UNIVERSITY OF TURKU

Cybersecurity Education for Children and Adolescents in Finland

A Study in Finnish Schools

Cyber Security

Master's Degree Programme in Information and Communication Technology

Department of Computing, Faculty of Technology

Master of Science in Technology Thesis

Author:

Topi Suvimeri

Supervisors:

Dr. Ali Farooq

Professor Jouni Isoaho

September 2023

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Cyber Security
Programme: Master's Degree Programme in Information and Communication Technology
Author: Topi Suvimeri
Title: Cybersecurity Education for Children and Adolescents in Finland - A Study in Finnish Schools
Number of pages: 101 pages
Date: September 2023

Abstract.

Along with the advancement of technology and the rising need for safety and security in the lives and education has raised concerns regarding cybersecurity knowledge and awareness. This thesis focuses on the cybersecurity education of students in Finnish schools. Interviewing teachers and cybersecurity professionals are done to gain insight, whether the current cybersecurity education in the existing curricula is enough, and how it could be improved.

While children and adolescents spend a considerable time for entertainment purposes, their lack of understanding and awareness of cybersecurity risks is evident based on the research done in the thesis, and in the existing cybersecurity related literature. This thesis aims to categorize the findings based on the interviews into three different categories regarding what, when, and how cybersecurity knowledge and safety should be included in the cybersecurity and ICT education.

The findings based on the interviews show that the most common key concerns regarding cybersecurity topics. In addition, children and adolescents should be monitored, however, the way of monitoring needs to be done by the parents to not infringe on the privacy of the youth. The concept of cybersecurity should be introduced for the youth when they first begin using electronic devices. Moreover, ICT should be introduced as its own school subject, albeit melded as a part of other subjects. The modern way of educating cybersecurity to the youth could be done through gamification (bringing gaming elements into non-gaming contexts), concrete examples, and different types of educational media.

The cybersecurity and ICT education should be introduced as its own school subject or as a part of other subjects to prepare them for the future. The education must be done per age category, and teaching materials must be revised yearly, similarly how other subjects are. However, the educational system requires teachers and parents to be a part of the education as well, as some of them are not very knowledgeable regarding cybersecurity and ICT topics. The education system must be done in cooperation between different municipalities to ensure that everyone gets equal chance for education, and to avoid inequity that might rise, if not addressed by the Ministry of Education and Culture level.

Keywords: cybersecurity education, ICT education, children, adolescents, cybersecurity risks, cybersecurity awareness

Table of contents

1 Introduction

The digitalization and modernization of the world have integrated IT devices as part of children and adolescents' daily lives and education. The rising need for technological literacy after COVID-19 has brought up concerns regarding their knowledge about cybersecurity, especially considering how much they are now dependent on technology, and the cybersecurity threats in such an environment. Students being inspected in this thesis are in the seventh to ninth grade in Finnish schools. Cybersecurity is a concern that affects every individual and industry, and nowadays, any individual with digital information might become a target of various attacks [1]. Password theft, malware, phishing attacks, social engineering, ransomware, and trojan viruses are real and common threats for everyone. Regarding children and adolescents, the common threats are password theft, phishing attacks, and social engineering [2]. Considering the risk of children falling victim to these threats while using the internet, there is a great need for cybersecurity awareness for their sake, and to prepare them for the future.

Many of them spend significant time on the internet, whether for educational, practical, or recreational purposes [1]. This is not inherently wrong, of course, but cybersecurity risks must naturally also be accounted for, as they may lack the understanding and awareness necessary for vital cyber skills. For example, it is crucial to be mindful of making strong passwords as the first line of defense, know the importance of anti-malware and anti-virus tools, and teach them about the potential threats of social engineering phishing techniques [3]. Nowadays, children are supposed to have fundamental cybersecurity skills, such as good password management and media literacy skills are already a good start for children, as such skills are relevant for a lifetime. There have been different studies and designs conducted regarding the design of different applications [4] and e-books that can be used for educational purposes regarding cybersecurity. Publicly available applications and e-books have given parents the opportunity to learn and teach their children regarding cybersecurity.[5]

There have been increasing amounts of cybercrime cases in Finland involving personal data, be it the case with Vastaamo, Facebook, or even Roblox [6-7]. Children on social media such as Facebook and TikTok or social platforms such as Twitch and Discord, are especially vulnerable [8]. Children make accounts on these platforms while they are underage and without their parents' knowledge since account creation is often trivial and

lacks proper age verification. Various phishing and adware scams are common for children to fall for because it is, for example, sent by a "friend" they know, or an influencer they follow [9-10].

1.1 Problem Statement

The security threats and risks mentioned in the previous section raise questions about: what is currently taught in schools for children and adolescents and whether it is enough to combat a new and ever-evolving cybersecurity landscape. Are the skills taught to children starting from primary school enough to prepare them for the cyberthreats that are happening currently.

A basic understanding of cybersecurity, even in a technologically developed country like Finland, is severely lacking in many cases. A 2022 survey published by the Global Cybersecurity Forum (GCF) reported that around 72% of surveyed children worldwide have experienced at least one type of cyber threat online. This must be considered, since another report mentioned that at least 90% of children aged eight and above are on the internet [11]. These highlight two core issues: one, the probability of them falling for cyber threats is higher than they likely expect; two, and more worryingly, there is an underlying apathy for staying vigilant to different types of cyber threats, especially when it comes to children and adolescents.

The main objective of this thesis is to find out what cybersecurity experts and teachers think about the problems of cybersecurity education within Finnish schools, whether teaching methods in schools are enough to prepare children and adolescents for the future, and how. Are we providing them enough knowledge to protect themselves from potential new threats that might arise in the future?

1.2 Objectives

This study indentifies when children and adolescents should be taught about cybersecurity, what they should be taught, and how they should be taught according to the teachers and cybersecurity professionals. The study will also explore if the opinions of the interviewed teachers and cybersecurity professionals differ in particular ways to spot key areas that education should focus on, how, and why.

This thesis answers the following research questions:

RQ1: When should cybersecurity be taught about?

RQ2. What should children and adolescents be taught about cybersecurity?

RQ3. How should cybersecurity be taught to children and adolescents?

This thesis will additionally explore stances from both teachers and cybersecurity experts, the difference between these stances, and analyze how both opinions could be utilized in future teaching.

1.3 Methodology

The interview questions were the same for each teacher and cybersecurity professional but were left open enough for them to determine how to interpret the question in accordance with their understanding, as the questions were structured to be opinion-based questions, instead of factual questions. The purpose of the data analysis is to analyze, compare and compile the answers of teachers and cybersecurity professionals to determine whether cybersecurity is taught enough in the current curriculum in Finnish schools.

This was done by interviewing cybersecurity professionals and primary school teachers to obtain their stances on the matter, what they think about adding cybersecurity to the curriculum as its own subject, whether there is already cybersecurity education at their schools, and whether that is enough to prepare them for the future.

After the interviews are compiled, they are analyzed to determine what the teachers and professionals think about teaching cybersecurity, whether it is taught sufficiently, and whether it should be added to the curriculum as its own subject.

The focus of this thesis is to hear about the teachers' and cybersecurity experts' opinions on whether cybersecurity is covered enough in the current curriculum, and if not, what students should be taught in more depth. There is always potential for future work on how cybersecurity could be integrated to be a part of the future curriculum.

1.4 Expected outcomes

In this thesis, I will propose a new primary school cybersecurity curriculum to replace the old one. The expected outcome of this thesis is the collation of various stances from experts and teachers. The thesis expects to provide knowledge that will provide children's guardians' view about cybersecurity/cyber wellbeing of theirs. The thesis will identify the knowledge that cybersecurity professionals think is relevant for children. The thesis also identifies the right age to make children aware of cybersecurity issues.

Cybersecurity professionals may likely think that the current curriculum does not go through cybersecurity thoroughly enough, and the teachers may likely consider the subject overwhelming for children and adolescents if all aspects of cybersecurity are exhaustively taught to them. Cybersecurity teaching should be brought into the curriculum in different layers or stages of teaching, like how other subjects are taught, teaching them little at a time. However, that would bring out the problem of where it should be placed in the curriculum: would it take time away from another subject that needs to be taught, and how well would the children and parents accept a new subject, even if it was required?

1.5 Thesis Structure

This thesis has been divided into six chapters. The first chapter introduced the subject of the thesis, the main objectives of the research, and what are the expected outcomes of this thesis. Chapter two covers background information, which includes the previous studies written regarding children and adolescents' cybersecurity teaching methods and platforms and is used in the analysis process of the thesis. Chapter three consists of the research methodology where the research process is explained thoroughly. Chapter four consists of the results and findings from the gathered data collection and the analysis of the findings. Chapter five contains a discussion of the results found. Finally, chapter six summarizes the research conducted, the main findings, and a summary of the thesis.

2 Background and related studies

Security has, by and large, always been an important consideration in available software and social media platforms, especially when children and adolescents are included as a part of the userbase or the target audience. When the security is involved, there are many more concerns and challenges, especially in the case of online integration with software. Researchers of the child-computer interaction (CCI) community primarily concern themselves with children's privacy and security, exploring different countermeasures to security and privacy risks to support children, youth, and their caregivers, including awareness of various cybersecurity risks [12]. Research into the CCI first began in the late 80s and early 90s, although it is difficult to pinpoint exact dates due to the lack of published research on the CCI. Most of the research at the time was focused on the Human-Computer Interaction (HCI). Despite this initial deficit of published research, privacy and security risks have become a critical issue in children's lives due to them growing up immersed in technological advancements. Compared to prior generations, these concerns were not considered just a few decades ago. [13]

With the increase of children and adolescents' online device usage and exposure to the internet, they often familiarize themselves quickly to their devices and the internet. This was more apparent after the COVID-19 pandemic led to a widespread reliance on devices to keep education systems afloat in the wake of social isolation. Cybersecurity, in this world, is now more relevant than ever. A literature review concerning internet activity and motivation for youth to use the internet identified risks on what they might be exposed to, listing them into five risk categories: [14]:

- Content risks
- Contact risks
- Children targeted as consumers
- Economic risks
- Online privacy risks

Content risks were further divided into three broad categories: illegal content (sexual exploitation of minors); harmful or age-inappropriate content (pornography and violence);

and harmful advice regarding alcohol and drugs, suicide, and disorders regarding psychology and nutrition. Content risks were elaborated on, citing cyberbullying and cyber-grooming.

Exposure of minors to harmful or inappropriate content has become a major concern. Numerous studies have gauged the impact of online pornographic content on their attitudes, beliefs, self-concept, behaviors, and social and mental development [15]. To raise cybersecurity awareness in children, researchers have explored the possibilities of using various gaming technologies to raise cybersecurity awareness. The findings of the research have shown that gaming can have a positive impact on cybersecurity awareness and its current limitations [16]. Researchers have been evaluating different cybersecurity themed games to determine what types of game-elements are needed to keep students engaged in the study materials, and to find different ways to deliver cybersecurity knowledge to them [17].

Research exists regarding social media usage increasing the risk of harm for children, which was supported by the data they used in their research. The hypothesis of their research was that "children who use social networking sites (SNS) will encounter more online risks; SNS users with more digital competency will encounter more risks; SNS users with more risky practices will encounter more risks; and SNS users with more digital competence will experience less harm associated with online risks." Of the five hypotheses, only the fourth was not supported by data: the others back the claim that children and youth that used SNS are more likely to encounter dangers online. [18]

Cyberbullying has become an increasingly common topic with the advancements in technology and the increased usage of the internet, which has garnered much attention from researchers and the public. A review in 2017 collated 132 peer-reviewed publications into a report on important trends, and among those publications, 66% of the review articles were focused on cyberbullying. [19]

In the past, there have been multiple different literature reviews on cyberbullying and the issues that cyberbullying has caused. Researchers have focused on cyberbullying to identify inappropriate online and offline behavior by children or directed at children. The point of the research was to identify the types of threats and consequences of cyberbullying. Different types of identified threats are [20]:

- Flaming (Intense arguments that take place in chatrooms, private messages, or email)
- Cyber-harassment

- Denigration
- Impersonation (Someone pretending to be a user to cause harm for their reputation)
- Masquerading (Pretending to be someone who they are not)
- Outing (Publicly displaying or forwarding private messages)
- Trickery
- Ostracism
- Exclusion

There have been numerous research investigations on the history of cyberbullying among children, all the way to higher education to determine if the number of incidents have changed from childhood to adulthood. Part of the reason why cyberbullying is still prevalent in every stage of development and education is the power of online anonymity; aggressors can remain anonymous and continually abuse their victims without revealing their own identity. Using this anonymity, cyberbullies (commonly known as "trolls") often avoid the social consequences of cyberbullying because online identity is often amorphous and intangible. [21]

Research has determined common factors connected to cyberbullying, such as the targets of cyberbullying, causes for cyberbullying, differences between bullying and cyberbullying, and comparing gender differences in relation to cyberbullying. [22] Researchers have also found that the consequences of cyberbullying can be associated with adolescents' depressive symptoms; for example, loneliness, insomnia, and loss of interest or pleasure in ordinarily pleasurable activities. [23]

All the above studies are relevant to the question of why teaching cybersecurity awareness and media literacy in schools would be beneficial for the younger generation of students and why.

2.1 Students and teachers' roles in cybersecurity and education

It goes without saying that teachers are essential to the act of teaching, as is the training that they themselves receive. However, information on cybersecurity training undergone by

teachers today is scarce: studies exist that investigate the insufficiency of teaching materials and the time given to prepare for teaching cybersecurity.[24]

The Finnish National Agency for Education has listed eight sectors of cybersecurity [25]:

- Administrative & organizational cybersecurity
- Personnel security
- Physical security
- Informational technology security
- Hardware security
- Software security
- Information subject security
- Application security

However, these sectors only provide the essential information regarding cybersecurity and what the information they gather at schools is used for, explaining some of the key words of cybersecurity. Importantly, they do not explain what kind of cybersecurity training that teachers themselves are required to go through. After the European General Data Protection Regulation (GDPR) in 2018, most city employees were required to go through a GDPR training process to correctly handle data. The extent at which teachers engage with this kind of training is difficult to quantify.

2.1.1 Definition of a child and an adolescent

It is important to precisely define what a "child" is in the context of cybersecurity, as well as understand the rights of children in online spaces. The usual consensus of the definition is that a child is, simply, a person who is under the age of 18 years old. However, the existing literature on cybersecurity has focused on various age groups of children, including young children, primary school students, middle school and high school students, and college students. Some studies have also examined the attitudes and behaviors of parents and teachers regarding children's cybersecurity. [26]

This broad categorization is insufficient when dealing with the complexities of internet security over such a wide age range. Children and youth cannot be put into a single group where five-year-olds are considered in the same light as seventeen-year-olds, especially when it comes to teaching them to protect themselves from the potential dangers of the internet.

There are many differences between children and youth [27]:

- Age
- Gender
- Evolving capabilities
- Social backgrounds
- Economic backgrounds
- Race and ethnic backgrounds
- Disabilities
- Refugee children and youth
- Children and youth in care
- LGBTQI+ children and youth

Of course, they cannot be taught as if they exist as a single category, disregarding age, and ability. Teaching cybersecurity should be approached in the way as any subject would be, depending on the group of children and youth being taught. Starting from the basics, and slowly building their knowledge and understanding of cybersecurity over time, with special exceptions kept in mind. However, for the sake of the scope of the thesis, they are under inspection in the seventh to ninth grade in Finnish schools.

Adolescence often happens when the children reach puberty, often during the ages 10-19, but it is unique to everyone. Adolescents go through a rapid physical, cognitive, and psychological growth that can be seen as [28]:

- Behavioral changes
- Substance use

- Risk taking
- Sexual activity
- Becoming more independent
- Decision making

As COVID-19 forced children to study from home, it brought new challenges to the whole education structure to ensure that everyone had an equal chance to study and learn. It also brought the need for security.

