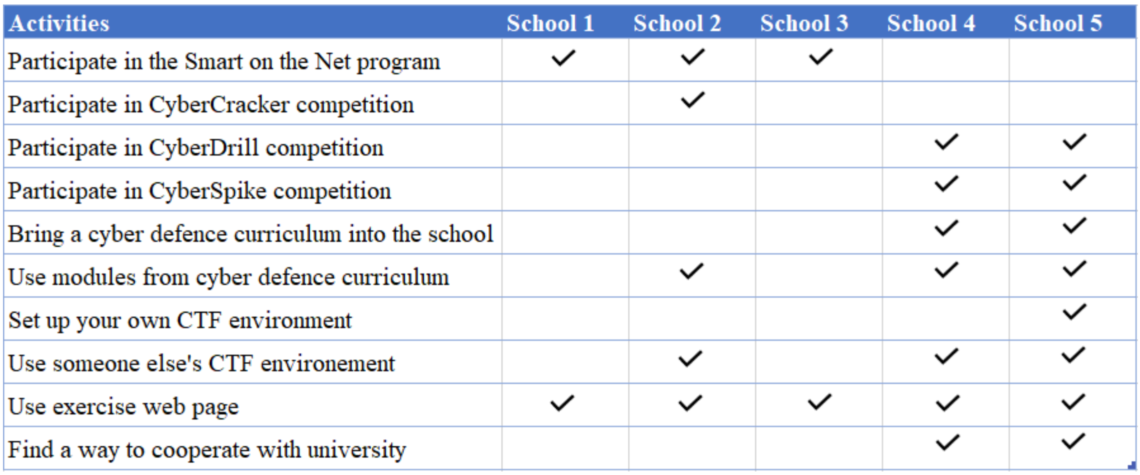
7.3 Summary of discussion

This chapter describes the possibilities on what schools should do to promote cybersecurity education in their school level. To get better overview we have created a table (see Table 3).

To use the table (see Table 3), you should first identify what kind of school you are, from the schools' criteria and what activities you can already do to promote cybersecurity in your school. But if you would like to move up on promoting cybersecurity in your schools, you should follow the criteria for the next school level.

School 1 criteria is that it is basic school, do not have specialized IT teacher and do not have many students interested in cybersecurity. School 2 criteria is that it is basic school, has IT teacher and have many students interested in cybersecurity. School 3 criteria is that it is high school, do not have specialized IT teachers and do not have many students interested in cybersecurity. School 4 criteria is that it is high school, has specialized IT teachers and many students interested in cybersecurity. School 5 criteria is that is vocational training centre with specialized IT teachers.

Table 3. School possibilities in teaching cybersecurity-related topics



Activities	School 1	School 2	School 3	School 4	School 5
Participate in the Smart on the Net program	✓	✓	✓		
Participate in CyberCracker competition		✓			
Participate in CyberDrill competition				✓	✓
Participate in CyberSpike competition				✓	✓
Bring a cyber defence curriculum into the school				✓	✓
Use modules from cyber defence curriculum		✓		✓	✓
Set up your own CTF environment					✓
Use someone else's CTF environement		✓		✓	✓
Use exercise web page	✓	✓	✓	✓	✓
Find a way to cooperate with university				✓	✓

For example, if you identify yourself as School 1 and you want to use CTF environments or use modules from cyber defence curriculum you should hire a specialized IT teachers and work on involving more students in cybersecurity. Overall if the schools want to participate in cybersecurity competitions and use CTF environment they would need IT specialized teachers in their school, to reach higher levels. To have a better workflow or understanding of what the school choices are for promoting cybersecurity among students can been seen in the following flowchart (see Figure 10).

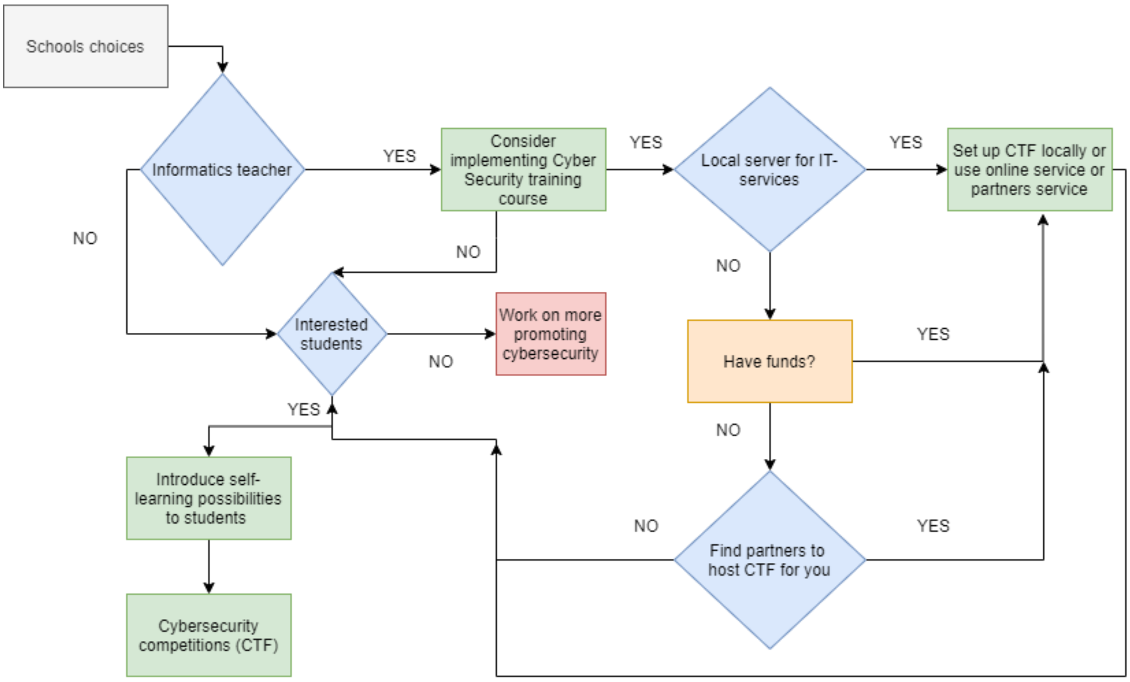

Schools choices
Informatics teacher
YES
NO
Consider implementing Cyber Security training course
YES
Local server for IT-services
YES
Set up CTF locally or use online service or partners service
NO
Interested students
Work on more promoting cybersecurity
NO
NO
Have funds?
YES
YES
Introduce self-learning possibilities to students
NO
NO
Find partners to host CTF for you
YES
Cybersecurity competitions (CTF)

Figure 10. Flowchart for improving their cyber security opportunities for students

The workflow starts with school choices, which would be basic, high school or vocational training centre. The requirements and activities schools can do are:

- First requirement would be if the school has informatics course teacher, the school could consider implementing cybersecurity training course or use modules from existing cybersecurity curriculum. If the school do not have informatics course teacher and have students who are interested in cybersecurity-related topics, school should introduce self-learning possibilities such as Smart on the Net or exercise web page. After learning cybersecurity materials independently, school should promote cybersecurity competitions depending on the student age, such as CyberCracker, CyberDrill and CyberSpike.
- Schools that have implemented cybersecurity training course or module and have local server machines with a person who have the skills to work with it, should set up CTF locally or use online services if they have funds for it. If the schools do not have funds for local server machines, they should find partners such as universities and cybersecurity companies, who would set up the CTF environment. Usually if the school has implemented cybersecurity course have already students interested in the field, for further actions the school should introduce self-learning possibilities and cybersecurity competitions.

- If the school do not have informatics teacher nor interested students, then they should work on more promoting cybersecurity in their school and try to hire informatics teacher.

Following the workflow and activities that school can do for raising cybersecurity learning possibilities, would benefit in competitions and in students further studies. CyberDrill study has shown, that students who are self-learning and school who are offering cybersecurity modules have better results.

7.4 Recommendations

The master's thesis results in several recommendations for different interest groups.

The recommendations for the Estonian government institutions (Ministry of Education and Research, Ministry of Economic Affairs and Communications, Ministry of Defence, CyberCommand, Education and Youth Board):

- support the creation of a central CTF environment for students in basic and high schools;
- create training and guides for teachers for teaching cybersecurity as well as using CTF in their school courses;
- direct more funding towards creating quality learning materials for cybersecurity;
- consider implementing separate programs for attracting girls into cybersecurity field.

Universities and companies that support schools' cybersecurity activities:

- host cybersecurity competitions more often than once a year;
- cooperate with schools to teach cybersecurity-related topics and share upper-level competencies to teachers and students;
- help government institutions to develop qualitative content for learning, competitions and CTF-solutions to be co-used.

For CTF-service providers who are interested in creating or modifying existing CTF environments, it is suggested that:

- environment should be online based, so that the teachers and students could use it any time;
- to keep the environment up to date with new exercises and that young talents would not take it down;
- environment should have the possibility to change languages (EST, RU, ENG);
- to create a complete guide on how to use and set up a CTF environment.

The recommendations for schools and teachers:

- include more cybersecurity-related topics in their syllabus;
- implement cybersecurity course if possible;
- promote more cybersecurity competitions among students and direct them to take interest of cybersecurity self-study for future studies;
- host a CTF environment when possible.

For parents:

- demand IT- and cybersecurity-related modules delivered via schools or professionals;
- promote more cybersecurity competitions among students and direct them to take interest of cybersecurity.

For students:

- take time to keep learning cybersecurity related topics using e-learning possibilities;
- find opportunities to participate cybersecurity competitions, visit IT-companies, learn about admissions to university IT-related programmes;
- try to create or set up a CTF environment if it is interesting to you and you have the means and skills to do it.