2.1.2 Children's rights and safety on the Internet

The rights of a child are the most widely accepted human rights treaty in the world, which in turn provides a common ethical and legal framework for the rights. All children's rights are equally important and essential for healthy global development of children [29]. These maxims are obviously essential when considering child safety on the internet. Ostensibly, children are sufficiently protected by the children's rights convention. However, it is important to recognize if it alone is enough to prepare them for the evolving digital age, especially upon examination of how some countries have more thoroughly prepared them for the potential dangers of the fast-developing digital world.

The European Union (EU) has been working on a strategy called Better Internet for Children (BIK) since 2012. The EU has understood that children have needs and vulnerabilities on the internet, particularly as the age of internet users becomes younger and younger with each generation. The internet has become a widely accessible place of opportunities for children to learn and communicate, just as it has proved itself to be a potentially dangerous space for children to inhabit. In response, the EU has worked to guarantee online safety for children. Their strategy articulates itself around four main pillars: [30]

- Stimulating quality content online for children
- Stepping up awareness and empowerment
- Creating a safe environment for children online
- Fighting against child sexual abuse and child sexual exploitation

The BIK strategy laid out a global benchmark for the online safety of children, but over the decade updates were needed to match the current digital age. The strategy was updated on May of 2022 and the strategy is named Better Internet for Kids (BIK+).

As the average age of internet users has become younger and younger in comparison to 2012, many areas of digital content and services have fallen out of step with the needs and safety of younger demographics. Importantly, the 2022 strategy also differentiates children, moving away from the distinguishment of a "child" as anyone under 18. This acknowledges that the two groups demand additional nuance in approaches to internet safety. [30]

The internet was essential in overcoming challenges posed by COVID-19, but it also highlighted issues of inequality and the importance for every child to have access to digital technologies: without internet access, issues such as poor mental health, a lack of ability to easily stay in touch with friends and family, and lowered education outcomes were exacerbated in the pandemic years.

Since 2012, the EU has funded the hub for child online safety (betterinternetforkids.eu), where they have compiled resources regarding internet safety for children in multiple languages. The site contains various textbooks, videos, and games that children can play and learn with. They have also reinforced the revised Audiovisual Media Services Directive (AVMSD) to extend to video-sharing platforms to protect children from harmful or illegal content.

The European General Data Protection Regulation (GDPR) requires children's personal data to have special protection with parental consent between the ages of 13-16, depending on the country. The Unfair Commercial Practices Directive aims to protect children from malicious business practices. Lastly, the Digital Service Act requires terms and conditions to be understandable for children and makes the designing of systems with rights of the child in mind an obligation.[27]

The strategy has been compiled and simplified for children and youth to understand easily, where pillars of the updated strategy and what they cover are explained. The strategy will be translated into every single EU language, plus Icelandic, Norwegian and Ukrainian. [30]

The BIK+ has proposed three pillars to act around [27]:

- Safe digital experiences to protect children from harmful and illegal online content, conduct, contact, and consumer risks, and to improve their well-being online through a safe, age-appropriate digital environment, created in a way that respects children's best interests
- Digital empowerment, so children acquire the necessary skills and competencies to make sound choices, and express themselves in the online environment safely and responsibly
- Active participation, respecting children by giving them a say in the digital environment, with more child-led activities to foster creative and innovative safe digital experiences

Pillar 1: Safe digital world	Pillar 2: Ensuring that they have the skills, knowledge and support needed	Pillar 3: Making sure that children and adolescents have a say
The European union will be working with online platform providers (for example, Meta, SnapChat, Tiktok, and others) to create a set of rules to make sure that online services are safe for children(called code of conduct). The EU wants to ensure that they only see things online that are good for their age (together with ways to prove their age to access some online services), and that things they see or do online don't make them feel scared, sad, or uncomfortable.	The EU wants to make sure that children learn how to use the internet safely, both at home and at school. They need have the skills to know what to trust online, and to decide what's real or fake. They also need to know where to get help with any online problems they have.	The EU wants children to be able to use the internet to learn new things, and to be able to share their ideas on the internet they want.
The EU wants to make sure that platforms children use give easy-to-understand terms and conditions to protect their private information, respects their rights, and do not target them with adverts using the information they shared online.	The EU will be working with the decision-makers in their member countries to make sure that online safety and media literacy is taught in schools, and that teachers, parents, and carers can also learn how to better help children go online.	The EU will be working with children - through BIK Youth Ambassadors and BIK Youth Panels in the member countries - to get regular feedback, and to plan activities and training by young people, for young people, on all sorts of online topics.
The EU also wants to make sure that children are protected from cyberbullying, hate speech, and harm of any kind. Over the coming years, the EU will be working on to give them easy ways to get help on bullying and other online problems, no matter what country they live in.	The EU also understand that children are unique, and that they have different needs and situations, both online and offline. As a part of this plan, the EU wants to help them all to have safe and positive online experiences. In short, no one gets left behind.	The EU's goal is to listen to the ideas of children and work with others to make change happen. The EU will be looking at the strategy plan every two years to check that it is still working and to help ifx any new online problems.

Table 1. BIK+ Strategy Pillars. [27]

The BIK+ strategy works with major online platform providers, such as Meta, TikTok, and YouTube, to refine and recreate their code of conduct in ways that allow children to understand them, protect their private information, respect their rights, and prevent the

targeting of children with specific advertising. The code of conduct changes will also be used to combat cyberbullying and harassment children might encounter on the internet.

The BIK+ strategy also mandates that children should be able to learn how to use the Internet safely both at school and home, saying that children need to have the knowledge and skills to decide what information they see on the internet is real and what is fake. The EU is also working with decision-makers to bring online safety and media literacy studies to schools.

The BIK+ strategy aims to allow children to learn and share new ideas on the internet through BIK Youth Ambassadors and BIK Youth Panels for various topics and activities for children. The goal is to enact real changes to the state of online safety, and the plan is checked every two years going forward to see what is still working and what issues must be addressed.

In the BIK+ strategy, it was noted that children's need for improved media literacy and online safety education should be brought to schools; for now, however, it is still very lacking, due to many of the adults responsible for teaching lacking the essential skills to effectively teach. [31]

Word or phrase	What it means
BIK Youth Ambassadors	BIK Youth Ambassadors are a group of young peoplewho represent all European youth and who share their ideas on a safer internet experience with companies, organizations, and people that work to create a Better Internet for Kids.
Code of conduct	A code of conduct is a document that shows a set of rules that make sure that online services are safe for you. For example, it might say how old you should be to be able to use a social media app like TikTok or Snapchat, or the ways in which your information will be protected.
Decision-maker	A decision-maker is a person or group of individuals who is responsible for making important decisions for a big group of people. This could be in a company or in a country, for example.
Empowering	To empower means to give someone the power and the authority to do something. It means to both make someone more confident and make sure they have the possibility to do things
European Commission	The European Commission (or EC for short) helps to shape laws and policies in the European Union. For example, it makes laws on economy, the internet, and security
European Union	The European Union (or EU for short) is a group of 27 countries in Europe that work together.

Hate speech	Hate speech is a form of communication that uses negative, aggressive, and mean words towards an individual or group of people. It is usually focused on specific groups based on things such as the country they are from, the color of their skin, their religion, their gender, or more.
Inappropriate	Inappropriate means unsuitable or something that can cause harm or will make you scared. We often talk about online content or contacts that is, the things you see online or the people who contact you online being inappropriate for children and young people.
Media Literacy	The goal of media literacy is to help children and young people to become safe and wise users of all sorts of media, including books, magazines and newspapers, TV and radio, and online content. It helps them to think about the content they find, find trusted sources of information, and express ideas in a respectful way.
Online platform providers	Online platform providers are the companies that own the social media platforms that we are using. For example, Facebook, Instagram and WhatsApp are owned and managed by Meta, SnapChat is owned by Snap Inc., and TikTok is owned by ByteDance.
Policies	Policies are a set of rules, laws or plants that are chosen by governments to achieve a goal. For example, if the goal is that every child goes to school, a policy might be to build a school in every city. The European Commission helps to create laws and policies for the European Union and comes up with new plans to make the EU better.

Stakeholders	A stakeholder is an individual, group of people, or an organization that has an interest in a particular project or initiative. In this case, it means all those people interested in helping children and young peoplehave a safer online experience and giving them the skills and knowledge, they need.
Targeted advertisements	Targeted advertisements (or targeted ads) are adverts that use the information you put online or information on the websites you visit and show you ads that thinks you want to see. This can be a problem because these ads are trying to convince you to buy things you don't need, or they only show one side of a story.

Table 2. BIK+ words and phrases. [27]

2.2 Current cybersecurity teaching approaches in Finnish schools

As for the different curricula used in teaching in the schools around Finland, it is important for us to see and understand what they consider important regarding media, data privacy and cybersecurity.

Comparing differences between publicly available curricula and what different big cities have considered is important in order to better understand the importance of cybersecurity when it comes to protecting students.

There are many different teaching methods used to teach cybersecurity [17]:

- Lectures: In this traditional method, instructors teach theory and concepts in classroom settings. Students take notes, listen, and ask questions.
- Hands-on labs: Students engage in practical exercises or simulations to learn cybersecurity concepts and tools, allowing them to apply theoretical knowledge in a practical environment.
- Online courses: Courses are delivered entirely online, providing flexibility for students to learn in their own time. These can utilize a combination of videos, interactive simulations, and quizzes.

- Case studies: Real-world examples of security breaches serve as a teaching tool for students to analyze how the breach happened, its impact, and how it could have been prevented.
- Collaborative learning: This method encourages students to work together to solve problems, share ideas, and learn from each other.
- Gamification: This method uses game design techniques such as points, badges, and leaderboards to make learning more engaging and enjoyable. The usage of game mechanics in non-gaming contexts.

These methods are often combined to create a comprehensive cybersecurity education program.

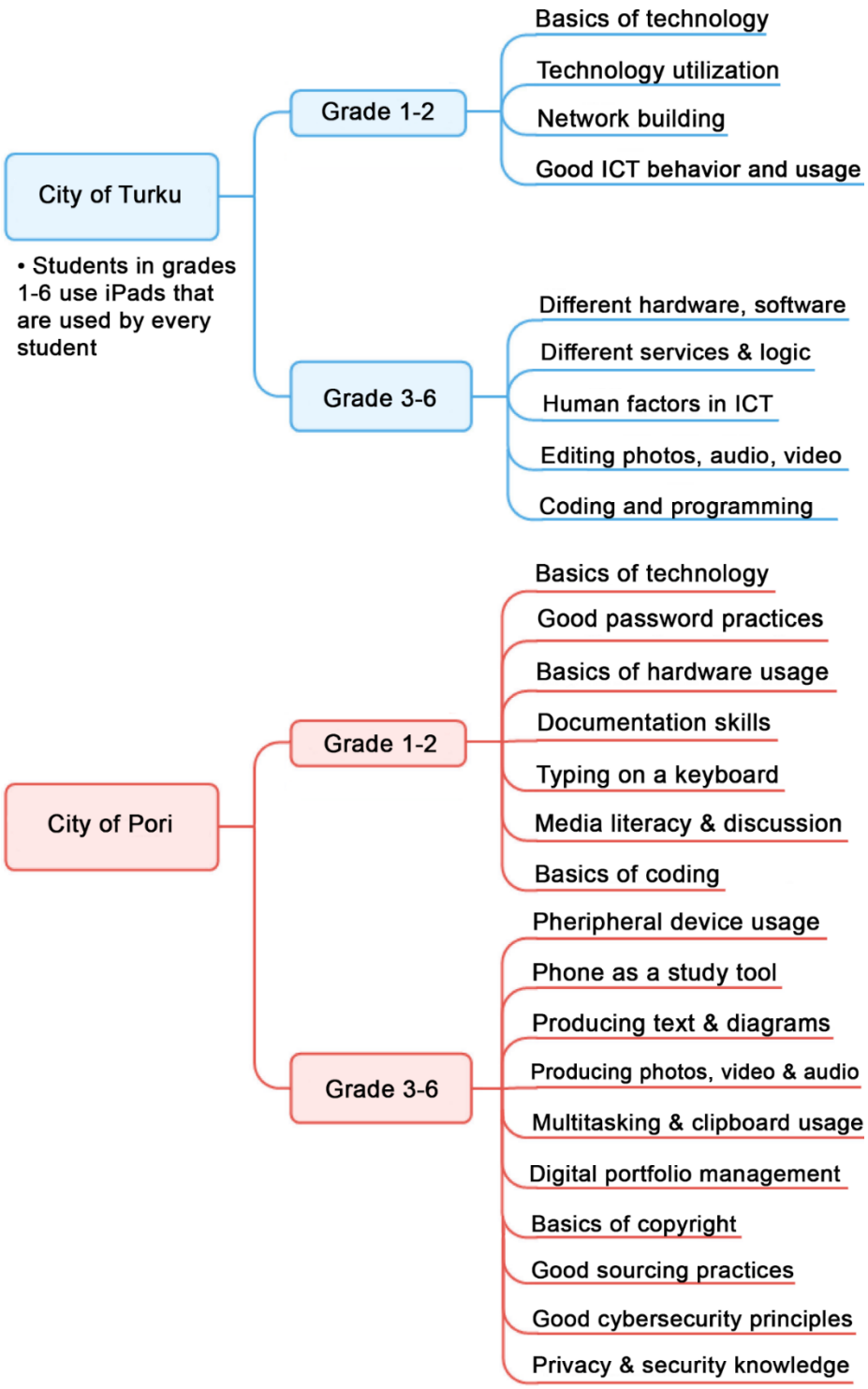

Figure 1. City of Turku & City of Pori's ICT education of the 2016 curricula

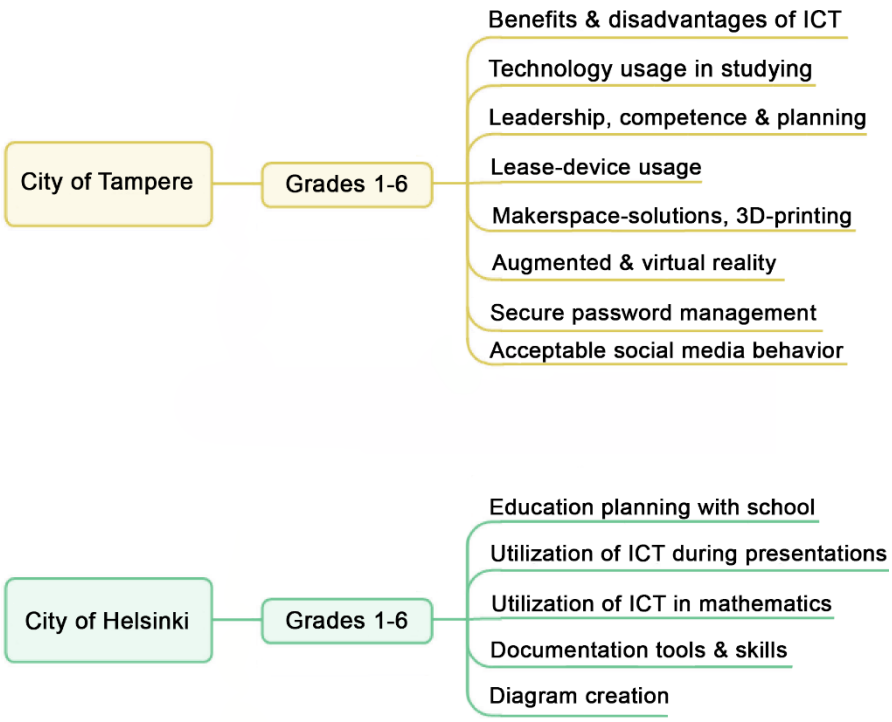

Figure 2. City of Tampere & City of Helsinki's ICT education of the 2016 curricula

2.2.1 City of Turku

To determine what types of cybersecurity knowledge and delivery approaches in official documents of four municipalities in Finland are examined and described. Most of the educational approaches are based on the instructions given by the Finnish National Agency for Education, however it is important to examine whether there are differences between municipalities to determine how differently they have approached the teaching approaches.

Information and communication technologies (ICT) is an essential learning subject and a learning tool that is utilized in each grade of basic education, in different subjects, and in multiple interdisciplinary learning modules. The students' learning of ICT can be categorized to four main groups:

1. Basic understanding of the usage and terminology of ICT, and development of their hands-on ICT skills while creating their own work
2. Learning how to use ICT responsibly, safely, and ergonomically
3. Learning to use ICT as a tool for information finding for research and creative purposes

4. Allowing students to experience and practice the usage of ICT through interaction and networking

For all the categories, students' own activity and propensity for creativity is useful in finding their own best work methods and possible future career paths. ICT offers tools to create students' thoughts and make ideas visible in many ways, which encourages the development of thinking and learning skills. The importance of collaborative learning and the pleasure of understanding is an important part of ICT education and can affect motivation to study positively. [32]

Students begin learning about ICT in their first and second grades. They learn how to use the technology, how it could be utilized in school and in their free time, and how to begin building networks between each other. Good standards of behavior and usage while using ICT is also practiced, primarily focusing on good work posture.

Children are encouraged to use and practice different tools and briefly explore topics that interest them, alone or in groups. Children also share their own thoughts when utilizing ICT. The positives about ICT mentioned is that they offer a natural and possibly a familiar way to teach languages in authentic situations. [33]

In grades three to six, students are encouraged to find, try, and learn to use different work tools and methods to best fit their own way of working and learning. Students learn how to use different hardware, software, and services, and learn to understand how they logically work. They also study and practice how to edit photos, audio, video, and how to create animations both alone, and in groups. Practicing coding and programming, students learn how technology is dependent on human choices and factors.

Students practice searching information from different sources through different search engines. They are encouraged to utilize sources for their own information creation and practice critical evaluation. They are also encouraged to find ways to express themselves, and utilize ICT in studying, documentation, and evaluation. [34]

The curriculum did not go into detail what type of learning the students go through when they are learning about ICT safety and responsible behavior, aside from the earlier mentions of learning the terminology. There was also no mention on how responsible and good behavior while using ICT is connected to cyberbullying and the risks associated with students using the internet.

Students in the grades 1-6 use iPads that are used by every student, ECO-PCs, and some computers that have been left unused by the middle school students [35]. One concern about the usage of iPads is that of security compared to Android devices; if the students do not learn the differences between the security of different operating systems, it could lead to them being more careless with their device security.

2.2.2 City of Pori

Most of the curriculum of the City of Pori is the same as the City of Turku; they both have listed what students should learn on the first through second grade, third through sixth, and seventh through ninth, specifying what students should know by the end of the sixth grade and ninth grade. The difference between Turku and Pori's curricula is that the city of Pori goes more into detail about what the students will learn, instead of leaving information somewhat vague.

In the first and second grade, students will be learning about the basics of ICT usage and terminology:

- Learning how to turn on and turn off a computer or a tablet in the proper way
- Learning how to use usernames and passwords, and understand the importance of them in terms of cybersecurity
- Learning the basics of the hardware being used, and understanding the differences between applications and different types of files
- Being able to produce text on their own, paste a picture to a document, understand the importance of saving the document, and the importance of the destination the document is saved to
- Learning the basic skills of typing with a keyboard based on the stage of the mother language
- Studying different topics through different types of learning games, learning the basics of media literacy, and learning to take part of discussions based on a picture or a video
- Having the possibility of learning the basics of coding through different activities, games, or applications

Allowing children to learn how to use ICT as a tool for information finding for research and creative purposes and allowing students to experience and practice the usage of ICT through interaction and networking, are the same as mentioned previously in the other curriculum.

In the grades third through sixth, students will use their earlier knowledge about ICT for more advanced studies:

- Students will be given personal accounts that they can use while working in different study environments that the school has provided
- Learning how to use peripheral devices, such as a camera or a printer in their studies with the hardware that they have
- Learning about using their own phone as a tool for studying, learning about using different types of text editing tools, and learning how to write and edit different types of documents both alone and in groups
- Learning how to produce text, diagrams, and how to share them with others
- Learning how to take videos, photos, and audios, and learning how to edit them
- Learning how to use multiple applications at the same time, and understanding the usage of a clipboard
- Learning how to do small programming work by themselves, and knowing how to organize their work in a digital portfolio

For the responsible, safe, and ergonomic usage of ICT, the students will learn about:

- Basics of copyrighted materials and copyright law
- Learning the best practices in sourcing their work
- Following good cybersecurity principles
- Understanding and creating strong passwords, and how passwords should be handled
- Protecting themselves and their privacy. This includes not sharing their personal information or pictures thoughtlessly, and not opening or downloading suspicious-looking emails or files

- Understanding what good behavior is while using ICT, not to share inappropriate material about themselves or others, and not to use inappropriate language
- Knowing how to ask for help while encountering security or other issues

The students will learn more about cybersecurity during the seventh through ninth grades; many of those notations are focused on management and creation of accounts, understanding how virus protection works and how to protect their devices, and understanding the consequences of their actions and the responsibilities of the criminal justice system when it comes to ICT. [36]

The curriculum goes into detail about how cybersecurity is taught in schools, but it leaves it vague enough to be able to be built upon later without the need for updating the curriculum plan itself, aside from some minor additions.

2.2.3 City of Tampere

The City of Tampere's curriculum itself did not iterate on the instructions given by the Finnish National Agency for Education. However, the sub-regional ICT strategy for the years 2019-2021 had much to say about the teaching methods of ICT, despite its strange absence on the curriculum page. [37]

Instead of seeing the digitalization and ICT as an alternative way to study, this sub-regional ICT strategy sees it as a necessity, teaching children about the benefits and disadvantages of ICT, the key threats, and the potential of ICT. To be able to use technology as a tool for studying and teaching, purposeful leadership, competence, knowledge, and planning is needed. The teaching organizer evaluates the implementation and realization of the plan.

The schools themselves lease devices instead of buying them, which allows students to learn and try a variety of devices without a need for commitment. Schools are also taking into consideration a Bring Your Own Device (BYOD) approach for teaching, where students bring their own electronic devices that they can utilize while studying. Schools can also implement Makerspace-solutions, 3D-printing, virtual and augmented reality solutions as collaborations between schools as different projects, or with third parties. These experiences are shared between sub-regions and are utilized in educational development work.

As for the students' cybersecurity knowledge, they will understand how to create secure passwords, and understand that passwords should never be shared with someone else. With this, they will understand what kind of behavior acceptable and what type of language students should use on social media platforms. [38]

Regardless of the strategy, the understanding of what the students are learning at schools is minimal, and the source materials that they have listed from the Finnish National Agency of Education has been either moved or deleted, meaning their guides and suggestions are unreadable.

2.2.4 City of Helsinki

Like the City of Tampere's Curriculum, the City of Helsinki has nothing to add to the guidelines of the Finnish National Agency of Education regarding ICT or cybersecurity [39]. However, they did have the foundation of their curriculum from 2014. There, they delve into more detail about the usage of ICT in education. As additions to the other curricula, they have mentioned that parents or guardians are able to participate in planning and development of the educational systems of the schools together with the school staff and students.

Students are encouraged to utilize ICT tools during oral evaluations or presentations. Schools will make sure that students have the chance to utilize these tools and get help when needed. Even minor learning issues are taken into consideration when planning and doing evaluation and presentation situations.

Mathematics education is enhanced with the usage of ICT by showing different types of tools, diagrams, drawings, and written material, especially during the first and second grades of school. This way, students can learn logical, creative, and punctual mathematical thinking, both alone and in groups, through different kinds of games. Most of the ICT studies that were mentioned, that go further into detail about what students will be learning, are during the seventh through ninth grade. [40]

Much of the information given was based on the guidelines of the Finnish National Agency of Education, and this information regarding the teaching of ICT and cybersecurity has not been updated since 2014, or at the latest 2016.

2.3 Cybersecurity awareness for children

There has been significant research done on children's understanding and awareness of different types of cybersecurity and ICT-related issues, such as online privacy related issues, and exposure to inappropriate content and pornography [12], as well as how it can be improved with several different methods.

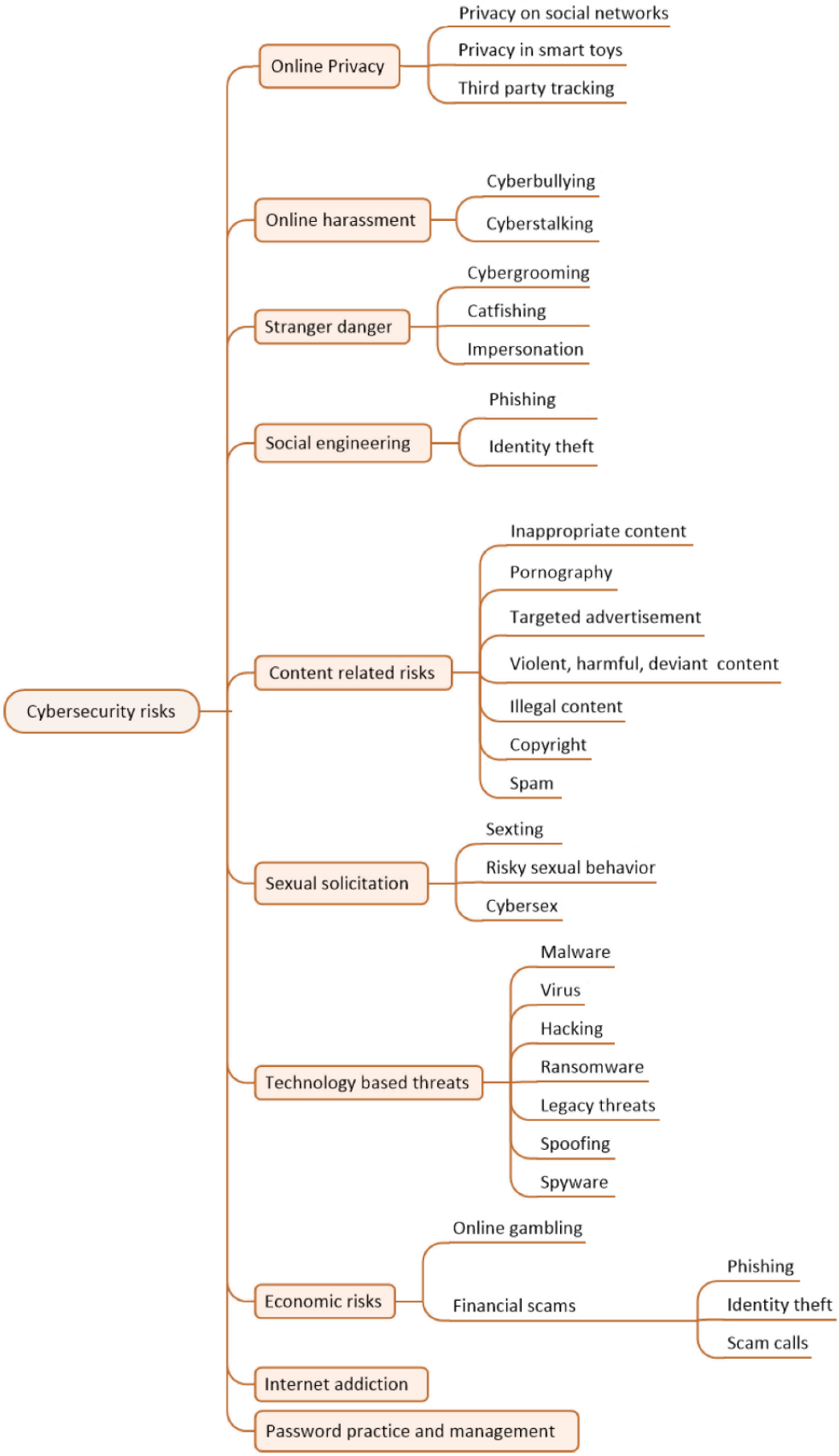

Figure 3. Cybersecurity risks. [12]

From the curricula of the different cities, we could see that children are taught about online privacy, economic risks, and password practice and management, but it leaves out many important elements of the understanding of cybersecurity and its risks. The curricula only mentioned content-related risks, online harassment, and technology-based threats partially or during later grades of education.

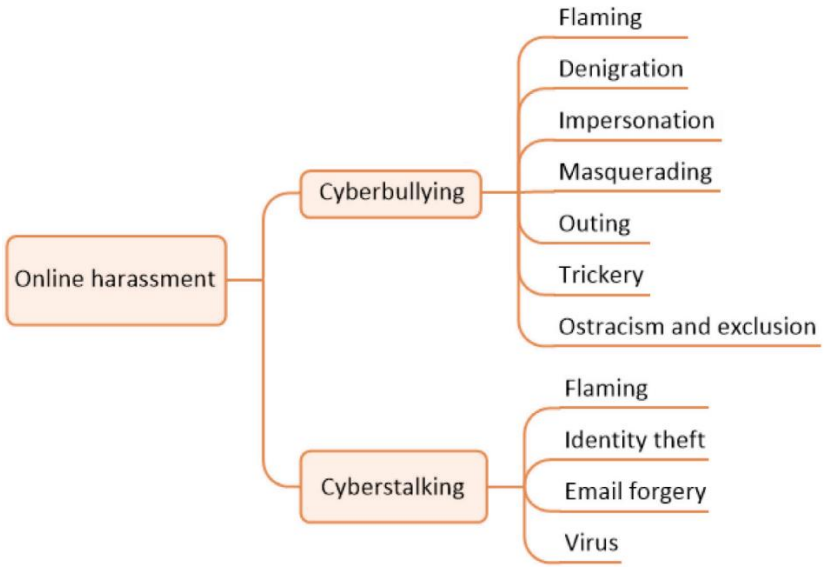

Figure 4. Cyberharassment and cyberbullying. [12]

Despite research on cyberbullying and different varieties of behavioral and psychological issues related to cyberbullying, it was left unmentioned in the curricula – including, surprisingly, on the topic of school bullying and bullying prevention.