8 Summary

Cybersecurity can be learned in schools, by participating in cybersecurity competitions, summer camps or learning the topics with online courses. In formal education, cybersecurity is usually taught at the university level. In Estonia there are digital safety courses for basic schools and cybersecurity curriculum for high schools. Since Estonian schools have the autonomy to choose what kind of elective course, they teach in addition to the national education curriculum, there are only a few schools who teach cybersecurity. Mostly basic schools and high schools are teaching digital safety topics such as how to protect your digital device, health risks, virtual identity management, public and private communication and safe use of smart devices and other digital equipment. Since only a few of the schools are teaching cybersecurity in general education, students mostly acquire the knowledge through non-formal education.

Learning cybersecurity through formal education is not the only option for students. There are a lot of cybersecurity extracurricular activities around the world starting from the summer camps and extracurricular activity groups all the way to cybersecurity competitions. The students' study showed that they are actively participating in cybersecurity competitions and learning cybersecurity through online material.

Studies with teachers have shown that there is a need for a CTF environment where students could practice for upcoming cybersecurity competitions. Teachers are in a need for a central online CTF environment, which would be available all the time. They suggest that the CTF environment should have a challenge creation functionality, user management functionality, scoreboard, and statistics functionality. The environment should also have a complete guide on how to use and set up one, or universities and companies would provide training for it. Currently there is only one option for creating and using a CTF environment, which is to have it created by another school, university or company and it is usable online and on mobile devices.

With work performed in this paper, the author has given an overview of current situation of cybersecurity education and the needs for creating a central CTF environment. For further study it is recommended to create a central CTF environment and gather data how this method has improved cybersecurity awareness among students.

References

[1] R. Garris, R. Ahlers and J. . E. Driskell, “Games, motivation, and learning: A research and practice model,” vol. 4, no. 33, pp. 441-467, December 2002.

[2] “Põhikooli riiklik õppekava,” RT I, 29.08.2014, 20.

[3] “Targalt Internetis,” [Online]. Available: https://www.targaltinternetis.ee/projektist/. [Accessed 11. December 2019].

[4] T. Sõmer, B. Lorenz, S. Mäses and T. Muulma, Küberkaitse, 2019.

[5] TalTech, “Bachelor´s studies. Cyber Security Engineering.,” [Online]. Available: https://www.taltech.ee/en/cyber-security-engineering?_ga=2.245796940.997633118.1619007056-1396101849.1609337542. [Accessed 11. December 2019].

[6] TalTech, “Master´s studies. Cyber Security.,” [Online]. Available: https://www.taltech.ee/en/cyber-security. [Accessed 11. December 2019].

[7] KüberNööpnõel. [Online]. Available: https://sites.google.com/view/kyberpahkel/kübernööpnõel. [Accessed 11. December 2019].

[8] KüberPähkel. [Online]. Available: https://sites.google.com/view/kyberpahkel/. [Accessed 11. December 2019].

[9] KüberPuuring. [Online]. Available: https://sites.google.com/view/kyberolympia/ajalugu/võistlus-2020/küberpuuring. [Accessed 21. April 2021].

[10] KüberNaaskel. [Online]. Available: https://sites.google.com/view/kyberolympia/avaleht. [Accessed 21. April 2021].

[11] “Magic CTF,” [Online]. Available: https://sites.google.com/view/kyberolympia/2021/magic-ctf. [Accessed 21. April 2021].

[12] European Cyber Security Challenge, [Online]. Available: https://ecsc.eu/ . [Accessed 21. April 2021].

[13] L. McDaniel, E. Talvi and B. Hay, “Capture the Flag as Cyber Security Introduction,” in *49th Hawaii International Conference on System Sciences (HICSS)*, 2016.

[14] A. S. Namin, Z. Aguirre-Muñoz and K. S. Jones, “Teaching Cyber Security through Competition: An Experience Report about a Participatory Training Workshop,” 2016.

[15] K. Boopathi, S. Sreejith and A. Bithin, “Learning Cyber Security Through Gamification,” *Indian Journal of Science and Technology,* vol. 8, no. 7, p. 642–649, 2015.

[16] Majandus- ja Kommunikatsiooniministeerium, “Küberturvalisuse Strateegia 2019-2022,” [Online]. Available: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019_vv-s_kinnitatud.docx. [Accessed 21. April 2021].

[17] P. Pernik, J. Wojtkowiak and A. Verschoor-Kirss, “National Cyber Security Organisation: United States,” CCDCOE, Tallinn, 2016.

[18] Government of Japan, “Cybersecurity Strategy,” 2018. [Online]. Available: https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf. [Accessed 21. April 2021].

[19] Australian Government, “Cyber Security Strategy,” 2009. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Australia_2009_AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf. [Accessed 21. April 2021].

[20] European Union Agency for Network and Information Security, “Enisa Strategy 2016-2020,” 2016. [Online]. Available: https://www.enisa.europa.eu/publications/corporate/enisa-strategy/view. [Accessed 21. April 2021].

[21] Secretariat of the Security Committee, “Finland's Cyber Security Strategy,” 2013. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Finland_2013_s_Cyber_Security_Strategy.pdf . [Accessed 21. April 2021].

[22] Government of the Republic of Lithuania, “Resolution on the approval of the national cyber security strategy,” 13. August 2018. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/LRV+818+National+Cyber+Security+Strategy+%28Lithuania%29.pdf. [Accessed 21. April 2021].

[23] The National Post and Telecom Agency, “Strategy to improve Internet security in Sweden,” 4. July 2006. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Sweden_2006_Strategy_Internet_security_2006_12_July_2006.pdf. [Accessed 21. April 2021].

[24] Majandus- ja Kommunikatsiooniministeerium, “Küberturvalisuse programm aastateks 2021-2024,” March 2020. [Online]. Available: https://www.rahandusministeerium.ee/system/files_force/document_files/kuberturvalisuse_programm_2021-2024_seisuga_marts_2020.pdf?download=1. [Accessed 21 April 2021].

[25] European Commission, “DigComp,” [Online]. Available: https://ec.europa.eu/jrc/en/digcomp. [Accessed 21 April 2021].

[26] Haridus- ja Noorteamet, “Õppija digipädevusmudel,” [Online]. Available: https://digipadevus.ee/oppija-digipadevusmudel/. [Accessed 21. April 20201].

[27] Eesti Koostöö Kogu, Eesti Haridusfoorum, Haridus- ja Teadusministeerium, “Eesti elukestva õppe strateegia 2020,” 2014. [Online]. Available: https://www.hm.ee/sites/default/files/strateegia2020.pdf. [Accessed 21. April 2021].

[28] Haridus- ja Teadusministeerium, “Haridusvaldkonna arengukava 2021-2035,” [Online]. Available: https://www.hm.ee/sites/default/files/eesti_haridusvaldkonna_arengukava_2035_seisuga_2020.03.27.pdf. [Accessed 21. April 2021].

[29] T. Rüütmann, Inseneripedagoogika : STEM valdkonna õppeainete mõjus õpetamine ja õppimine. II, Tallinn: Tallinna Tehnikaülikooli kirjastus, 2019.

[30] Australian Cyber Security Growth Network, “Education map,” [Online]. Available: https://www.austcyber.com/resources/dashboards/education-map. [Accessed 21. April 2021].

[31] European Union Agency for Network and Information Security, “Cybersecurity Higher Education Database,” [Online]. Available: https://www.enisa.europa.eu/topics/cybersecurity-education/education-map. [Accessed 21. April 2021].

[32] Study in the USA, “Cyber Security,” [Online]. Available: https://www.studyusa.com/en/field-of-study/511/cyber-security. [Accessed 21. April 2021].

[33] Technical University of Denmark, “Cyber security,” [Online]. Available: https://www.dtu.dk/english/education/continuing-education/master-programmes/cyber-security. [Accessed 21. April 2021].

[34] University of Turku, “Master's Degree Programme in Information and Communication Technology: Cyber Security,” [Online]. Available: https://www.utu.fi/en/study-at-utu/masters-degree-programme-in-information-and-communication-technology-cyber-security. [Accessed 21. April 2021].

[35] Vilnius Gedmininas Technical University, “Information and Information Technologies Security : Masters studies,” [Online]. Available: https://vilniustech.lt/studies/study-programmes/master-study-programmes/317411?element_id=317413&sp_id=44&f_id=4&qualification=a%3A1%3A%7Bi%3A0%3Bs%3A1%3A%22M%22%3B%7D. [Accessed 21. April 2021].

[36] G. Jin, M. Tu, T.-H. Kim, J. Heffron and J. White, “Game based Cybersecurity Training for High School Students,” in *the 49th ACM Technical Symposium*, 2018.

[37] Georgia Institute of Technology, “Online Master of Science in Cybersecurity - Curriculum,” [Online]. Available: https://pe.gatech.edu/degrees/cybersecurity/curriculum. [Accessed 21. April 2021].

[38] Maryville University, “Online Bachelor's in Cybersecurity Curriculum,” [Online]. Available: https://online.maryville.edu/online-bachelors-degrees/cyber-security/curriculum/. [Accessed 21. April 2021].

[39] “ITSVET-project,” [Online]. Available: http://itsvet-project.eu/. [Accessed 21. April 2021].

[40] Lower Dauphin School District, “High School Curriculum,” [Online]. Available: https://www.ldsd.org/Page/15517. [Accessed 21. April 2021].

[41] Carr Hill High School, “Year 10 Information Presentation 2020,” [Online]. Available: https://www.carrhillschool.com/curriculum/year-10. [Accessed 21. April 2021].

[42] The Committee on European Computing Education (CECE), “Informatics Education in Europe: Are We All In The Same Boat?,” 2017.

[43] Pärnumaa Kutsehariduskeskus, “IT-turvaspetsialist,” [Online]. Available: https://www.hariduskeskus.ee/index.php/koik-erialad/kutsekeskharidusope-4/897-it-turvaspets. [Accessed 21. April 2021].

[44] RT I, 14.04.2020, 3, “Info- ja kommunikatsioonitehnoloogia erialade riiklik õppekava,” RT I, 14.04.2020, 3.