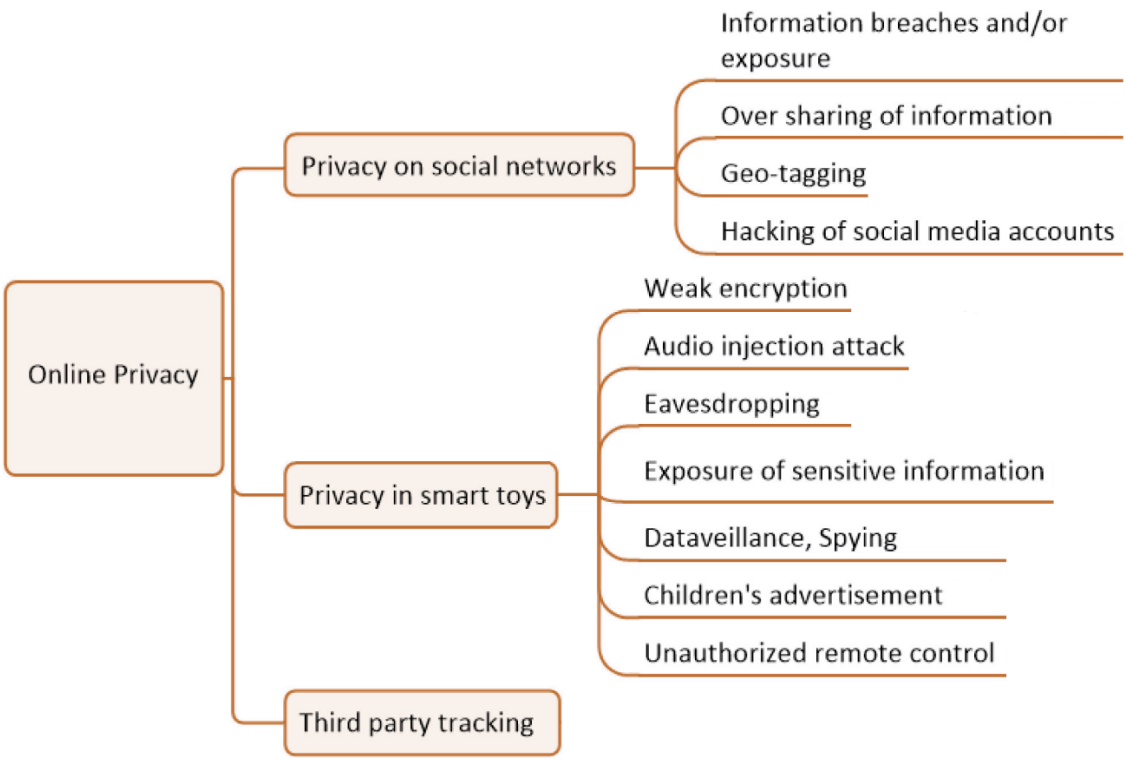

Figure 5. Privacy-related risks. [12]

Although online privacy was covered well in the curricula, it omitted certain areas that are pertinent for children to understand. An especially important example of an omitted area, is the poor privacy protection of "smart toys", considering that an increasing number of toys are connected to smart devices through Bluetooth and Wi-Fi, leaving them exposed to cyberattacks with little to no protection. Young children, of course, are especially vulnerable to cyberattacks via the means of smart toys. Some of the toys have the function to take pictures and record voices that can be played back to the child, but the information saved in these types of toys can be potentially accessed by attackers. Some of these toys can be further used to gain access to the whole home network. There are multiple potential risks involved in this, varying from privacy related risks to risks related to cyberstalking. People often say and do things in the privacy of their homes that they would not otherwise, which can lead into different types of issues, such as identity theft, blackmail, and cyberbullying.

2.4 Philosophical and ethical standing of cybersecurity

With the increasing need for cybersecurity and cybersecurity education, it brings forth questions about the philosophy and ethics of cybersecurity and technology. Philosophy and ethics can be used to provide tools and concepts to tackle and prevent rising cybersecurity issues, such as the usage of Artificial Intelligence (AI) in cybersecurity, which has become an

important element of both defense systems and attack systems. There are plenty of philosophical values that can be investigated when thinking about cybersecurity [41]:

- Security
- Privacy
- Fairness
- Accountability

Cybersecurity can be divided into multiple topics, such as information security, and the CIA triad (confidentiality, integrity, and availability) of (computer) data. This can bring forth morally problematic issues and questions about the protection of humans and valuables that could be used to potentially harm them, which can range from data breaches and loss of data integrity, all the way to cybercrime and cyberwarfare. The amount of critical information keeps growing, and the safety and integrity of the data should be one of the highest priorities of cybersecurity.

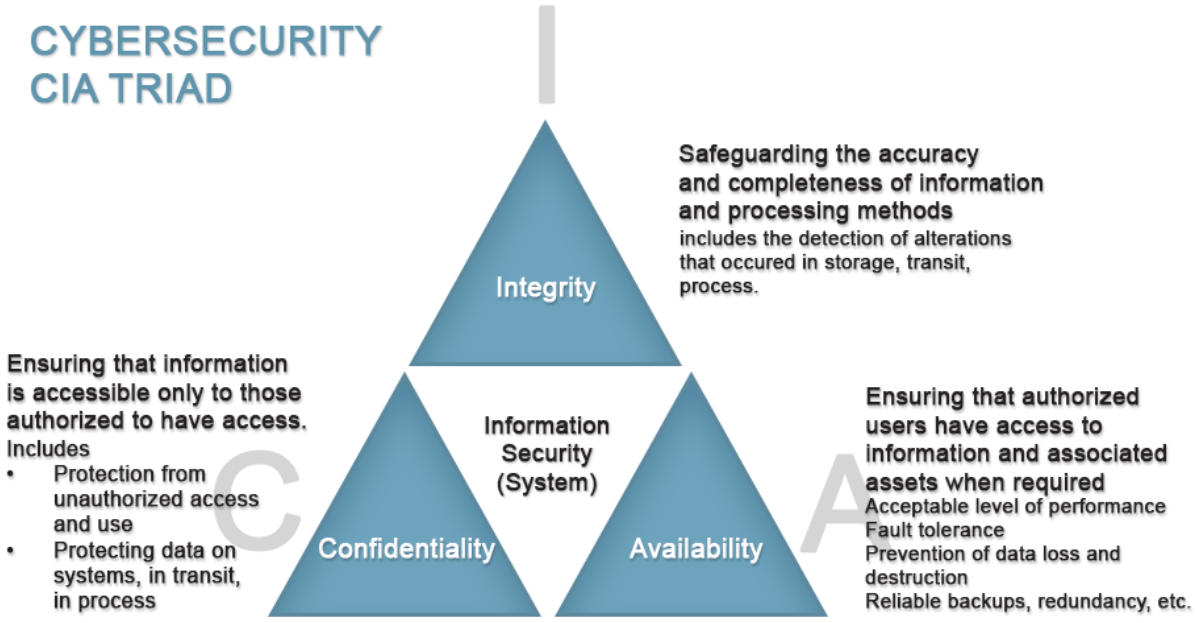

Figure 6. The CIA Triad. [42]

The philosophy of cybersecurity is rooted in the principles of ethics, particularly in the areas of privacy, confidentiality, and integrity. Privacy is a fundamental right that allows individuals to have control over their personal information. Confidentiality is related to

privacy and involves the protection of sensitive information. Integrity is the maintenance of the accuracy and completeness of information.

Privacy is related to many concepts; identity, liberty, anonymity, confidentiality, moral autonomy, human dignity, and personhood as examples. Cybersecurity serves to counter that which compromises these aspects of privacy. As an example, saving and sharing people's personal and private data without their consent, and sharing them to third parties that benefit from the data without the knowledge of the data owner. [41]

There have been steps taken to neutralize some of the morally and ethically questionable problems with the GDPR, which gave users a lot more control over their personal data, and minimized the kind of data that companies are allowed to save about the user. Fairness can be seen as other things as well, such as justice, accessibility, freedom from bias, and non-discrimination. Currently, cybersecurity threats, and measures on how to avoid them, do not affect everyone equally. This brings forth another type of moral problem: equal cybersecurity measures and threats can undermine civil rights and liberties of individuals and countries depending on their laws and regulations, which might prevent them from using the internet the same way as others can. [41]

Unequal treatment results in injustice. Anonymity and invisibility can be the only barriers between a person of justice and one who is unjust. [43] Anonymity and invisibility on the internet can be a double-edged sword; on the one hand, it allows people to use a Virtual Private Networks (VPNs) to hide their private data from third parties, but it also allows them to watch shows and connect to websites that they would normally not be able to, due to region locks. This may be morally questionable, but it is not inherently wrong. On the other hand, anonymity can give people a sense of power over people. As mentioned in Chapter 2, it can be used for online abuse.

Accountability itself can include values such as openness, transparency, and explicability. Accountability can be used to weigh in on the conflicting values of cybersecurity, which includes the obligations of individuals and organizations to take accountability for their actions and behaviors that have been found unjustified. As an example of this, Google was given a $400 million dollar penalty for illegally tracking people's location without their consent and is now required to provide detailed information about the location tracking data and show transparency on the matter. [44]

The ethics of cybersecurity involve balancing the need to protect sensitive data with the need to maintain availability and accessibility. There is constant tension between these two factors, and cybersecurity professionals must navigate these issues with care and responsibility.

Regarding the ethics of cybersecurity, there have been two broad approaches to it. One approach can be done by utilizing core moral theories, such as utilitarianism, which is an ethical theory that determines right or wrong by focusing on the outcome to cybersecurity. Another approach is developing different middle level ethical principles for cybersecurity contexts, commonly known as principlism. In principlism, there are four basic principles of autonomy, justice, beneficence, and non-maleficence. [45]

One issue with using ethical theories as guidelines is the way in which they contradict and conflict against each other instead of operating in a complimentary matter. Another important problem is that they may be too complex to be effectively used for real-life scenarios and issues.

Most of the current cybersecurity ethics frameworks use the principlist approach, where they specify ethical user principles of cybersecurity [45]:

- Beneficence: A ‘good’ within the just society
- Non-maleficence: A right to non-interference to prevent harm
- Autonomy: An aspect of human dignity
- Justice: A right to be let alone
- Explicability: A right to freedom from arbitrary surveillance

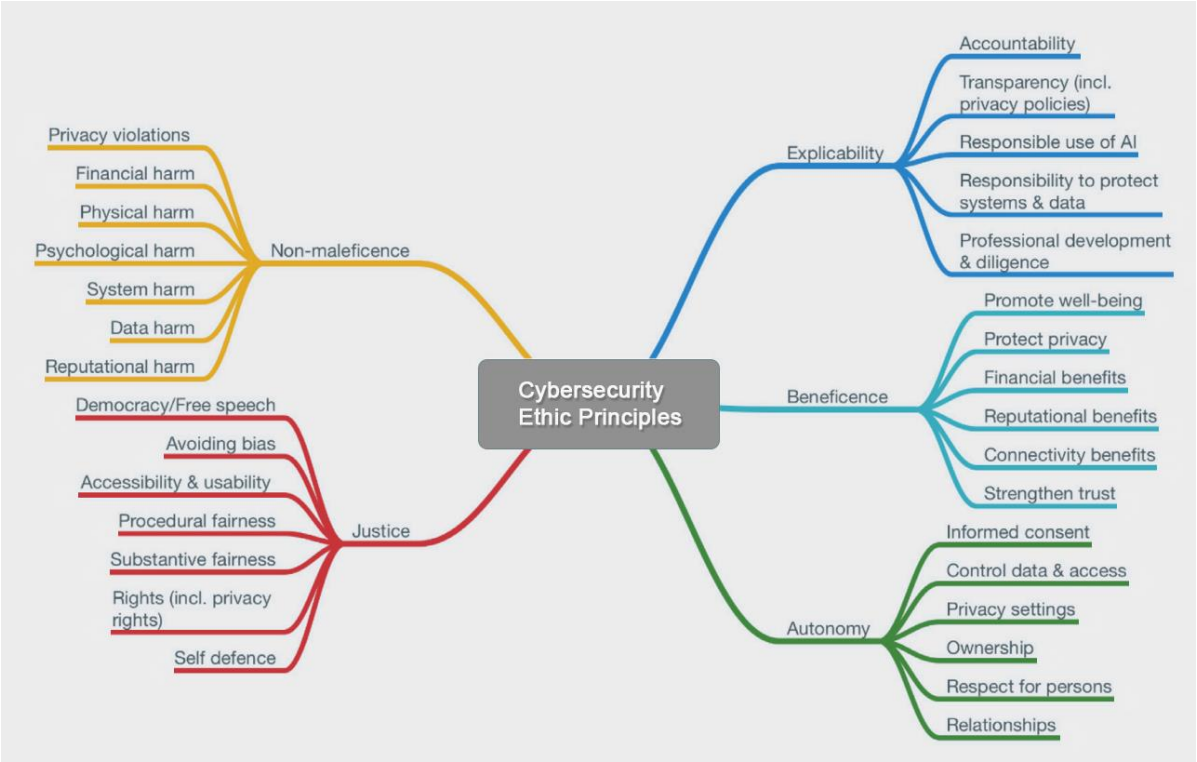

Figure 7. Five cybersecurity ethics principles. [45]

The major problem of the principlist framework is privacy. The definition of privacy is complex and wide, and often encompasses many things, such as [46]:

- Freedom of thought
- Control over one's body
- Solitude in one's home
- Control over personal information
- Freedom from surveillance
- Protection of one's reputation
- Protection from searches and interrogations

The multifaceted nature of privacy brings challenges of its role and function within a principlist framework – regardless, privacy could be included as a component of the non-maleficence principle alone as a right for non-interference. This can only work in certain definitions of privacy, however, as the definitions might conflict with each other.

This definition of privacy is not absolute, and it could indeed be used in alternative approaches by incorporating privacy as its own ethical principle to bring diversity to the existing framework. This approach, however, ignores the conceptual relationships between the existing principles (Figure 6) and privacy. [45]

As the importance and relevance of cybersecurity keeps growing, it is important to understand the different types of philosophical and ethical problems that it can bring, and how complicated the issues can be. Many ethical problems in cybersecurity require cybersecurity professionals to balance the technical aspects of their jobs with ethical considerations to ensure that they act in the best interests of their organizations, society, and individuals.

3 Methodology

This chapter aims to explain how the interviews were conducted and examine how scientific literatures' viewpoints of the questions in chapter 1.2 differ from the viewpoints of teachers and cybersecurity professionals. Chapter 3.1 begins by describing the philosophical standing and ethics of cybersecurity, and how they can be used to tackle some of the problems that cybersecurity teaching is currently facing. Chapter 3.2 goes into detail about the search strategy used to facilitate finding answers to the research objectives and questions. Chapter 3.3 goes through the interview process of the thesis; questions asked to gather the data and then going through the process of analyzing the data that has been gathered.

3.1 Search Strategy

The research objectives in chapter 1.2 were formulated to examine the current situation of cybersecurity teaching, when should it be taught, what should be taught, and how it should be taught, to see if there are ways to improve the cybersecurity education in the Finnish education system. Therefore, this research methodology follows a qualitative research method. [47]

The literature review serves as a foundation for understanding the current state of cybersecurity teaching in education, what types of information and material are available for teaching purposes, and how up to date the materials are. It also gives insight on the curriculum of four different cities, mentioned in chapter 2.2, to see how they have published their ICT and cybersecurity teaching methods in the curricula publicly.

The qualitative case study complements the literature review by collecting firsthand information through interviews from different cybersecurity professionals and teachers. The combination of these methods allows for a better understanding of the research topic, the issues that it is facing, and how it could be changed for the better in the opinion of the teachers and cybersecurity professionals to conclude how it could be done in the future.

The gathering of the research data started quite early in the process to get a better understanding of the current situation of cybersecurity education in terms of research papers, educational materials, European Union strategies regarding cybersecurity, and the ethics of cybersecurity. However, the interview questions were designed around the existing literature

to get answers to key questions and areas that are still relevant in the existing studies and cybersecurity literature.

3.2 Interviews

This section aims to explain how the interview process has been completed and how the interview questions are related to the research objectives introduced in chapter 1.2. Section 3.3.1 begins by describing the process of recruitment of the interview participants and why they were chosen to be interviewed. Therefore, section 3.3.2 continues with the interview questions asked from the interviewees. Section 3.3.3 goes further into the data analysis process and goes into the strategy used to facilitate finding answers to the research objectives and questions by analyzing the gathered empirical data.

To gather data for the thesis, there were interviews done for both teachers and cybersecurity professionals. There were 10 interviews done that were audio-recorded, transcribed, and translated from Finnish to English for further analysis.

For the demographics of the interviewees, there were simple questions to find about their gender identity, age, current occupation title, and their understanding of some of the terminology commonly used in cybersecurity to get a better understanding and view on whether some of the terminology was easier to comprehend or important for the interviewees. Interviews were fully anonymous; therefore, the interviewees provided themselves nicknames.

3.2.1 Participants and recruitment

For the participants, the interviewees, emails were sent to different schools and cybersecurity professionals to find willing participants for the study. There were five teachers and five cybersecurity professionals who were willing to participate and give their opinions on the topic. The teachers that were interviewed worked with students in middle schools, mostly in the seventh grade to ninth grade, though some of the teachers taught younger classes as well. The cybersecurity professionals worked on multiple types of work assignments, which provided a greater variety of answers to analyze.

The interviews were meant to give the interviewees an opportunity to bring up issues and suggestions for changes that they would personally like to see happen, and how they would go about teaching cybersecurity, or how they would suggest the education to be deliver

in a way most beneficial for the students' learning. The interview questions were the same for each teacher and cybersecurity professional but were left open enough for them to determine how to interpret the question in accordance with their understanding, as the questions were structured to be opinion-based questions, instead of factual questions.

The interviewees were selected by using a method of purposive sampling, which is a method used in qualitative research approach to highlight the research questions as the basis for the participants [48]. The aim of using a qualitative research method was to get an in-depth understanding of the teachers and cybersecurity professional's own understanding of cybersecurity education, their experiences with ICT and cybersecurity, and perspectives to see when and how they handle the education of cybersecurity for children and adolescents. For the sake of protecting the interviewees privacy and anonymity, the places of work and their personal information will not be described in this thesis.

Out of the 10 interviews, four of the teacher's interviews were conducted in-person despite the busy schedule during the spring semester, and others were conducted via online meetings, whichever was more convenient and possible for the interviewees was chosen. The interviews lasted from approximately 30 minutes to 60 minutes. All the interviews were recorded and transcribed to facilitate the analysis of the results later in the process.

Lastly, after the interviews, the interviewees were asked to fill out some simple questions regarding themselves, and their knowledge regarding some areas of cybersecurity to get a better understanding of what areas might be more lacking than others.

Give yourself a codename	Are you a teacher or a cybersecurity professional?	What grades do you teach?	What is your gender?	What is your age bracket?	What is your highest level of education?	How many years have you been doing your current job?
Mustarastas	Teacher	Classes 8-9	Female	40-49	Master's degree	25
Kesäheinä	Teacher	Classes 7-9	Female	30-39	Master's degree	15
JR	Teacher	Classes 1-9	Female	30-39	Master's degree	13
Jäärä	Teacher	Classes 7-9	Female	60+	Master's degree	31
Saimaannorppa	Teacher	Classes 4 and 7-9	Female	40-49	Master's degree	4
Saippuakauppias	Cybersecurity professional		Male	40-49	Bachelor's degree	5
Vihreä Varis	Cybersecurity professional		Male	50-59	Master's degree	5
Olutmies	Cybersecurity professional		Male	30-39	Bachelor's degree	1
Vanhakettu	Cybersecurity professional		Male	40-49	Bachelor's degree	6
Punainen Leijona	Cybersecurity professional		Male	30-39	Master's degree	2

Table 3. The demography of the interviewees.

As for the areas that they were questioned about, they were based on the key areas mentioned in the figures of chapter 2.3. The key areas were:

- Authentication
- Cyberbullying
- Cybersecurity
- Internet addiction
- Online gambling
- Online hate
- Online etiquettes

- Online marketing
- Pornographic content
- Sexual exploitation
- Sexting

The interviewees answered these questions by checking between numbers 1 to 5. Number 1 meaning they were not very knowledgeable about the topic, and number 5 being that they were very knowledgeable about the topic.

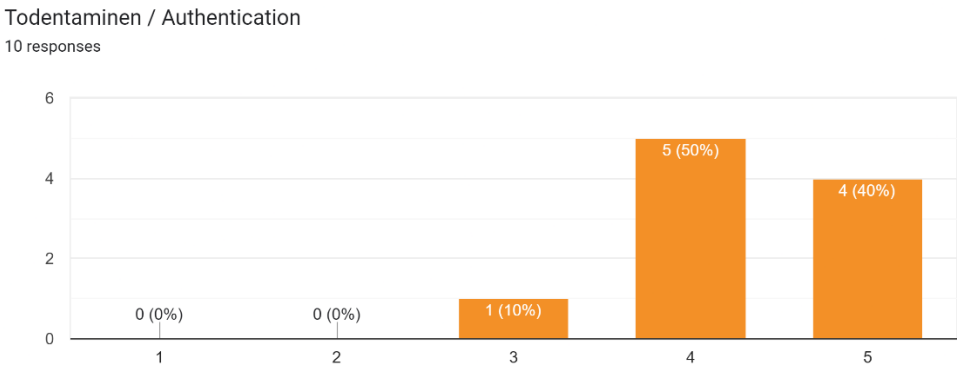

Figure 8. Knowledge of the interviewees regarding authentication.

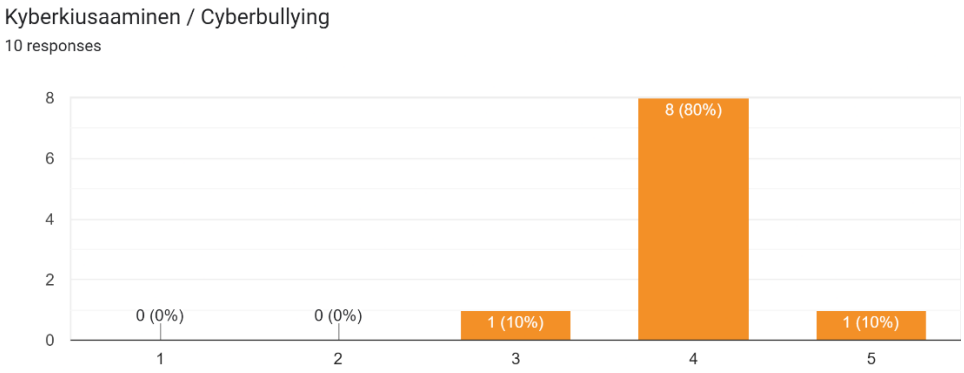

Figure 9. Knowledge of the interviewees regarding cyberbullying.

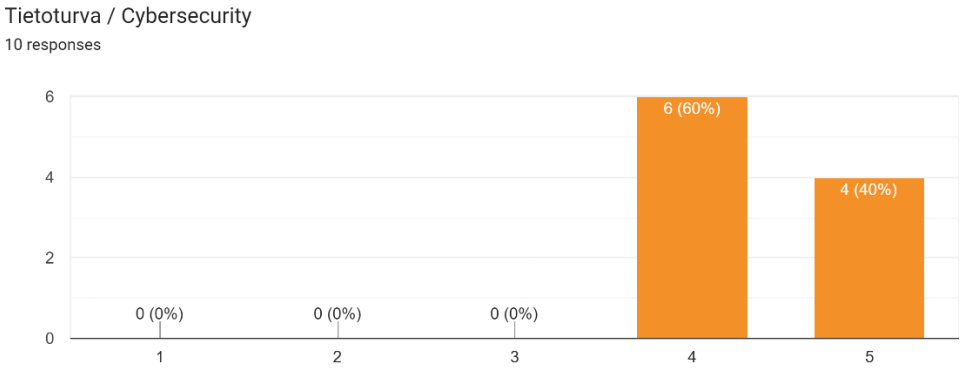

Figure 10. Knowledge of the interviewees regarding cybersecurity.

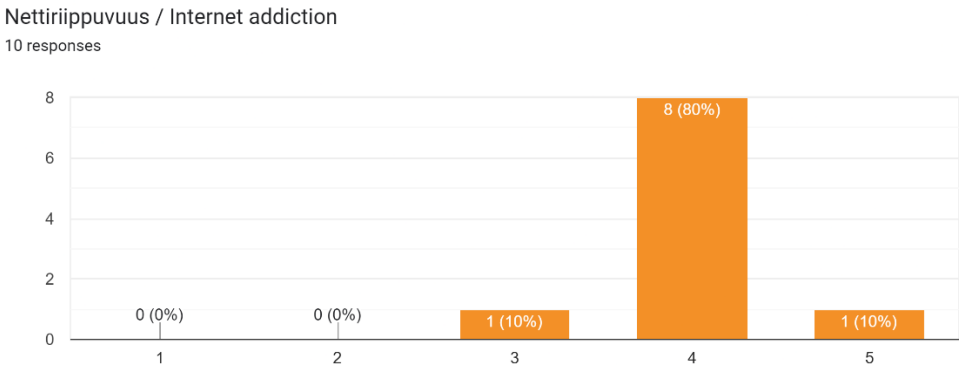

Figure 11. Knowledge of the interviewees regarding internet addiction.

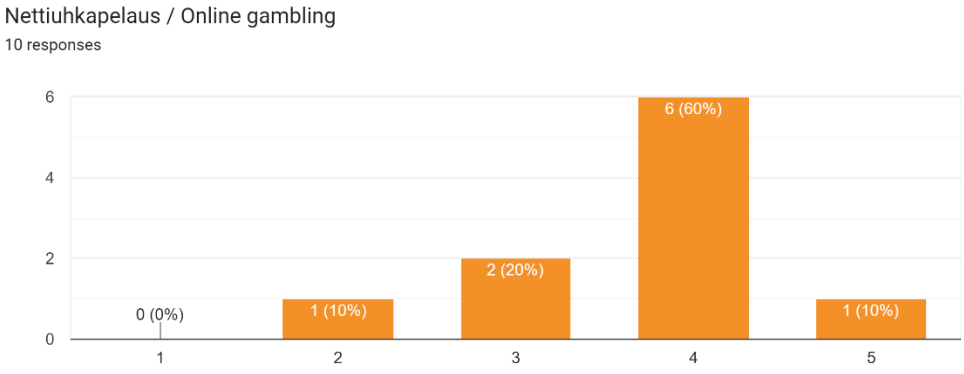

Figure 12. Knowledge of the interviewees regarding online gambling.

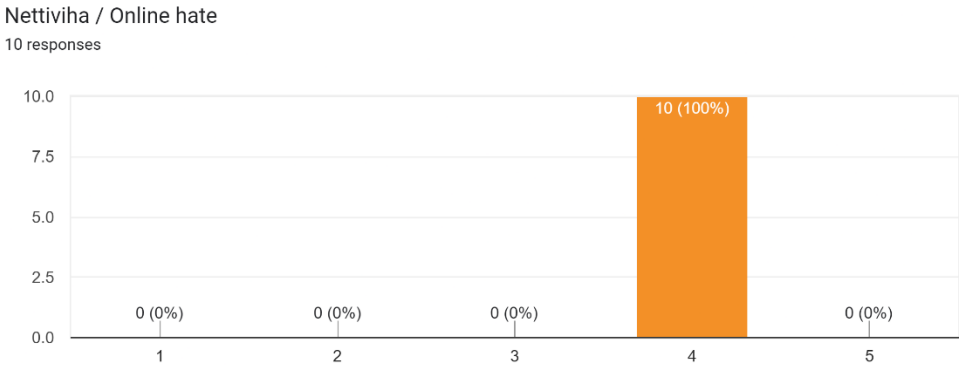

Figure 13. Knowledge of the interviewees regarding online hate.

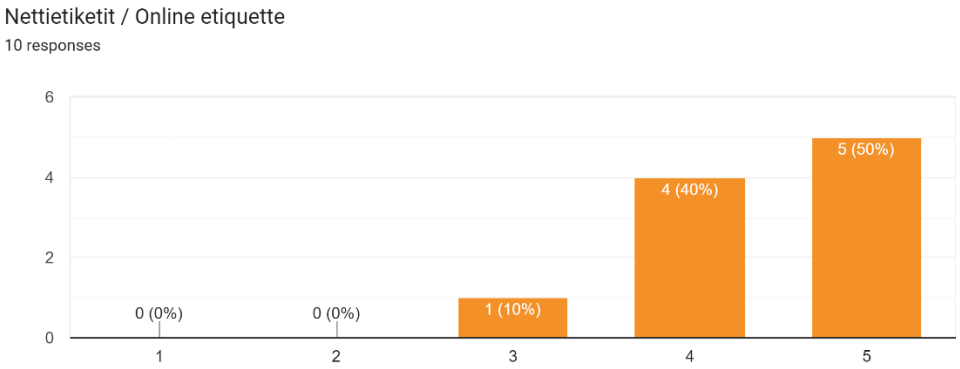

Figure 14. Knowledge of the interviewees regarding online etiquette.

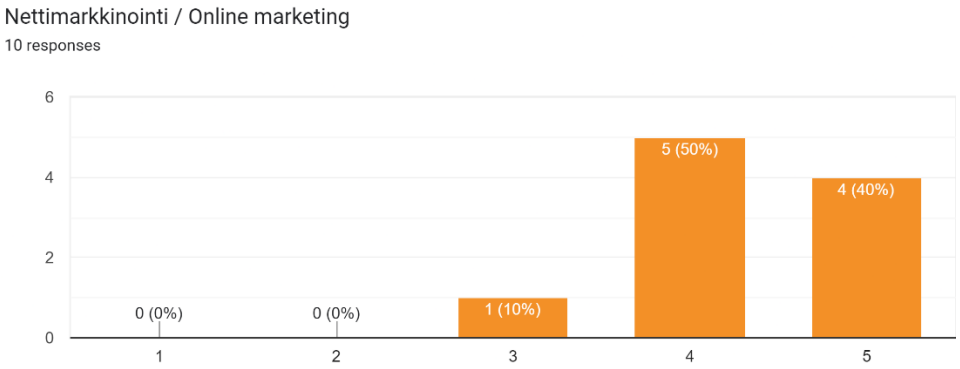

Figure 15. Knowledge of the interviewees regarding online marketing.

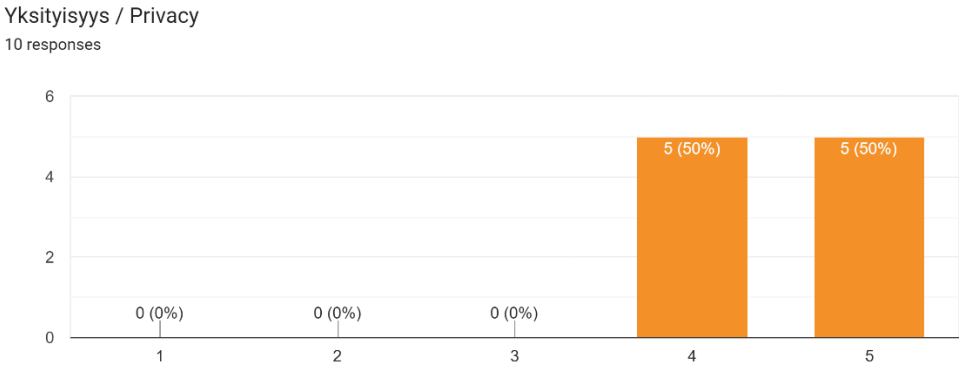

Figure 16. Knowledge of the interviewees regarding privacy.

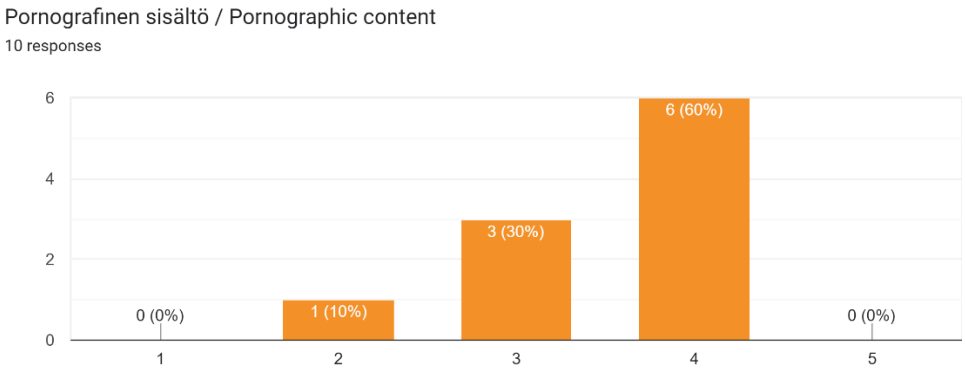

Figure 17. Knowledge of the interviewees regarding pornographic content.