[45] cyVETsecurity, “Küberturvalisuse õppekava”.

[46] “Gümnaasiumi riiklik õppekava,” RT I, 29.08.2014, 21.

[47] “Põhikooli riiklik õppekava. Lisa 10.,” RT I, 14.01.2011, 1, 2011.

[48] Hariduse Infotehnoloogia Sihtasutus, “Kontseptsioon: Uued õppeteemad põhikooli informaatika ainekavas nüüdisaegsete IT-oskuste omandamise toetamiseks,” 2017. [Online]. Available: https://drive.google.com/file/d/0B1-0pZFgjFnQX29Gb0ZYb1FMc0k/view. [Accessed 21. April 2021].

[49] Tartu Ülikooli arvutiteaduse instituut, “Informaatika digiõpik I ja II kooliastmele,” [Online]. Available: https://courses.cs.ut.ee/t/digiopik/. [Accessed 21. April 2021].

[50] “Valikõppeaine/valikkursus "Küberkaitse" ainekava,” 2017. [Online]. Available: https://onedrive.live.com/view.aspx?resid=7B5915FDC0CD4BE4!9609&ithint=file%2cdocx&authkey=!AGo9f4nh7CguAjI. [Accessed 21. April 2021].

[51] Kärla Põhikool, “Informaatika ainekava,” 10. December 2019. [Online]. Available: https://kpk.edu.ee/sites/kpk.edu.ee/files/informaatika_ainekava.pdf. [Accessed 21. April 2021].

[52] Ääsmäe Põhikool, “Informaatika ainekava,” [Online]. Available: https://www.aasmaekool.ee/wp-content/uploads/2016/09/Valikaine-Informaatika-PDF.pdf. [Accessed 21 April 2021].

[53] Viimsi Kool, “Informaatika ainekava,” [Online]. Available: https://viimsi.edu.ee/wp-content/uploads/2020/01/informaatika.pdf. [Accessed 21. April 2021].

[54] Vasalemma Põhikool, “Informaatika ainekava,” [Online]. Available: https://www.vask.edu.ee/wp/wp-content/uploads/2016/01/Informaatika-karj%c3%a4%c3%a4ri%c3%b5petus.pdf. [Accessed 21. April 2021].

[55] Vastseliina Gümnaasium, “Multimeedia ja küberkaitse õppekava,” 2018. [Online]. Available: http://www.vastseliina.edu.ee/wp-content/uploads/2018/10/Multimeedia-ja-k%C3%BCberkaitse-3.klass_.pdf. [Accessed 21. April 2021].

[56] Põltsamaa Ühisgümnaasium, “Küberkaitse õppesuuna õppekava,” 2018. [Online]. Available: https://www.poltsamaa.edu.ee/sites/poltsamaa.edu.ee/files/kuberkaitse_oppesuuna_oppekava_2018.pdf. [Accessed 21. April 2021].

[57] Põltsamaa Ühisgümnaasium, “Küberkaitse- infotehnoloogia (IT) õppesuuna õppekava,” 2021. [Online]. Available: https://poltsamaa.edu.ee/sites/poltsamaa.edu.ee/files/ainekavad/kuber_it_oppekava_2021.pdf. [Accessed 21. April 2021].

[58] Rocca al Mare Kool, “Valikained 2017/2018,” [Online]. Available: https://ramkool.edu.ee/wp-content/uploads/2015/08/Valikained-2017_2018.pdf. [Accessed 21. April 2021].

[59] Jõhvi Gümnaasium, “Valikained,” [Online]. Available: https://johvig.ee/valikained. [Accessed 21. April 2021].

[60] Tallinna Laagna Gümnaasium, “Põhikooli ja Gümnaasiumi Õppekava,” 2020. [Online]. Available: https://laagna.tln.edu.ee/wp-content/uploads/2021/02/1-2-69-1-Lisa-Laagna-Gumnaasiumi-oppekava-2020.pdf. [Accessed 21. April 2021].

[61] Pärnu Rääma Põhikool, “Informaatika põhikooli ainekava,” [Online]. Available: https://raama.ee/sites/raama.ee/files/dokumendid/oppekavad/valikaine_informaatika_ainekava.pdf. [Accessed 21. April 2021].

[62] Ridala Põhikool, “Valikaine informaatika,” [Online]. Available: http://www.ridala.edu.ee/wp/wp-content/uploads/2018/02/Lisa-10-Valikaine-INFORMAATIKA.pdf. [Accessed 21. April 2021].

[63] Tartu Kristjan Jaak Petersoni Gümnaasium, “Õppekava,” [Online]. Available: https://kjpg.tartu.ee/sites/kjpg.tartu.ee/files/kjpg_oppekava_2019-20201.pdf. [Accessed 21. April 2021].

[64] Järveküla Kool, “Järvekülla Kooli informaatika ainekava,” [Online]. Available: https://jarvekyla.edu.ee/wp-content/uploads/2019/01/J%C3%A4rvek%C3%BCla-Kooli-informaatika-ainekava_HM.pdf. [Accessed 21. April 2021].

[65] Rapla Gümnaasium, “Rapla Gümnaasiumi õppekava,” 2020. [Online]. Available: https://cloud7g.edupage.org/cloud/RG_oppekava_2020_11_kodulehele.pdf?z%3A9GckFuWSQtz235JAdnmGIyJBLajkO40%2F4Lst6a5dKjWQIKb9Jtes63jKDOjpjw73. [Accessed 21. April 2021].

[66] R. S. Cheung, J. P. Cohen, H. Z. Lo, F. Elia and V. Carrillo-Marquez, “Effectiveness of Cybersecurity Competitions,” [Online]. Available: https://www.josephpcohen.com/papers/seccomp.pdf. [Accessed 21. April 2021].

[67] C. Herr and D. Allen, “Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors,” in *SIGMIS-CPR '15: 2015 Computers and People Research Conference*, California, 2015.

[68] Hacker Highschool, [Online]. Available: https://www.hackerhighschool.org. [Accessed 21. April 2021].

[69] National Initiative for Cybersecurity Careers and Studies, “Cybersecurity in the Classroom,” [Online]. Available: https://niccs.cisa.gov/formal-education/integrating-cybersecurity-classroom. [Accessed 21. April 2021].

[70] Virginia Cyber Range, “Introduction to Cybersecurity for High School Students and K12 Educators,” [Online]. Available: https://www.virginiacyberrange.org/courseware/introduction-cybersecurity-high-school-students-and-k12-educators. [Accessed 21. April 2021].

[71] GenCyber, “2021 GenCyber Camps,” [Online]. Available: https://www.gen-cyber.com/camps/. [Accessed 21. April 2021].

[72] NYU Tandon School of Engineering, “Computer Science for Cyber Security (CS4CS),” [Online]. Available: https://engineering.nyu.edu/academics/programs/k12-stem-education/nyc-based-programs/computer-science-cyber-security-cs4cs. [Accessed 21. April 2021].

[73] Denmark Technical College, “CyberSTEM Camp 2019,” [Online]. Available: https://www.denmarktech.edu/cyberstem-camp-2019/. [Accessed 21. April 2021].

[74] Air Force Association's, “What is CyberPatriot?,” [Online]. Available: https://www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx. [Accessed 11. May 2021].

[75] Major League Hacking, [Online]. Available: https://mlh.io/about. [Accessed 21. April 2021].

[76] DEFCON, [Online]. Available: https://www.defcon.org/. [Accessed 21. April 2021].

[77] Euorpean Cyber Security Challenge, “Euorpean Cyber Security Challenge Curricula,” September 2019. [Online]. Available: ecsc.eu/about/ecsccurricula.pdf/download. [Accessed 21. April 2021].

[78] Carnegie Mellon University, “About picoCTF,” [Online]. Available: https://picoctf.com/about. [Accessed 21. April 2021].

[79] CTFtime, [Online]. Available: https://ctftime.org/. [Accessed 21. April 2021].

[80] CodeHS, “Introduction to Cybersecurity (Vigenere),” [Online]. Available: https://codehs.com/course/introcyber_vig/overview. [Accessed 21. April 2021].

[81] Global Cyberlympics, [Online]. Available: https://www.cyberlympics.org/. [Accessed 21. April 2021].

[82] National Collegiate Cyber Defense Competition, [Online]. Available: http://www.nationalccdc.org/. [Accessed 21. April 2021].

[83] The National Cyber League, [Online]. Available: https://nationalcyberleague.org/. [Accessed 21. April 2021].

[84] Cyber Quests, [Online]. Available: [https://uscc.cyberquests.org/. [Accessed 21. April 2021].

[85] US Cyber Challenge, [Online]. Available: https://www.uscyberchallenge.org/. [Accessed 21. April 2021].

[86] SANS, “DFIR NetWars and Continuous,” [Online]. Available: https://www.sans.org/cyber-ranges/netwars-tournaments/digital-forensics-incident-response/. [Accessed 21. April 2021].

[87] Panoply, [Online]. Available: http://www.cyberpanoply.com/. [Accessed 21. April 2021].

[88] CyberPatriot, “The National Youth Cyber Education Program,” [Online]. Available: https://www.uscyberpatriot.org/competition/Competition-Overview/competition-overview. [Accessed 21. April 2021].

[89] PACKETWARS(TM), [Online]. Available: http://packetwars.com/about-packetwars. [Accessed 21. April 2021].

[90] International Collegiate Cyber Defense Invitational, [Online]. Available: https://iccdi.org/. [Accessed 21. April 2021].

[91] Digital Forensics Security Treasure Hunt, [Online]. Available: http://digitalforensics.securitytreasurehunt.com/. [Accessed 21. April 2021].

[92] Shellphish, “iCTF: the International Capture The Flag Competition,” [Online]. Available: https://ictf.cs.ucsb.edu/. [Accessed 21. April 2021].

[93] National Cyber Analyst Challenge & Conference, [Online]. Available: https://cyberanalystchallenge.org/phases/. [Accessed 21. April 2021].

[94] Technology Student Association, “Cybersecurity Competition,” [Online]. Available: https://tsaweb.org/competitions-programs/tsa/cybersecurity-competition. [Accessed 21. April 2021].

[95] Department of Energy's CyberForce Competition, [Online]. Available: https://cyberforcecompetition.com/. [Accessed 21. April 2021].

[96] Küberring, “Õppekava,” [Online]. Available: https://xn--kberring-65a.com/oppekava.html. [Accessed 21. April 2021].

[97] Noored Progejad, “Õppekava,” [Online]. Available: https://nooredprogejad.ee/ithuviring/oppekava. [Accessed 21. April 2021].

[98] Euroopa Komisjon, “Lastele parema interneti loomise Euroopa strateegia,” 2012. [Online]. Available: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52012DC0196&from=EN . [Accessed 21. April 2021].

[99] Safer Internet Day, “Estonian Safer Internet Centre - Smartly on the Web,” 7. January 2021. [Online]. Available: https://www.saferinternetday.org/in-your-country/estonia. [Accessed 21. April 2021].

[100] RangeForce, [Online]. Available: https://www.rangeforce.com/. [Accessed 21. April 2021].

[101] Hack The Box, [Online]. Available: https://www.hackthebox.eu/. [Accessed 21. April 2021].

[102] The NATO Cooperative Cyber Defence Centre of Excellence, “Locked Sheilds,” [Online]. Available: https://ccdcoe.org/exercises/locked-shields/. [Accessed 21. April 2021].

[103] A. Knowles, “Behind the Scenes at a Capture the Flag (CTF) Competition,” SecurityIntelligence, 8. December 2016. [Online]. Available: https://securityintelligence.com/behind-the-scenes-at-a-capture-the-flag-ctf-competition/. [Accessed 21. April 2021].

[104] Team Probably, “What is CTF?,” Medium, 8. April 2019. [Online]. Available: https://medium.com/@teamprobably/what-is-ctf-d5871a791e24. [Accessed 21. April 2021].

[105] CyberVista, “Capture the Flag (CTF): A Gamification of Cybersecurity Learning,” 29. October 2019. [Online]. Available: https://certify.cybervista.net/capture-the-flag-a-gamification-of-cybersecurity-learning/. [Accessed 21. April 2021].

[106] V. Vizz, “What is CTF(Capture the flag) for Beginners,” Medium, 30. November 2018. [Online]. Available: https://medium.com/@vyshnavvizz/what-is-ctf-capture-the-flag-for-beginners-e79552a2e529. [Accessed 21. April 2021].

[107] “What is Capture the Flag?,” [Online]. Available: https://ctfd.io/whats-a-ctf/. [Accessed 21. April 2021].

[108] “SecGen,” GitHub, [Online]. Available: https://github.com/cliffe/SecGen. [Accessed 21. April 2021].

[109] “pwntools,” GitHub, [Online]. Available: https://github.com/Gallopsled/pwntools.

[110] “librectf,” GitHub, [Online]. Available: https://github.com/easyctf/librectf. [Accessed 21. April 2021].

[111] “hack-the-arch,” GitHub, [Online]. Available: https://github.com/mcpa-stlouis/hack-the-arch. [Accessed 21. April 2021].

[112] “RootTheBox,” GitHub, [Online]. Available: https://github.com/moloch--/RootTheBox. [Accessed 21. April 2021].

[113] “mkCTF,” GitHub, [Online]. Available: https://github.com/koromodako/mkctf. [Accessed 21. April 2021].

[114] “mellivora,” GitHub, [Online]. Available: https://github.com/Nakiami/mellivora. [Accessed 21. April 2021].

[115] “NightShade,” GitHub, [Online]. Available: https://github.com/UnrealAkama/NightShade. [Accessed 21. April 2021].

[116] “fbctf,” GitHub, [Online]. Available: https://github.com/facebook/fbctf. [Accessed 21. April 2021].

[117] Y. Pan, S. Mishra and D. Schwartz, “Gamifying Course Modules for Entry Level Students,” in *SIGCSE '17: The 48th ACM Technical Symposium on Computer Science Education*, Seattle, Washington, 2017.

[118] “CTFd,” GitHub, [Online]. Available: https://github.com/CTFd/CTFd. [Accessed 21. April 2021].

[119] “picoCTF,” GitHub, [Online]. Available: https://github.com/picoCTF/picoCTF. [Accessed 21. April 2021].

[120] “ctfspace,” GitHub, [Online]. Available: https://github.com/puilp0502/ctfspace. [Accessed 21. April 2021].

[121] S. Jamieson, “Likert scale,” Britannica, [Online]. Available: https://www.britannica.com/topic/Likert-Scale. [Accessed 21. April 2021].

[122] A. Medelyan, “Coding Qualitative Data: How to Code Qualitative Research,” Insights Thematic, [Online]. Available: https://getthematic.com/insights/coding-qualitative-data/. [Accessed 11. May 2021].

[123] Haridus- ja Teadusministeerium, “Tähtsad tegevused 2020/2021. õppeaastal,” [Online]. Available: https://www.hm.ee/sites/default/files/htm_koolialgusepakett_a4_2020-2021_viimane.pdf. [Accessed 21. April 2021].

Appendix 1. Questions for the students

Millises klassis õpid?

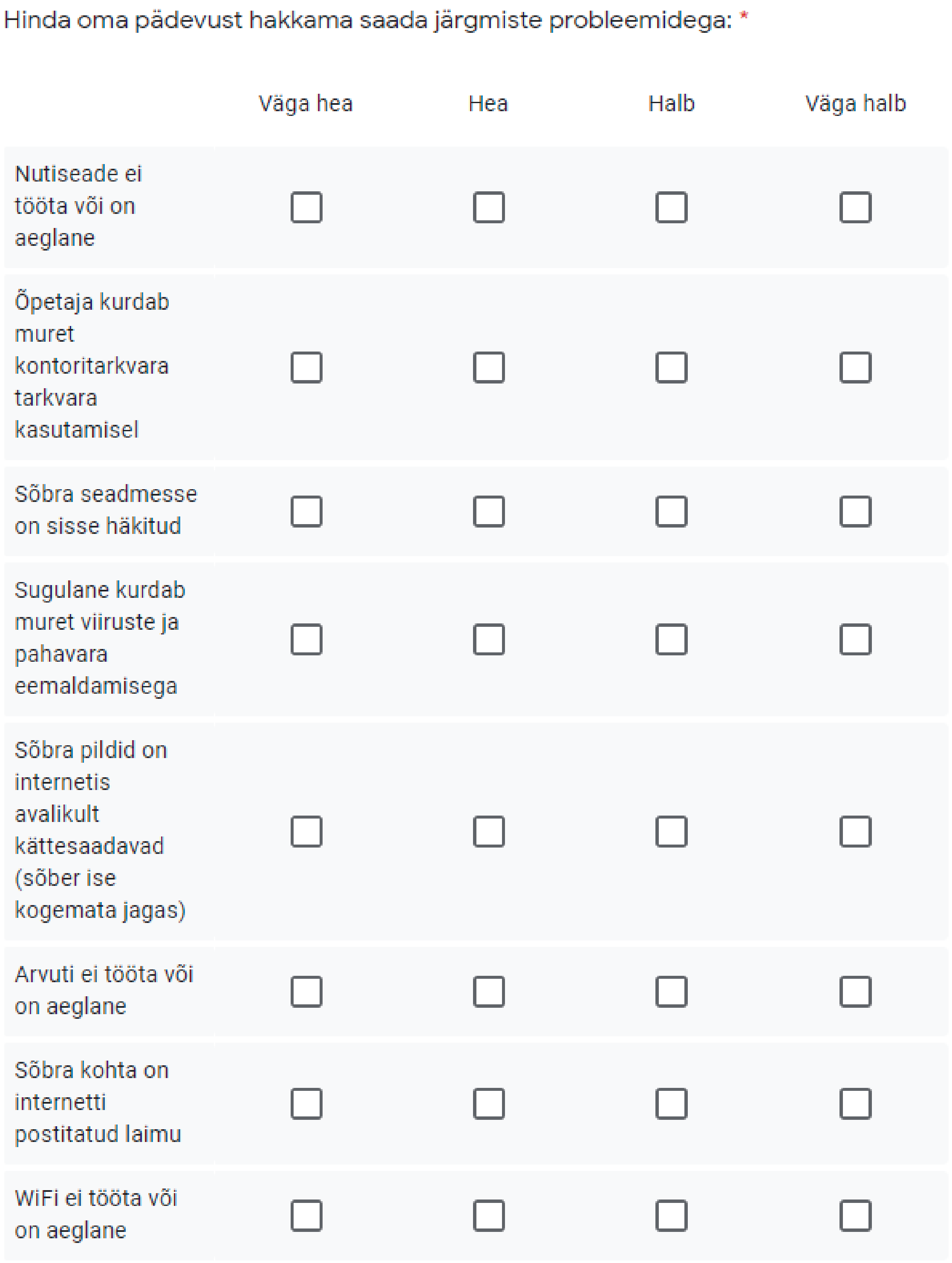
- 7
- 8
- 9
- 10
- 11
- 12
- kutsekool
- muu