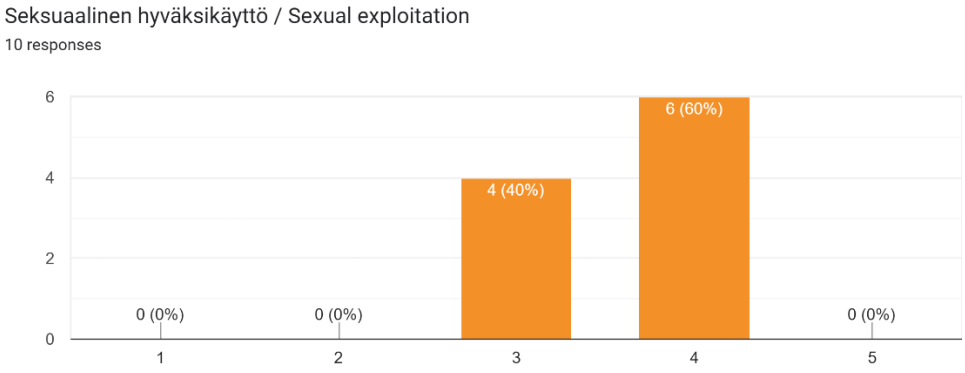

Figure 18. Knowledge of the interviewees regarding sexual exploitation.

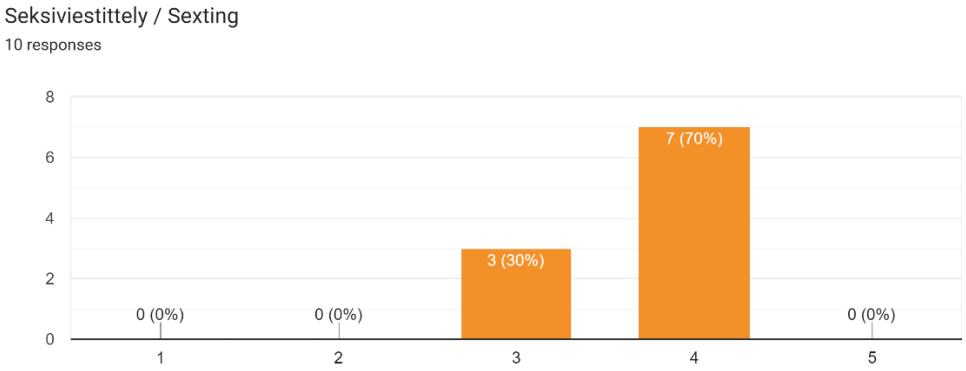

Figure 19. Knowledge of the interviewees regarding sexual exploitation.

3.2.2 Interview questions

As mentioned in Chapter 1.2, the interview questions will be revolving around the thesis' research questions:

- When should cybersecurity be taught about?
- What should children and adolescents be taught about cybersecurity?
- How should children and adolescents be taught about cybersecurity?

As the topic of cybersecurity is a broad subject, as seen in the figures of chapter 2.3, asking the research questions directly would not give sufficient data to analyze what the key areas and problems in the current ICT and cybersecurity education are; therefore, the questions had to be expanded on to be able to get the most out of the research questions.

However, asking the same questions from both teachers and cybersecurity professionals would not be possible, as we cannot assume that teachers are knowledgeable about cybersecurity, and that cybersecurity professionals have worked with children. For this reason, some of the questions are different for both teachers and cybersecurity professionals, while keeping the major questions the same.

The interview questions were divided into three different categories: What, when, and how, for convenience to help with the analysis process of the thesis.

#1. When (Both):

- Should a child or an adolescent's internet usage be monitored? How should that be done?
- What concerns do you have about children and adolescents's safety and cybersecurity on the internet?
- Safety meaning: to protect children and adolescents from harmful and illegal online content, conduct, contact and risks.
- Can you name three issues that children and adolescents could face due to internet use? Feel free to say more if you think there are many issues.
- In your opinion, which one is the biggest problem?
- At what age do you think children and adolescents would understand the concept of cybersecurity?

#2. What (Teachers):

- Do you think teaching ICT is enough, or should it include cybersecurity?
- What should be taught to children and adolescents regarding online safety and cybersecurity?
- Do you think there is a need for improvements in the existing teaching materials?

#2. What (Cybersecurity Professionals):

- How can cybersecurity knowledge be best shared with children and adolescents?
- What is the best way to teach cybersecurity skills to children aged 10-15?
- In your opinion, when should children be made aware of cybersecurity threats/challenges, and in what way?

#3. How (Teachers):

- Have you heard of the Better Internet for Kids strategy (BIK+)?

- Do you think children and adolescents enjoy using electronic devices, for example, iPads, at school?
- In your experience, for what purpose do children and adolescents use their electronic devices besides schoolwork?
- Would you mind cybersecurity or ICT being its own subject in schools? And if not, if you had to choose, what subject would you switch for ICT or cybersecurity?
- Would children and adolescents benefit from ICT or cybersecurity being its own subject?
- Would teaching ICT or cybersecurity be too overwhelming for children and adolescents as its own subject?
- In which ways can cybersecurity be made interesting to children and adolescents?

#3. How (Cybersecurity Professionals):

- How should teaching material be kept up to date?
- Have you heard of the Better Internet for Kids strategy (BIK+)?
- Do you think children and adolescents enjoy using electronic devices, for example, iPads, at school?
- What do you think children and adolescents use electronic devices for beside schoolwork?
- Would children and adolescents benefit from ICT or cybersecurity being its own subject?
- What methods would you use to teach cybersecurity for children and adolescents?

3.2.3 Data analysis

The purpose of the data analysis is to analyze, compare and compile the answers of teachers and cybersecurity professionals, as mentioned in chapter 1.3, to determine whether cybersecurity is taught enough in the current curriculum in Finnish schools. Likewise, asking what else should be taught to determine the key areas that need to be changed in a way to

make it more beneficial for the students' learning. After this, it is compared to already existing literature for teaching cybersecurity for them, to see whether the answers of teachers and cybersecurity professionals aligns with the existing literature, and if there are some key areas that the literature does not mention.

The gathered data from the interviews can be analyzed the best with a thematic content analysis process where the goal is to identify common themes between the interviews, common patterns during the interview analysis process, and compare them to the already existing literature to see if the key areas are like the existing material [49]. Out of the different data analysis methods, thematic content analysis is suited best for this research, analyzing the gathered data from the interviews can be used to see whether it supports the existing literature, and possibly fills gaps and brings forth issues that the existing literature does not mention regarding the teaching of cybersecurity of students in Finnish schools..

First, the transcripts were read a few times to go through the notes and main key areas that were mentioned in each one of the interviews. However, there were some preliminary interpretations and findings that were already made based on the interview data before the actual interview analysis process. The preliminary interpretations and findings were made to focus on the already uncovered problems and statements that could help find more relevant literature to compare with the interviewee's answers for the analysis process.

Next, the different key areas that commonly appeared in the interviews could be divided into different types of themes that could be more thoroughly analyzed with existing literature. Different themes can be examined and linked together to create larger categories while bearing in mind the research objectives and questions, allowing the possibility to compare different types of data with one another [50]. Finally, the last step of the thematic content analysis method was aimed to find conclusions regarding the findings to discover possible suggestions and possibilities to improve the cybersecurity teaching methods.

4 Findings

This chapter aims to show the findings from the interview process and how the findings are related to the research objectives introduced in chapter 1.2, to find out when, what, and how cybersecurity should be taught to students in Finnish schools . The findings are based on the interview questions in chapter 3.3.2.

As seen in chapter 3.3.2, the interview questions were divided into three different categories. The categories have then been divided into chapter 4.1, chapter 4.2, and chapter 4.3 based on the research objectives of the thesis to help draw out the conclusions in a categorized manner, as the objectives cannot be summarized within one single category. However, this gave the opportunity to categorize the data further as mentioned in chapter 3.3.3, as the categorization aids to notice key areas and issues that have arisen based on the interviews. [49]

To ensure the quality of the data, the questions for the interviewees were kept opinion-based, instead of knowledge-based, to limit the potential biases that may have come up during the interviews. The interview questions were not given to the interviewees to avoid biases and avoid allowing them to think about the questions beforehand to ensure the quality of the data to be purely opinion-based. This was also to avoid the interviewees from researching different topics from the questions before the interviews themselves.

However, the findings were only based on a small pool of interviewees, which limited the amount of data to draw findings and conclusions from. There is a reason to suspect that there was some bias regarding some of the interview questions, depending on the age of the interviewees and if they had children of their own.

4.1 When should cybersecurity be taught about?

As seen in chapter 3.3.2, the questions asked to teachers and cybersecurity professionals remained the same, as the key points of the questions revolved around monitoring, safety, and understanding of cybersecurity. More specifically, chapter 4.1.1 focuses on the opinions of the interviewees regarding monitoring of children and adolescents, chapter 4.1.2 focuses on the key concerns of the interviewees regarding their usage of the internet, and lastly, chapter 4.1.3 focuses on the interviewee’s opinions regarding at what age should concepts of ICT and cybersecurity should start being taught for them.

4.1.1 Monitoring the internet usage of children and adolescents

The reason for this question is to find out how teachers and cybersecurity professionals feel about the monitoring of children and adolescents, while leaving the question vague enough to give room for opinions on monitoring at home versus at school and whether monitoring should be done the same by parents and teachers.

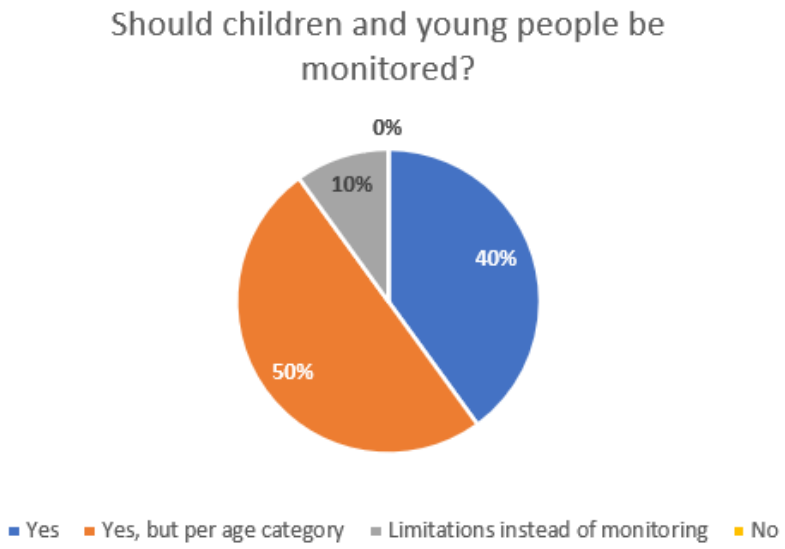

Figure 20. Should children be monitored according to the interviewees.

Based on the answers from the teachers, the consensus was that theyshould be monitored regarding their usage of the internet. However, there were varied answers regarding how strictly they should be monitored. The monitoring should vary depending on the age group of the minors. Starting out, it should be done more strictly through limiting what types of applications and content the children are able to use and watch. They might not understand the consequences and dangers of the internet which could have far-reaching consequences on their lives. The majority of teachers thought that it should be done up until quite late into teenage years, if needed. However, the older the minor is, the more lenient the monitoring should be, as being too strict can lead to trust being broken.

One teacher nicknamed Kesäheinä mentioned regarding monitoring:

> *"The most essential thing is not that you monitor what your child is doing on the internet, rather it should be more about teaching what type of internet usage is safe, beneficial, or level-headed, and what type of usage is not, rather than disallowing them from doing something. The monitoring should not have the "Big Brother is watching you" mentality (like in George Orwell's novel 1984), as it is not the best*

option. But of course, the stricter type of monitoring can work for some, such as having limitations on screen time, or on applications they cannot use without a password. The teaching should be done and built on through providing correct information and through discussion with them."

Teachers themselves mentioned that the stricter monitoring methods, such as checking the minor's phones to see what types of applications they use or whom they talk to should be done by the parents, instead of a teacher. The monitoring of them in schools should be to ensure that they focus on the materials of the class, rather than browsing websites or using applications that they are not allowed to.

Cybersecurity professionals had a different opinion on the matter and strictness of the monitoring. The monitoring and teaching of safe internet usage should be adjusted according to the age group of minors . Some cybersecurity professionals thought that the teaching should be on the same level as any other daily basic skills, such as using a sharp kitchen knife safely. However, this should majorly be done by the parent. When the education for safe internet usage starts young, learning about it is easier later in life, even if they are different types of individuals, their education and interests go hand-in-hand.

However, a major problem with the education at home is that most parents are not well versed in technology, as they lack media literacy skills, are unaware of the scope of ICT and cybersecurity. Another major problem is that strict monitoring of children could be infringing upon the rights of their privacy.

As mentioned in chapter 2, the European GDPR and BIK+ strategy is there to reinforce the safety and privacy of children on the internet, and they have their rights to privacy. Strict monitoring can easily infringe on their privacy, especially if it is done outside the home environment. However, they require consent and permission from their parent or guardian when an application or website wants to monitor and use their personal data, since they are likely less aware of the risks and consequences of sharing data and their rights. The age threshold for the parental consent is between 13 and 16 years old [51]. In Finland the age limit is 13 years, when a child is allowed to consent for their personal data to be used [52].

4.1.2 Internet safety and concerns regarding children and adolescents

The reason for this question was to find out different key concern areas according to teachers and cybersecurity professionals, and to see if the answers were something that the literature

suggested according to the literature mentioned in chapter 2. Another reason was to find out if there were some specific problems that have arisen in recent years that the literature has not yet taken into account.

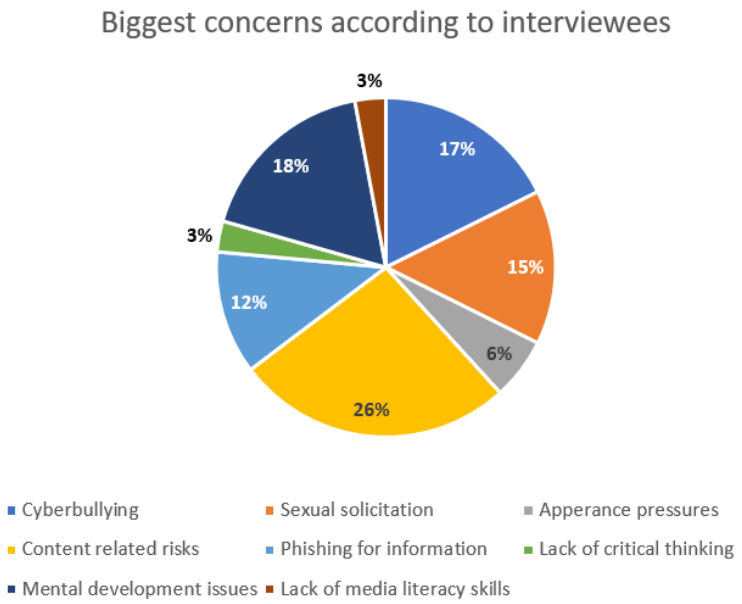

Figure 21. Biggest concerns according to the interviewees regarding children and adolescents' internet usage

The biggest key area found within the question regarding the concerns of their internet usage was that they have access to vast swathes of information, immediately, once they have access to the internet. One point mentioned by the interviewees was that the parents do not care or know what type of information and content is available on the internet, nor do they know what types of applications their children can use without their permission, as it is very easy to create fake accounts by lying about one's age.