Oled

- mees
- naine

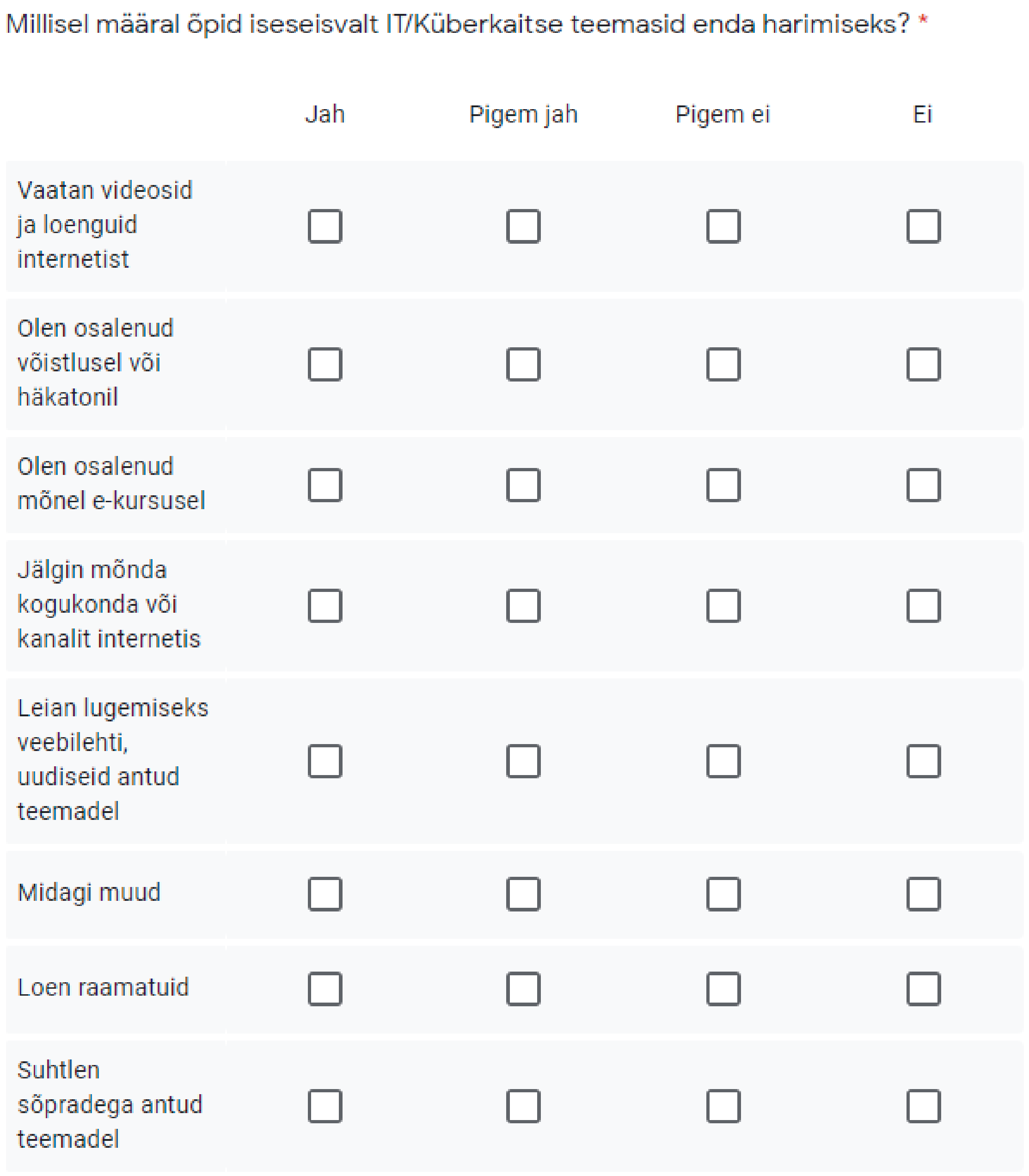
Oled viimasel kahel aastal osalenud:

- Programmeerimise tunnis/ringis
- Milleski muus IT/küberkaitse teemal
- Digitaalse ohutuse/küberkaitse võistlusel/uuringus
- IT teemalistes loengutes koolist suunatuna
- Robootika tunnis või ringis
- Mitte üheksi nendes tegevustes
- Arvutitunnis
- Robotexil või Noorel meistril võistlustel osalejana
- 3D, VR või muude uute tehnoloogiate tunnis, ringis
- IT teemalisel võistlusel
- Robotexil või Noorel Meistril pealtvaatajana
- Küberkaitse kursusel/ringis
- Interneti turvalisust puudutavatel üritustel/tegevustes
- Ekskursioonil IT ettevõttes
- Häkatonil koolist suunatuna
- Muu:



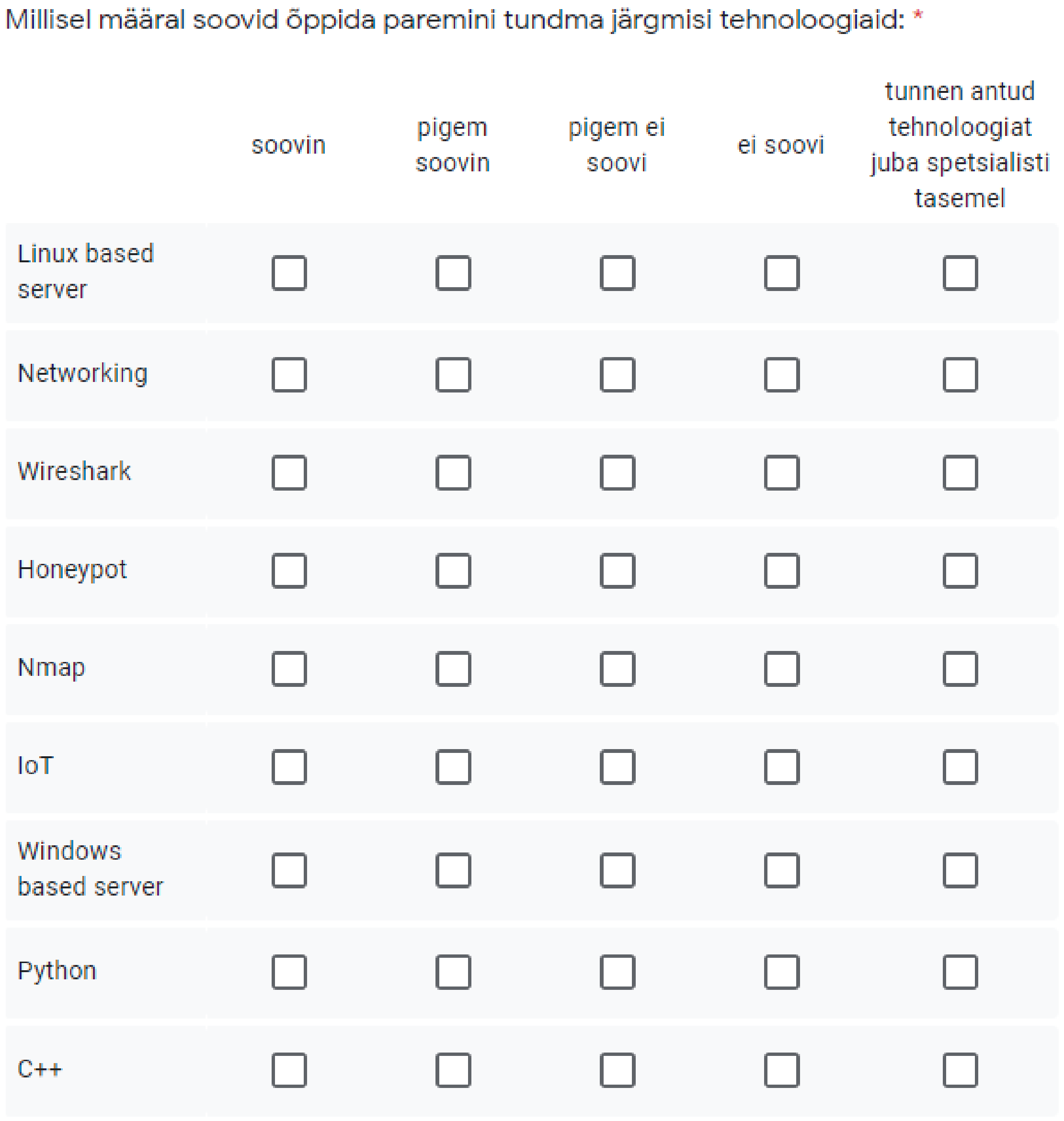
Hinda oma pädevust hakkama saada järgmiste probleemidega: *

	Väga hea	Hea	Halb	Väga halb
Nutiseade ei tööta või on aeglane	□	□	□	□
Õpetaja kurdab muret kontoritarkvara tarkvara kasutamisel	□	□	□	□
Sõbra seadmesse on sisse häkitud	□	□	□	□
Sugulane kurdab muret viiruste ja pahavara eemaldamisega	□	□	□	□
Sõbra pildid on internetis avalikult kättesaadavad (sõber ise kogemata jagas)	□	□	□	□
Arvuti ei tööta või on aeglane	□	□	□	□
Sõbra kohta on internetti postitatud laimu	□	□	□	□
WiFi ei tööta või on aeglane	□	□	□	□



Millisel määral õpid iseseisvalt IT/Küberkaitse teemasid enda harimiseks? *

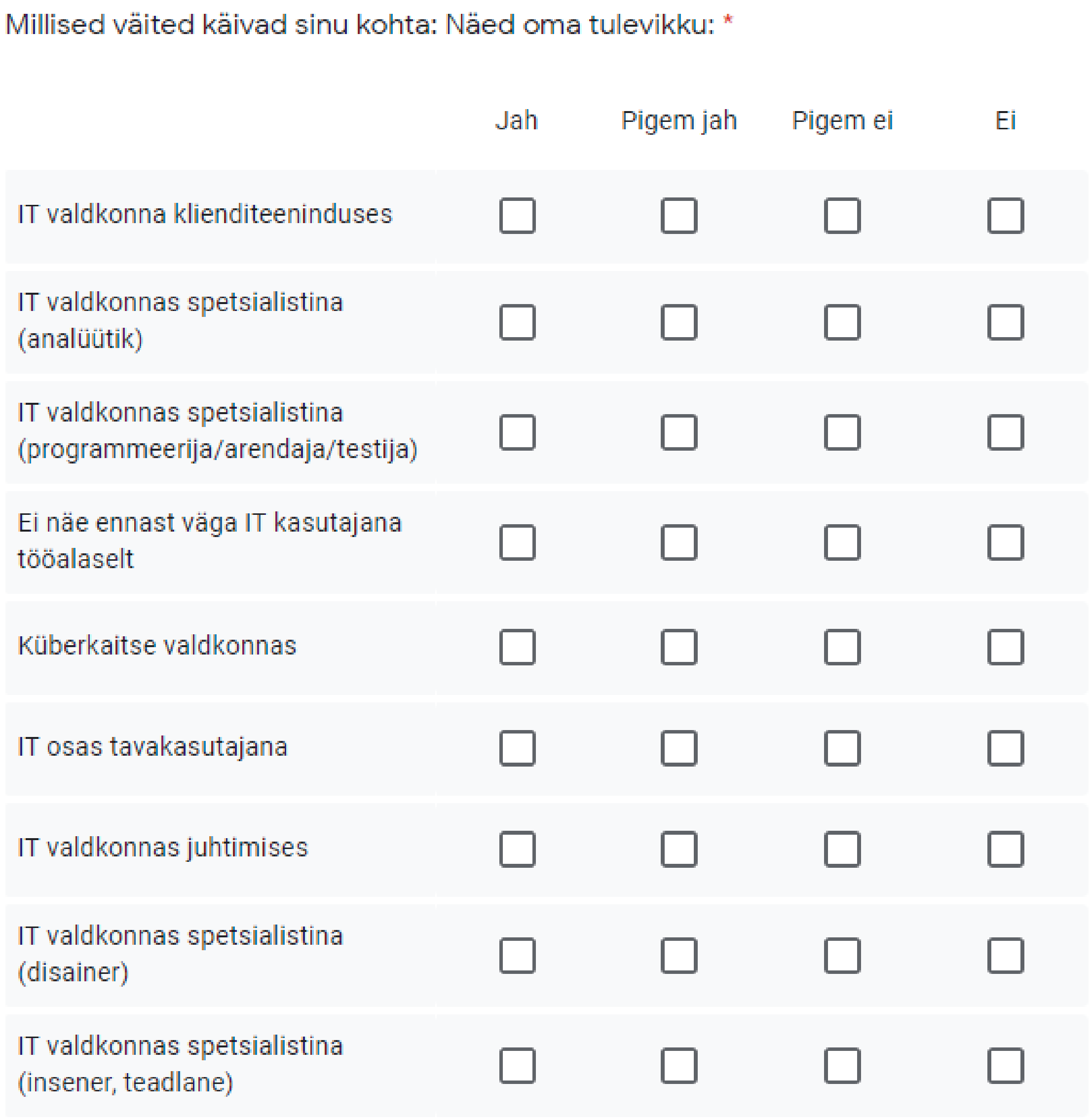
	Jah	Pigem jah	Pigem ei	Ei
Vaatan videosid ja loenguid internetist	□	□	□	□
Olen osalenud võistlusel või häkatonil	□	□	□	□
Olen osalenud mõnel e-kursusel	□	□	□	□
Jälgin mõnda kogukonda või kanalit internetis	□	□	□	□
Leian lugemiseks veebilehti, uudiseid antud teemadel	□	□	□	□
Midagi muud	□	□	□	□
Loen raamatuid	□	□	□	□
Suhtlen sõpradega antud teemadel	□	□	□	□



Millisel määral soovid õppida paremini tundma järgmisi tehnoloogiaid: *

	soovin	pigem soovin	pigem ei soovi	ei soovi	tunnen antud tehnoloogiat juba spetsialisti tasemel
Linux based server	□	□	□	□	□
Networking	□	□	□	□	□
Wireshark	□	□	□	□	□
Honeypot	□	□	□	□	□
Nmap	□	□	□	□	□
IoT	□	□	□	□	□
Windows based server	□	□	□	□	□
Python	□	□	□	□	□
C++	□	□	□	□	□

Kui vastasid muu, siis mida soovid veel teada saada?



Millised väited käivad sinu kohta: Näed oma tulevikku: *

	Jah	Pigem jah	Pigem ei	Ei
IT valdkonna klienditeeninduses	□	□	□	□
IT valdkonnas spetsialistina (analüütik)	□	□	□	□
IT valdkonnas spetsialistina (programmeerija/arendaja/testija)	□	□	□	□
Ei näe ennast väga IT kasutajana tööalaselt	□	□	□	□
Küberkaitse valdkonnas	□	□	□	□
IT osas tavakasutajana	□	□	□	□
IT valdkonnas juhtimises	□	□	□	□
IT valdkonnas spetsialistina (disainer)	□	□	□	□
IT valdkonnas spetsialistina (insener, teadlane)	□	□	□	□

Appendix 2. Survey questions

Küberturbe õpetamine koolis - uuring

Lugupeetud vastaja!

Pöördun teie poole, et viia läbi oma magistritöö uuring.
Uuringu eesmärgiks on mõista, kuidas õpetatakse küberturvalisusega seotud teemasid õpilastele teie koolis.

Tulemusi kasutatakse anonüümselt lõputöö analüüsis, mille eesmärgiks on pakkuda välja keskkond küberturvalisuse tehniliste oskuste võistluslikuks (CTF ehk küberkaitse lipuvõistluse laadi) õpetamiseks. Uuringu tulemused aitavad parendada koolidele suunatud KüberOlümpia programmi toetustegevusi ja KüberPuuringu võistlust.

Küsimistiku täitmine võtab 25-30 minutit.
Uuringus on kolm osa: taustainfo (8), IT-õpetus koolis (16), Küberturbe teema võistlused ja tulevik (12). Enamus vastused on valikvastused, avatud vastuste lahtrites on võimalus oma arvamust põhjendada ja soovi korral tuua näiteid. Kui jõuate lehele 4, siis vajutage "submit" ja saatke oma vastused ära.

Ankeedile saab vastata kuni 31.01.2021
Olen teile väga tänulik!

Alex Bindevald
Tallinna
Tehnikaülikool
alex.bindevald@tal
tech.ee
56869474

* Kohustuslik

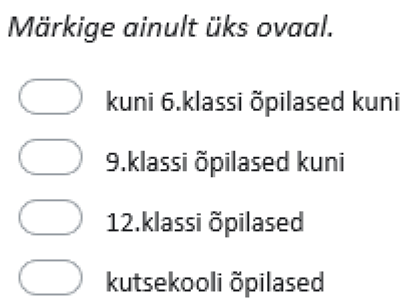
Taustainfo

1. Kooli nimi:

   Infot kasutatakse uuringus osalenud koolide märgendamiseke Eesti kaardile. Uuringu sisulises osas koolide vastused anonümiseeritakse.

2. Teie koolis õpivad *

   Vali üks



Märkige ainult üks ovaal.

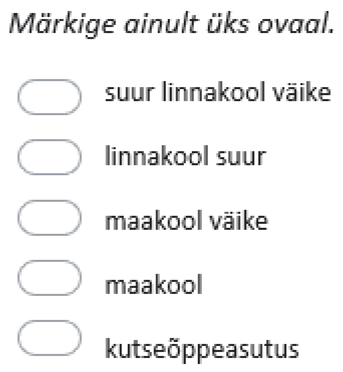
○ kuni 6.klassi õpilased kuni

○ 9.klassi õpilased kuni

○ 12.klassi õpilased

○ kutsekooli õpilased

3. Teie kooli kirjeldab kõige enam: *



Märkige ainult üks ovaal.

○ suur linnakool väike

○ linnakool suur

○ maakool väike

○ maakool

○ kutseõppeasutus

4. Hinnake oma kooli digipöörasuse astet: *

"Digipöörane" on kool, kes otsib võimalusi ja osaleb erinevates õpilaste digioskuseid arendatavates kohalikes, riiklikes ja rahvusvahelistes ettevõtmistes.

Märkige ainult üks ovaal.

○ Jah, oleme digipöörased

○ Oleme tavaline kool nagu teised tavalised koolid

○ Me ei ole väga digilembesed

5. Hinnake, kuidas läheb teie koolil võrreldes teiste koolidega küberturbe teemade õpetamisel: *

Märkige ainult üks ovaal.

○ paremini kui

○ teistel

○ samaväärselt

halvemini kui

teistel

6. Mitu ametikoha väärilist IT töötajat, arvutiõpetajat või IT ringiõpetajat on teie koolis (arv kokku): *

nt. IT 0,5 ja HT 0,5 = 1

____

7. Teie roll/ülesanded koolis: *

Vali üks või mitu

Märkige kõik sobivad.

□ Arvutiõpetaja
□ Muu aine õpetaja
□ Haridustehnoloog
□ Huvijuht
□ IT-juht
□ Muu juhtkond

Muu: □ ____________________________________

8. Kas Te olete osalenud kunagi CTF (küberkaitse lipuvõistlus) võistlusel võistlejana? *

Märkige ainult üks ovaal.

○ Jah
○ Ei

IT-õpetus koolis

9. Teie koolis toimuvad järgmised tegevused: *

Vali üks või mitu

Märkige kõik sobivad.

□ arvutiõpetus kõikidele

□ arvutiõpetus ainult valitud

□ klassidele robootikaring

□ huvilistele muud IT ringid

□ huvilistele IT-d puudutavad

□ üritused

□ tehakse digitaalse ohutuse valdkonnas teavitustööd

□ osaletakse küberturbe teemalistel võistlustel nt.
KüberPuuring osaletakse muudel erinevatel IT võistlustel

muu: __________________________

10. Kuidas teie kool õpetab küberturbe teemasid? *

Vali üks või mitu

Märkige kõik sobivad.