Teachers' answers were more focused on students feeling pressure to be like someone else, stemming from the use of social media platforms such as Instagram. Teachers report that Instagram has been affecting self-image and self-confidence; this was more apparent in younger girls than boys.

Another major key concern mentioned was the inappropriate content that a minor can see on the internet, which can affect their mental development. For them it is harder to understand what type of information is true, and what is fake, which can lead to them having a twisted view of certain topics or lead to them to a "black and white" view on various issues. They lack the ability to think critically and lack the media literacy skills to understand that

some content on the internet is faked for “entertainment purposes”. They are more likely to spread disinformation, or attempt viral challenges they see on different types of social media platforms, which can lead to permanent injury, or even death. It is easy for a minor to believe what they saw, since disinformation is easy to spread. One teacher mentioned how easy it is for disinformation to spread among students, as they feel the pressure to share something that their friend has shared to them and have seen others sharing as well.

Some of these dangerous challenges that have been widely reported on have been the “Tide Pod Challenge” and “Blackout Challenge”. The Tide Pod Challenge was a challenge where children and teenagers were eating detergent pods and filmed themselves doing it for different social media platforms as they resembled gummy candies [53]. The Blackout Challenge, also known as the “Choking Game” or “Pass-out Challenge” is the challenge where a person tries to hold their breath as long as they can and filming themselves doing it for different social media platforms [54]. Both of these challenges were linked to them being more prone to taking risks. However, their ability to calculate risk is less sophisticated than most adults, leading them to dangerous activities exacerbated by peer pressure. As social media trends have been grown in popularity, peer pressure has gone from a simple friend group or classmates to potentially millions of people pressuring them into trying out different challenges and broadcasting it for potential fame and popularity [53].

With the growth of social media and the anonymity that the internet provides, another key issue mentioned especially by the teachers was bullying and sexual harassment, which can lead to aforementioned mental development issues, attempting potentially dangerous challenges, or affecting their self-image. As mentioned in chapter 2, bullying and especially cyberbullying can affect the development of a minor negatively, as it can lead to depressive symptoms [24]. Sexual harassment, on the other hand, is prevalent because children do not understand the consequences and dangers it can lead to. It is easier for predators to use social engineering tactics (such as fake identities, profiles, lying about age) on a child to groom them. Grooming is defined as manipulative behavior that the predator or abuser uses to gain access to potential victims, convince them to be complacent with abuse, and reduce the risk of being caught. [55]

Another issue that was mentioned by the majority of interviewees was oversharing, especially when it regarded the personal information of a minor. They do not understand the potential dangers of oversharing information, and not thinking what type of information

should not be shared on the internet, which can lead into dangerous or harmful situations. Teachers mentioned that yearly they have heard of private pictures being shared or leaked, both spread around at school, and on different types of social media platforms. Minors are less likely to understand the consequences of sharing private photos and information, which then can lead to further cyberbullying and sexual harassment.

4.1.3 Understanding the concept of cybersecurity

The point of the question was to find out what age group would be the best suited for teaching cybersecurity according to the teachers and cybersecurity professionals, and then giving their reason for that. However, the answers varied depending on the interviewees understanding of cybersecurity topics and what is included in cybersecurity rather than ICT.

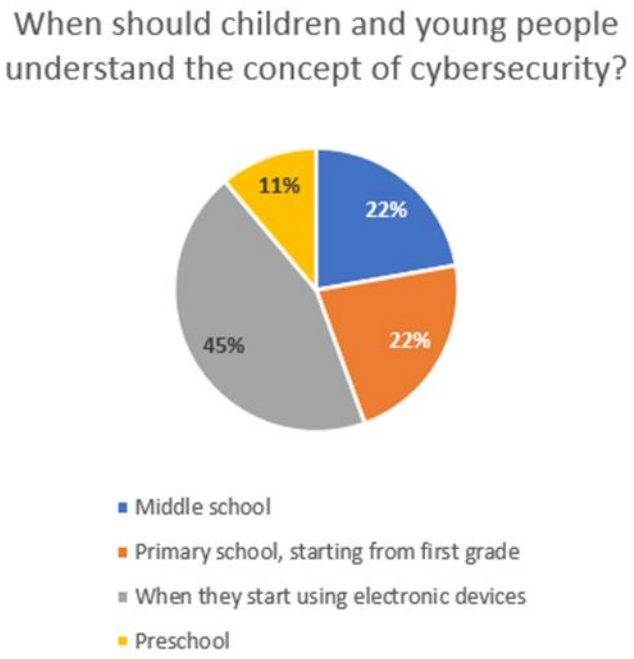

Figure 22. When should children and adolescents understand the concepts of cybersecurity according to the interviewees.

The answers from teachers were vastly different from one another. Some answers varied from starting to teaching cybersecurity after the age of 10; there were mentions that even some students might not understand the concept of cybersecurity even at the age of 14. However, other teachers reported that teaching should be done per age group, on the level of a child, mentioning that there were obvious topics that younger children would not be able to understand, but if the material was made with different age groups in mind, it would be easier

to teach it, and understand the basics of cybersecurity and build on the knowledge from there, as one would with any other school subject.

These teachers thought that it would be best for students to learn the basics of ICT and especially cybersecurity starting from the first grade, or even before that with the guidance of the parent. The examples of "basics" are, for example, a child's ability to remember their own password, alongside ensuring a strong password is used. Another basic cybersecurity practice is allowing a parent to also know the child's password too when they are young, while also acknowledging that this level of trust could be abused by the parent, if the password is used in multiple places.

There was also the mention of writing the password down on a piece of paper to remember it. Writing passwords down on a piece of paper carries a stigma of being an insecure method. However, with the digitalization of the world, writing passwords down on a piece of paper is nowadays more secure than some password manager systems, as it is more unlikely for a hacker to steal the piece of paper, rather than breaching the password management system where they are stored. Teaching people that writing passwords down can only burden their memory, making them more likely to reuse already existing passwords, or have bad and weak password practices. [56]

Cybersecurity professionals had a different opinion on the matter, mentioning that teaching should start from the beginning once the children have access to electronic devices. However, they did acknowledge that they do not trust parents to effectively teach the subject, as parents likely lack knowledge about the concept of cybersecurity themselves. This is why professionals emphasized the importance of schools when it comes to teaching the concepts of cybersecurity for children and adolescents. A specialist nicknamed Vihreä Varis mentioned this about the issue:

> *"Schools must have a big role in this because I do not trust only homes. Some homes are more aware of the issues than others, but there is a big mass of people who are not aware of these types of issues. The schools have an obligation, and it must sharpen the children and adolescents' knowledge, but the schools themselves are behind times when it comes to the ICT education. The current school curriculum was finished in 2016, and they started forming it since 2010-2011, the world was way different back then. Of course, it has some digitalization baked in, but it is badly behind. In the*

curriculum, they have mentioned all the things of digitalization, and they were already acknowledged then, but they are not actually in the curriculum.

So that something can be taught in practice, it must be done in the way that teaching mathematics or native language, or something similar like that. The information needs to be so firmly set in the curriculum, that it is acknowledged and understood, and should not be just glued on alternative studies that you can teach. It must be a part of the school subjects, the curriculum, and the study material. The teaching materials are often done by viewing the curriculum and using it to create textbooks that reflect the information in the curriculum. Of course, they have tried to glue on some teaching materials created by the Ministry of Education and Culture, where we have noticed that the curriculum is behind the current needs and issues. This type of parallel program that schools can and should monitor, but taking it into practices a big problem, due to it not being tied into school subjects. They do not say at what point you should teach these things, rather they have extra after-school lessons for this.

We must acknowledge that the knowledge of teachers regarding this topic is poor, and the education and training of teachers do not prepare them for these things in Finland, except maybe on a surface level. The organizations educating and training teachers are even more clueless about these things, and are disconnected from the real world, especially when we talk about the common digital skills in the education of teachers. Teachers should be taught something about coding, programming, how to work different types of digital environments, and especially teach them about data privacy and cybersecurity. Our teachers have not been to teach about the topics, but of course, there are different updating trainings, but we can only reach a limited number of teachers. Teachers are unsure and timid about teaching about topics that their students are more innate at. This topic is a tough problem to fix."

4.2 What should children and adolescents be taught about cybersecurity?

In this chapter, the aim is to see what should be taught about cybersecurity. Chapter 4.2.1 focuses the opinions of teachers regarding bringing ICT or cybersecurity as its own school subject and to hear how they would like to see it be integrated into the curriculum in the future. Chapter 4.2.2 on the other hand focuses on the expertise of cybersecurity professionals to hear more about their opinions on how they would keep the teaching material up to date and what type of information they would personally teach. For this, keeping the information

separate from one another will give a best understanding of the different views that the interviewees have.

4.2.1 Teachers' views on teaching about online safety and cybersecurity

Many of the teachers thought that ICT on its own is not enough, and the core problem is the lack of ICT education and if some teachers teach about ICT voluntarily, there is not enough time reserved to do it properly, due to them having to teach everything else that is already set in the curriculum. Despite ICT and cybersecurity being needed, teachers acknowledged that the current teaching will never be enough for the modern world due to the strict schedule that things must be taught. However, must also be noted that some thought that parents expect the teachers to do the entire teaching process of ICT and cybersecurity, when they think it should start from home, as it is part of the parents' responsibility to teach their child as well.

Starting basic education from home would be beneficial for minor's learning as they age. Furthermore, it was also noted by one teacher that it is dependent on what type of a municipality it is, what type of school, and what type of teachers the school have, as there are many different variables that can affect what type of ICT education students currently are receiving. Some teachers, for example, might be more interested in teaching something regarding cybersecurity and ICT, despite not knowing everything about it, for the pure sake of wanting to provide students with the information on how to protect themselves on the internet, and what types of dangers can hide in there.

Regarding what should be taught to the children and adolescents regarding online safety and cybersecurity, teachers unanimously agreed that they should be taught about protecting their privacy and information. The teachers were worried about the content that they watch, what type of information they share, and what type of content they post online. Regarding the topic and how students should be taught about the issues, one teacher nicknamed Kesäheinä had this to say:

> *"In the key position is certain kind of criticality regarding every type of picture, post, comment, et cetera, on the internet, so in a sense having some type of critical media literacy. It is in the key position because learning it young will teach them that even if some picture shows something, it might not be true after all, and I think that one important point is also to teach them to a certain type of discussion, as I mentioned earlier (Chapter 4.1.1), since you cannot block out everything that a child or an*

adolescent sees on the internet, they would have someone they could easily talk about the things they have seen, be it whatever they saw. And the discussion should not be the type where it is "Why are you watching that type of content?" because it is not always their decision to see it, and sometimes it just comes up whether they want it or not. So, the discussion should rather be more about what they saw, and did they have any thoughts about the things they saw.

Teaching that everything can be discussed about, and teaching not to believe everything you see, and also, which is in my opinion a problem nowadays, that you should not share everything immediately without stopping to think if you have read the whole thing, or watched the whole video, or did you watch this without audio, so you do not even know what they were talking about in the video, and just shared it, because everyone else was sharing it. This type of misinformation sharing can spread like wildfire, therefore teaching some type of consideration filter would be important as well. And of course, teaching that the most important asset that you have on the internet is your own private information. You should be very strict with them, that should you post your address, phone number, age, or anything else to places where they are not needed at after all."

Most teachers are unsure what type of teaching material was readily available for them since there were so many different types of teaching materials. It was difficult for them to know what type of teaching materials would be the most beneficial for the students, as they were either not age categorized, or the materials were significantly scattered. Teaching the scattered material was dependent on how interested they were in teaching the topic; however, once again the issue with this was that there was no time reserved for it, and even if there was time, there was no clear package of teaching materials that the teachers could teach.

On the other hand, there was acknowledgement that the current teaching material is way behind the times with rising concerns regarding AI and deepfakes. The teaching simply cannot keep up, or there is no teaching material that is kept up to date. A teacher nicknamed Kesäheinä mentions another major issue here:

"The problem in a way is that we have a certain perception nowadays that children and adolescents are quote unquote 'diginative' (a person who has grown up with the presence of digital technologies, and having grown up with it, they are comfortable and fluent in technology), and they really are not. Well, maybe in a way that yeah

surfing surfing surfing, and click click click, and yeah video video video, and yeah TikTok TikTok TikTok, and something like that. Ergo, they can understand the entertainment side of technology, but the utilization side is kind of lacking. When I think about work life, like making meetings and generally hosting, organizing, and the netiquette how to behave in meetings, or how some texts are supposed to be written. You cannot really write 'um lol' (internet lingo in general), or write the text in a way one would write a comment, rather one should be able to write pragmatically rather fast too, when you think about it, that you should take notes at a meeting and still be able to listen and write at the same time, it requires the type of multitasking skills. And then I think about that we have the type of a barrier when they come to school, and they can easily have the assumption, that 'yeah, we know how to use the internet or a computer, or whatever it might be'. And when we try to tell them 'Well, there is this that you don't know', it is a little problematic in my opinion, the teaching should be different with the teaching materials and the whole point of the education. It cannot be 'Now listen to this lady say and warn you to be careful on the internet' all the time, that is also stupid, teaching cannot be demeaning from above type of thing, rather it should really be material on the level of their age group, and the kind of material that shows clearly that they have this material has this type of benefit, which can maybe motivate them to think about the teaching materials, even if they can surf the internet well.

Even in normal google searches we came across problems when we were searching for abbreviations. The students were googling the uppercase H letter, and they found out anything that was asked. We were searching for the Vety (Hydrogen), but we got all kinds of stories what it is, and I listened to them baffled what the search results were that they found. And when I told them that we were looking for hydrogen, they were like 'oh, I saw this on google though'. So, we looked it up, and it was the first google result, and mind you, it was not any globally known abbreviation, rather it was just something that happened to pop up there for some reason or another. This is sort of a problem as well, where they think that they can quickly search for some information, which might not be correct at all, or not the information that they were looking for.

They do not stop to think about it and realize like wait a minute, this is not the information I'm looking for, and how do I find the information that I want. That is the

problem. The sort of 'do not post nudes on the internet' is starting to be something that they understand, which is important to talk about of course, but the teaching materials should be focused more on the point of view of useful purpose and work life skills."

4.2.2 Translating cybersecurity expertise for education

Many cybersecurity professionals thought that the best way to share cybersecurity knowledge for children and adolescents was to approach them per age category. However, some of the methods were varied from each other. Some of the ideas that the professionals mentioned:

- Gamification
- Leaflets (physical & digital)
- Cybersecurity education (similar to tobacco education in schools)
- Learning materials per age category

While cybersecurity professionals were unsure as to the best means of providing education, they had plenty of ideas what should be included the learning materials and in the education itself. Most were adamant that cybersecurity and ICT education should be treated as one would treat teaching them; for example, how to use kitchen knives (as mentioned in Chapter 4.1.2). A professional nicknamed Vanhakettu had this to say about the issue of sharing cybersecurity knowledge to children and adolescents:

"I would say the how in this question is essentially the type of a question, if you want to share the information about cybersecurity, the person who is sharing should understand the facts and issues already quite well. They do not necessarily need to be a cybersecurity professional, or an ICT nerd, or someone who has worked on the ICT field for long, but they need to know about the subject, understand the consequences and causal connections, and understand the technology behind it. We do not need to go on code level, but say if you post a video to SnapChat, you should understand what can happen to the video, what does it technologically mean, the different types of formats that can happen to it.