□ Eraldi temaatiline aine või ring

□ Mõne teise aine/ringi sees (nt informaatika)

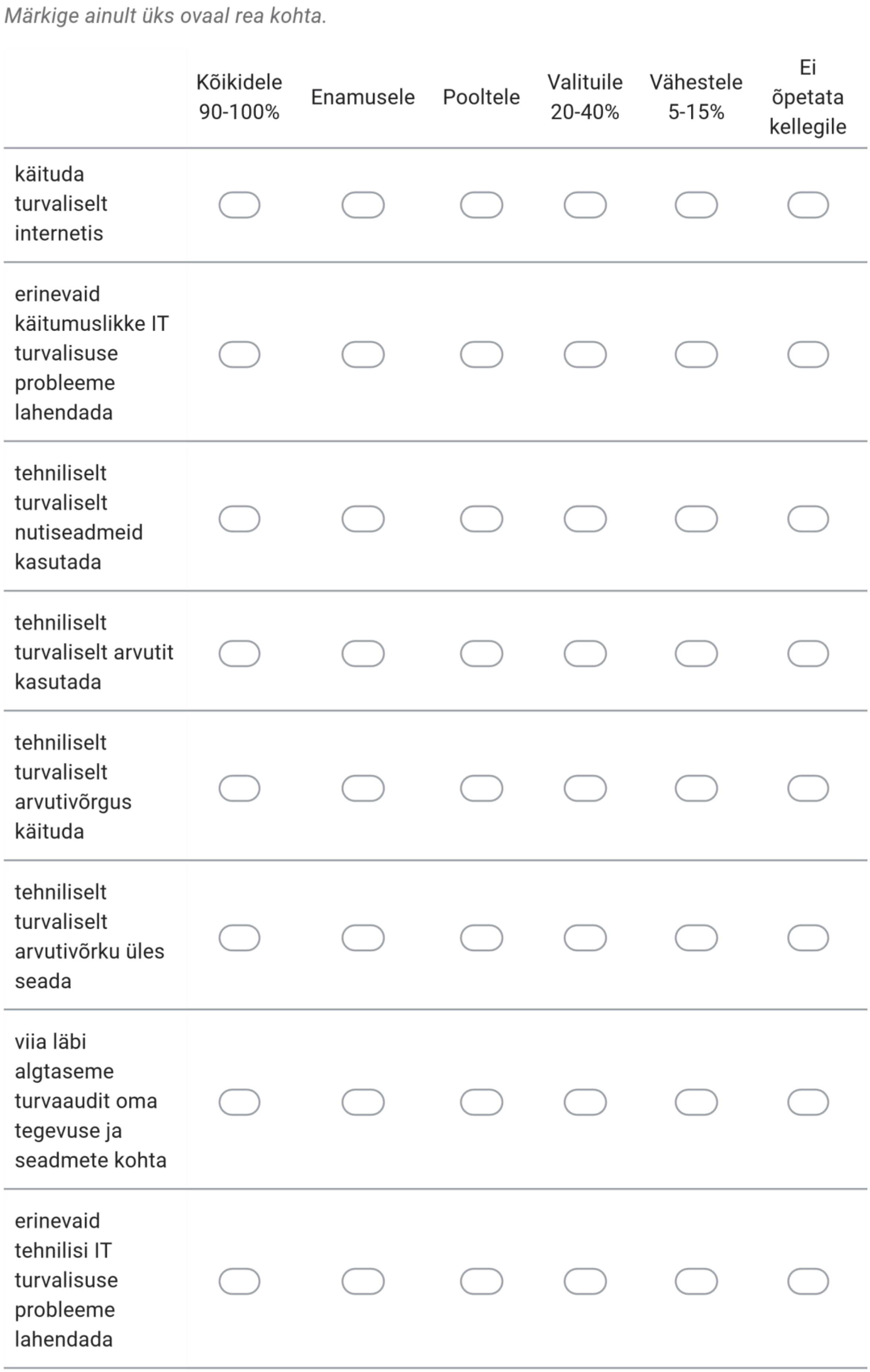
□ See on kõikide õpetajate ühine ja jagatud vastutus

□ Ainult eriüritustel sh. võistlused

□ Ei õpeta

Muu: □ __________________________________

11. Kui palju teie koolis õpilastele õpetatakse järgmisi teemasid: kuidas... *



Märkige ainult üks ovaal rea kohta.

	Kõikidele 90-100%	Enamusele	Pooltele	Valituile 20-40%	Vähestele 5-15%	Ei õpetata kellegile
käituda turvaliselt internetis	○	○	○	○	○	○
erinevaid käitumuslikke IT turvalisuse probleeme lahendada	○	○	○	○	○	○
tehniliselt turvaliselt nutiseadmeid kasutada	○	○	○	○	○	○
tehniliselt turvaliselt arvutit kasutada	○	○	○	○	○	○
tehniliselt turvaliselt arvutivõrgus käituda	○	○	○	○	○	○
tehniliselt turvaliselt arvutivõrku üles seada	○	○	○	○	○	○
viia läbi algtaseme turvaaudit oma tegevuse ja seadmete kohta	○	○	○	○	○	○
erinevaid tehnilisi IT turvalisuse probleeme lahendada	○	○	○	○	○	○

12. Milliseid keskkondi ja materjale kasutate digitaalse ohutuse ja küberturvalisuse teemade õpetamiseks, kui kasutate? Nimetage võimalusel 3-5 (võivad olla ka
lingid). *

13. Kas teie õpilastele meeldib IT-võistlustel osaleda? *

Märkige ainult üks ovaal.

○ Jah

○ Pigem jah

○ Pigem ei

○ Ei

14. Kas teie õpilased osalevad CTF võistlustel (CTF= küberkaitse lipuvõistlus) nt KüberPuuring, Magic CTF, KüberNaaskel või nende analoog? * *Märkige ainult üks ovaal.*

○ Jah

○ Ei

15. Mõeldes edasistele aastatele, kas teie kooli õpilased oleksid huvitatud/jätkuvalt huvitatud ülaltoodud võistlustel osalemisest? * *Märkige ainult üks ovaal.*

○ Jah

○ Ei

16. Palun põhjendage, miks? *

17. Millised on suurimad väljakutsed koolis IT-võistlustel osalemisel? *

18. Olukord: Võistlus toimub onlines ja koolis. Kuidas tagate koolisisesel võistlusel (nt KüberPuuringu eelvoorus) vastamise aususe (fair game) ja pettuste tuvastamise? *

19. Kuidas valmistate ette õpilasi, kes osalevad IT või CTF võistlustel? *

20. Võistlused toimuvad harva. Kuidas hoiate ja toetate noorte huvi IT ja küberkaitse teemadel võistlustevahelisel perioodil? *

21. Kirjeldage, kas ja milliseid eritegevusi teete, et kaasata rohkem tüdrukuid IT ja küberkaitse teemadega tegelema? *

22. Kas olete ka ise oma koolis pannud üles mõnda CTF võistluse tehnilist lahendust? *

Märkige ainult üks ovaal.

○ Jah

○ Ei

23. Kui jah, mida kasutasite ja kuidas üles seadmine läks?

24. Kui jah, siis kui tihti kasutate CTF võistluse tehnilisi lahendusi?

Küberturbe teema võistlused ja tulevik

25. Teie kooli ootus riiklikule ainekava arendustegevusele järgmisel 5 aastal on: *

Märkige ainult üks ovaal rea kohta.

	Jah	Pigem jah	Pigem ei	Ei
Uuendatakse informaatika ainekava küberturbe osa 1.-6. klassile	○	○	○	○
Luuakse informaatika ainekava küberturbe osa 7.-9. klassile	○	○	○	○
Luuakse küberturbe ringikava 4.-9. klassile	○	○	○	○
Uuendatakse informaatika õppekava küberturbe osa gümnaasiumis	○	○	○	○
Luuakse lisa valikaineid gümnaasiumis küberturbes (nt. inimlikud või tehnilised aspektid)	○	○	○	○

26. Midagi muud/veel:

27. Teie kooli ootus õpetajate küberturbe teemade ettevalmistuse toetuseks järgmisel 5 aastal on: *

Märkige ainult üks ovaal rea kohta.

	Jah	Pigem jah	Pigem ei	Ei
Luuakse toetav lugemisvara õpetajatele/vanematele, mis puudutab talentide ettevalmistust küberkaitse teemades	○	○	○	○
Luuakse eraldi e-kursus, mille keskne teema on küberkaitse võistlusteks ettevalmistus (kasutatav nii õpetajatele kui õpilastele)	○	○	○	○
Lisatakse uusi ülesandeid kesksesse ülesannete portaali nt. ylesanded.targaltinternetis.ee	○	○	○	○
Antakse soovitusi CTF lahenduseks, mida koolid saavad ise kasutada (nt oma serveris)	○	○	○	○
Luuakse keskne Eesti CTF lahendus, mis on kättesaadav onlines koos ülesannete pangaga	○	○	○	○
Luuakse keskne Eesti CTF lahendus, mis on kättesaadav onlines, kuhu igaüks saab ülesandeid ise sisestada	○	○	○	○

28. Midagi muud/veel:

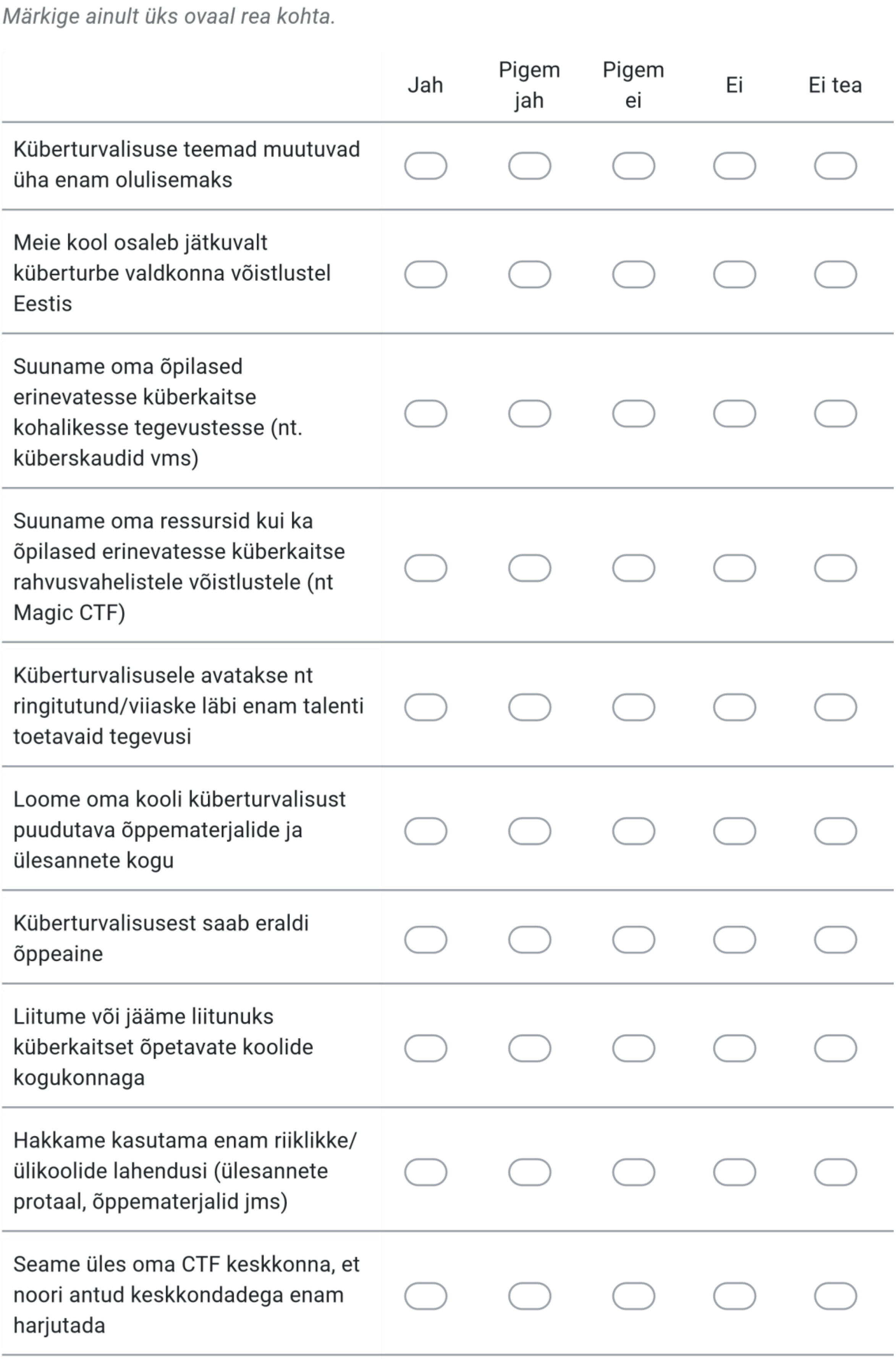
29. Teie kooli ootus küberturbe võistlusele KüberPuuring järgmisel 5 aastal: *

Märkige ainult üks ovaal rea kohta.

	Jah	Pigem jah	Pigem ei	Ei
Võistluse eelvooru peaks korraldama kool ise (looma küsimused, valima keskkonna jms)	○	○	○	○
Eelvoorus peaks olema jagatud vastutus nagu täna ehk ülikool loob ülesanded ja koolil jätkuvalt oluline roll (eelvooru korraldamisel nagu talle sobib)	○	○	○	○
Lõppvoor peaks toimuma alati onlines	○	○	○	○
Lõppvooru auhinnad peaksid jääma alati harivateks (elamused, koolitused)	○	○	○	○

30. Midagi muud veel:

31. Andke hinnang oma kooli tegevuse osas küberturbe teemades järgmisel viiel aastal: *



Märkige ainult üks ovaal rea kohta.

	Jah	Pigem jah	Pigem ei	Ei	Ei tea
Küberturvalisuse teemad muutuvad üha enam olulisemaks	○	○	○	○	○
Meie kool osaleb jätkuvalt küberturbe valdkonna võistlustel Eestis	○	○	○	○	○
Suuname oma õpilased erinevatesse küberkaitse kohalikesse tegevustesse (nt. küberskaudid vms)	○	○	○	○	○
Suuname oma ressursid kui ka õpilased erinevatesse küberkaitse rahvusvahelistele võistlustele (nt Magic CTF)	○	○	○	○	○
Küberturvalisusele avatakse nt ringitutund/viiaske läbi enam talenti toetavaid tegevusi	○	○	○	○	○
Loome oma kooli küberturvalisust puudutava õppematerjalide ja ülesannete kogu	○	○	○	○	○
Küberturvalisusest saab eraldi õppeaine	○	○	○	○	○
Liitume või jääme liitunuks küberkaitset õpetavate koolide kogukonnaga	○	○	○	○	○
Hakkame kasutama enam riiklikke/ ülikoolide lahendusi (ülesannete protaal, õppematerjalid jms)	○	○	○	○	○
Seame üles oma CTF keskkonna, et noori antud keskkondadega enam harjutada	○	○	○	○	○

32. Midagi muud veel:

33. Kas teie arvates on keskse teenusena CTF lahendus kasutamiseks kõikidele koolile Eestis vajalik? *

Märkige ainult üks ovaal.

○ Vajalik

○ Pigem vajalik

○ Pigem ei ole vajalik

○ Ei ole vajalik

34. Kui loodakse Eesti keskne CTF lahendus või antakse koolidele soovitusi mõne sellise üles seadmiseks, peaks: *

Märkige ainult üks ovaal rea kohta.

	Jah	Pigem jah	Pigem ei	Ei
Keskkond olema onlines kättesaadav (kool ei pea tegelema tehnilise poolega)	○	○	○	○
Keskkond olema kooli serverisse installeeritav (ja ainult seal kasutatav)	○	○	○	○
Keskkonnas saama luua endale permanentse konto	○	○	○	○
Nii õpetajad kui ka õpilased saama ise luua ja muuta küsimusi	○	○	○	○
Küsimused olema keskselt ette antud (küsimuste pank)	○	○	○	○
Paketi võistluste tarbeks loomise puhul olema see kasutatav kuni 3 kuud (pärast seda aegub).	○	○	○	○
Lahendus õpilase vastused ülesannetele edastama õpetaja emailile	○	○	○	○
Õpilaste vastused olema kättesaadavad keskkonnas üldtabelina õpetajale	○	○	○	○
Keskkonnast saama näha võistluse edetabelit	○	○	○	○

35. Juhul, kui soovite midagi veel lisada:

36. Kui soovite osaleda jätku-intervjuus, kus pakutakse lahendus kesksele Eesti CTF keskkonna kasutamiseks, siis lisage siia oma e-mail:

Appendix 3. Questions for the interviews

Esmalt mainin ära, et küsimuste vastuseid kasutan töös üldistatud kujul ning kõik vastused on anonüümsed. Lisaks küsiks, kas Teie jaoks on okei see, kui ma seda vestlust enda jaoks lindistan, et hiljem vajadusel kokkuvõtet kirjutades intervjuud uuesti kuulata.

Sissejuhatavad ja taustaküsimused

Mis kooli esindate ja milline on teie taust koolis?

Mis vanuseklassidega te igapäevaselt kokku puutute?

Milline on teie kogemus küberkaitse teemadel? Pigem algaja, ekspert või vahepealne?

Eeluuringust üles kerkinud küsimused, millele vajad kinnitust, seletust

Uuringu tulemustest tuli välja, et küberkaitse teemasid ei õpetata 7.-12.klassides, kui siis ainult huviringides. Kas see vastab tõele ka teie kooli puhul?

Uuringu tulemustest selgus, et õpilased on huvitatud küberkaitse teemadest, kuid nendega kurssi viimiseks pole piisavalt ressursse, nagu näiteks näidis CTF keskkondasid. Miks see Teie hinnangul nii on?

Samuti tuli välja, et paljud õpetajad pole ise ühtegi keskkonda üles seadnud, mis võib teie hinnangul olla selle põhjus?

CTF keskkonda puudutavad küsimused:

CTF keskkonna seletus, kui ei tea

Milline on teie ettekujutus CTF keskkonnast?

Millised on teie varasemad kokkupuuted CTF keskkondadega? *Kui on kokkupuude, siis millise keskkonnaga*

Kelle poolt peaks teie hinnangul olema CTF keskkond üles seatud? (kas kool ise, ülikool vms)

Millistest osadest peaks teie arvates CTF keskkond koosnema?

Missugused kasutajad, rollid ja õigused peaksid teie arvates olema CTF keskkonnas?

Kuidas te näete ette CTF keskkonda sisenemist ning kasutajate haldust?

Millistest teemadest peaksid küsimused/ülesanded loodud olema?

Kirjeldage palun, mis moel peaks küsimusi/ülesandeid looma ning kuidas neid kätte saada?

Kuidas peaks olema näidatud õpilaste ülesannete lahendamise tulemused?

Kui tihedalt leiaks tsentraalne CTF keskkond kasutust?

CTF keskkonna näidet puudutavad küsimused:

Kas te osalesite "Küberturvalisuse koolitamine küberturbe lipuvõistluse CTF meetodil" koolitusel? Kui jah, siis kas teile meeldis see CTF keskkond ja miks?

Tutvustan 3 keskkonda, ning küsin nende üleüldist arvamust.

1) CTFd
2) Ctfspace
3) picoCTF

Kas ja mis võiks olla teie hinnangul teisiti tutvustatud keskkondades?

MUU

Kas te soovite veel midagi lisada või minu käest küsida?