So being conscious about the subject, and having a real want to understand the environment, in this case we are talking about digital environments what children and

adolescents use. If we think about city environments, where a child or an adolescent is allowed to go, I am sure it is obvious to most parents and educators, that the children are allowed to go, what places and what times of days are not appropriate, and so on. The environment they understand in one way or another, but it is the same way digital environments should be understood as well. If you do not understand them, it is hard to educate your children or your students at home and at school."

Many of the professionals mentioned that the problem is that teachers and parents' lack of teaching materials that would teach them and help them teach their children at the same time. If they do not understand what they are teaching, neither will their children. If the material was categorized per age, it would be easier for the parents to learn about the subjects involved in it as well. Of course, there are different types of teaching materials mentioned for the parents and teachers, but as mentioned in Chapter 4.2.1, the material is too scattered to be helpful. If the parents do not know anything about the topics and issues, how would they know what type of teaching materials they should be looking for to educate their children with.

As for the best ways to teach cybersecurity for children, teaching should be something that they would be interested in and should not only be text and monotone repetition. The teaching materials should be something that they can approach easily and enjoy, be it through different types of media, applications, videos, gamification, et cetera. But some thought that talking about the issues and topics is also important, as mentioned in chapter 4.2.1 by the teachers, especially due to the rise of new technologies, such as artificial intelligence chatbots such as ChatGPT. One professional thought that some kind of education where one person goes around schools showing facts and consequences of irresponsible internet usage with different types of media and examples without beating around the bush, treating them as one would adults could also be possible, similarly to how education about smoking and violence has been done in schools. Regarding this, a specialist nicknamed Vihreä Varis had this to say:

"The best way that we have found is that we create teaching materials for teachers, the type of teaching material that the teachers can teach through that, and we give them instructions how to teach them. This does not vary from teaching, for example, mathematics, the teacher gets a math textbook to teach from. Of course, the teacher knows how to teach it, but we give them a teaching plan. The middle schools are not the only ones, we are creating at least a teaching package for four different age

categories in primary schools and middle schools regarding data privacy, cybersecurity, and personal and school electronics. And how we strive to ensure that it passes through all the age groups, making sure everyone gets it and is not reliant on the teacher's interest, we created this where a principal is responsible for their own department. The principals acknowledge during the yearly check to make sure that in their schools every single student group, meaning classes 7A, 7B, 7C, et cetera., has received the education to pass the seventh grade, and that every single student on the seventh grade has gone through the same education. The dates, and if there are multiple classes, then dates from those, and so on. We made this for primary schools, middle schools, and the first years of high school are getting one too. The essential thing are the teaching materials we are giving to teachers, and some kind of monitoring mechanism. Of course, many can argue that the materials that we are producing in our organization might not be the best, or if there is a better alternative. But essentially it is the same thing if it was a math textbook published by Otava or Sanoma Pro (Finnish book publishers), but I am not going to comment on that issue, but this is how it should be done.

This is handled by the biggest cities, there is the Ministry of Education and Culture's New Literacies Programme, which is also done the biggest cities. The City of Kuopio has a good website called Digitaitokalenteri.fi (digital skills calendar) which you can check out. They made it with project funding, and we have borrowed some of their ideas, and given some of our own ones for their calendar. We could say that the Finnish cities in front have already brought digitalization quite far, the City of Pori is one of them. Pori was the first big city in Finland, where they introduced personal computers in education in 2017, and during the COVID-19 pandemic most cities followed suit. After the pandemic we noticed that the number of personal computers distributed before was beneficial in those types of situations, and another thing was that during the couple of years of teaching subjects digitally taught itself quite fast. We have around 15-20 municipalities or cities in Finland that are doing this in front, but if we take Satakunta as an example, Finland is starting to become inequal in that the City of Pori has done this for a long time, but no other city in Satakunta has done anything. We are coming to a critical state that organizations do not have the broadness when there needs to be support organizations, there cannot be just principals and teachers, there needs to be somebody who is thinking these things

through, and some kind of development organization. In Finland there are a little over 300 municipalities, and around 20-40 of them are in ahead, living their own bubble where they are developing things rapidly and taking things forward, but then we have the 260 municipalities that are clueless about these things. We are doing this type of impact evaluation about our own digital systems, which is a huge headache due to them being tied to American cloud services. In the cloud services, there are a lot of information about our children and youth due to the EU not providing an alternative cloud service. Of course, we need the Google and Microsoft tools, and it would not work if we just used Linux computers. We are spending a lot of times on the impact valuations and their technical security methods, but this still only applies to around 15 municipalities that are doing this, and the rest of them have never even thought about the problems that we are shoving a lot of student information to servers and services outside of the EU."

The new literacies program launched in autumn of 2020 for the years 2020-2023, made by the Ministry of Education and Culture of Finland, aims to strengthen media literacy skills, competence in ICT and programming skills of students, starting from early childhood education all the way to lower secondary education.[56] The purpose for organizers of teaching and early childhood education to update their digital strategies and plans as well as their curricula to reflect the national reference framework for digital competence of Finland. The detailed definition of competence promotes equal opportunities for studentsto achieve the digital competence needed in studies, working life and social participation. The Ministry of Education and Culture are working with the Digital Compass of Finland (Suomen digitaalinen kompassi) to create future strategic foundation for advancement digital education. Among with the creation of the policies of digitalization regarding raising and education, the description and development of digital knowledge will continue inf the future. [58]

As mentioned in the chapter 4.1.3, cybersecurity professionals concluded that ICT and cybersecurity education should start once the minors get their hands on the electronic devices. The teaching should be done little by little per age category, as complex topics are harder for younger people to understand and comprehend properly.

The teaching material could and should be kept up to date with a yearly checkup and updating, due to technological changes and innovations that happen every year, such as, the uprising of crypto currencies and usage of Artificial Intelligence (AI). Be it from the usage of

AI to in art competitions [59], or the usage of ChatGPT to create documentations, which is leading schools and Universities to rethink whether it can be used as a tool or is it a cheating engine [60]. These types of innovations are creating a problem, the research and the teaching materials cannot keep up with them.

There were some ideas from professionals to tackle the sudden changes as well. One of them recommended an organization of cybersecurity personnel would come together to create teaching materials and go around teaching teachers at schools about the new and rising topics and issues, so they can be taught immediately when it is necessary, rather than next year, when the topic is already dated. One of the examples of these types of communities that were given was the KyberVPK Community Cyber Response Force, which was established to help providers of critical services to fight against cyber-attacks and recover from them [61].

4.3 How should cybersecurity be taught to children and adolescents?

In this chapter, the aim is to gain a better understanding of teachers' and cybersecurity professionals' knowledge and thoughts about how theyuse their electronic devices, the currently existing strategy, and whether ICT or cybersecurity should be brought as its own subject.

Chapter 4.3.1 focuses on the Better Internet for Kids (BIK+) strategy, to find out how many of the teachers and cybersecurity professionals have heard of the introduced strategy. Chapter 4.4.2 focuses on the thoughts of teachers and cybersecurity professionals to find out what type of purposes do they think children and adolescents use their electronic devices for. Chapter 4.3.3 focuses on the interviewee's perspectives and thoughts whether ICT or cybersecurity should be brought to schools as its own subject, and how they would like it to be integrated in the future to tackle of some of the problems that have been brought up in previous chapters.

4.3.1 Knowledge about Better Internet for Kids (BIK+) strategy

The question regarding the BIK+ strategy mentioned in chapter 2.1.2 was an interesting one. The European Union clearly had worked on a strategy to protect the children, but asking the interviewees if they had heard about such initiatives is helpful in finding out how widespread the knowledge of said strategy in EU member countries actually is.

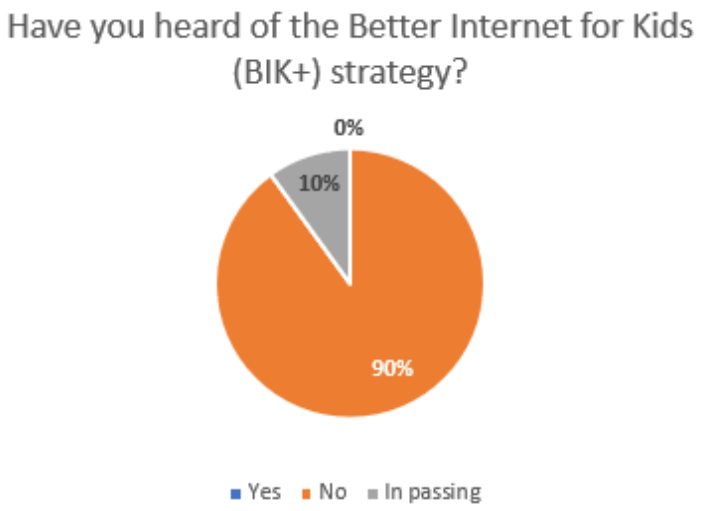

Figure 23. Answers of interviewees if they have heard of the BIK+ strategy.

Out of the 10 interviewees, only one teacher had heard about the European Union's Better Internet for Kids (BIK+) strategy. Even this, however, was only in passing when browsing other articles meant for teachers. However, despite this general unawareness, when they were given the BIK+ strategy's website, most of them agreed that it was a good idea. There was some discussion about the reasons why the BIK+ strategy is broadly unknown too, as well as discussion of significant problems with this type of 'digitalization venture'.

The EU means well with the strategy and can be seen as a step toward a safer internet, however some professionals thought that the EU strategy might chastise, restrict, and rein in some of the services that are needed within the European Union. As mentioned by Vihreä Varis in chapter 4.2.2, the European Union does not offer any type of European alternative for foreign services, meaning that they know how to slow things down, but they are unable to provide any type of growth needed.

Safety is always important for EU citizens, and the General Data Protection Regulation (GDPR) has been seen as a positive thing for people to have more control over their data. The BIK+ strategy on the other hand has not been as successful with this, and some of the professionals thought that in this aspect the EU has failed on marketing this new strategy for their member countries. And for these types of strategies, one professional thought that it would be best to have a director responsible for this, such as Traficom or the National Cyber Security Centre of Finland, that would implement the strategy.

Despite the BIK+ strategy being introduced in 2022, it must be noted that the earlier version of the strategy Better Internet for Children (BIK) was introduced back in 2012.

Despite this, the strategy itself was unheard of to the interviewees. One of the professionals did note that they might have taken some inspiration from the strategy, when creating teaching materials, though that was speculation on their part.

4.3.2 Understanding the versatile use of electronic devices by children and adolescents

Do children enjoy electronic devices, and to what extent? What are children doing on the internet? The reason for these questions in the interview was to uncover what teachers have observed, and whether cybersecurity professionals see them as still enjoying the use of electronic devices in schools, and what they use their electronic devices for.

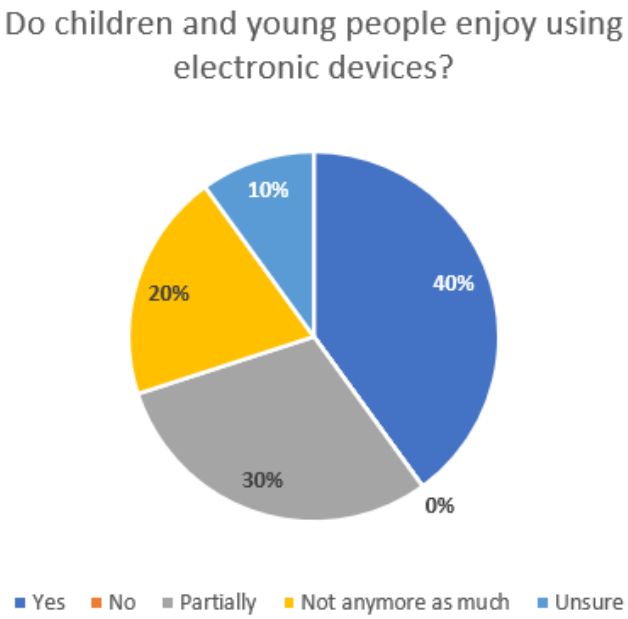

Figure 24. How interviewees think whether children and adolescents enjoy using electronic devices.

Most interviewees thought that they enjoy using electronic devices. However, some teachers reported that this enjoyment has been diminished. They justified this by explaining that they have observed in students that using electronic devices such as Chromebooks in studying was no longer a novelty, as they had been in use for quite a while now. They also mentioned that some students were more willing to use pen and paper, due to fatigue over using an electronic device the whole day. Of course, some students still find it easier to take notes and find information with the available devices, but some thought that using a physical book was easier for them than a PDF file.

There were some issues with using electronic devices too. Some of the interviewees thought that the devices were a great tool, but at the same time, there exists temptation to browse content outside of schoolwork. These issues in some schools have been tackled by blocking the installation of applications to the devices— however, they are still able to use the web browser or their own phones to bypass the issue. To tackle some of the issues, the Finnish government has been pushing to ban the usage of mobile phones in schools to reinforce the power of teachers and principals to intervene in activities that disrupt teaching and give the students restrictions to help the better concentrate on teaching.[62]

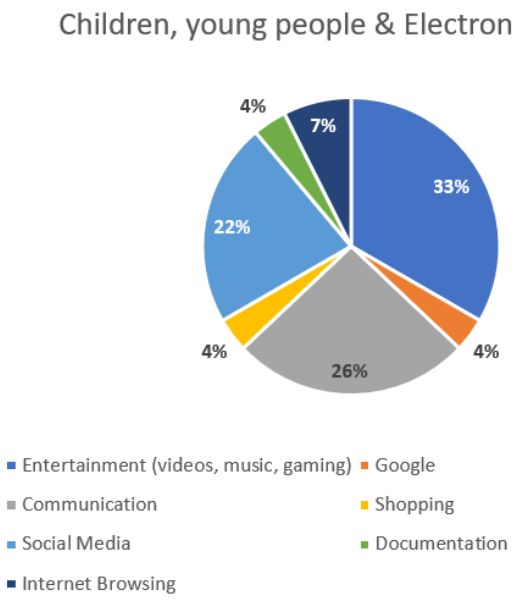

Figure 25. How interviewees think children and adolescents use electronic devices.

The teachers had some personal knowledge and experience of what the students were using phones for at school during class and during free time. Some of these topics and issues could easily be linked to the concerns regarding their internet usage, as mentioned in chapter 4.1.2. Speculations on what they use their electronic devices for was mostly conjecture on the part of the cybersecurity professionals, as they had not worked with children before, but they were in line with the answers from the teachers.

Most of the interviewees mentioned three key areas the most: entertainment, communication, and social media. Entertainment can vary from watching videos on platforms such as TikTok and YouTube, gaming on their electronic devices, listening to music on platforms such as Spotify. It is not difficult to imagine how these can serve as distracting temptations for students in schools if they have unlimited access to it. Regarding communication the interviewees mentioned that they keep in contact mostly with their friends

with platforms such as Snapchat and WhatsApp— and regarding the usage of social media, there are multiple platforms that are rising in popularity between them, such as TikTok, Instagram, and Snapchat that are more widely known, as well as new faces in the social media scene such as BeReal and Yubo.

As mentioned in the by the teacher Kesäheinä in Chapter 4.2.1, children and adolescents know the entertainment and communication side of technology well, but only a single interviewee mentioned writing documentations. They know how to entertain themselves and know how to find something interesting to watch and listen to, but they are lacking the skills to use technology for their benefit, which brings a big gap between entertainment versus utilization. Furthermore, the three key areas can bring in issues and concerns, as mentioned in chapter 2 and chapter 4.2.1, where some of these platforms are so new and upcoming, the researchers, teachers, and parents cannot keep up with them. No one can predict whether an application will become a success between children and adolescents, as there is a large amount of competition to gain their attention. The same can be said for video games: for example, the userbase of Pokémon Go within the United States plummeted within a year by around 80% in 2016. [63]

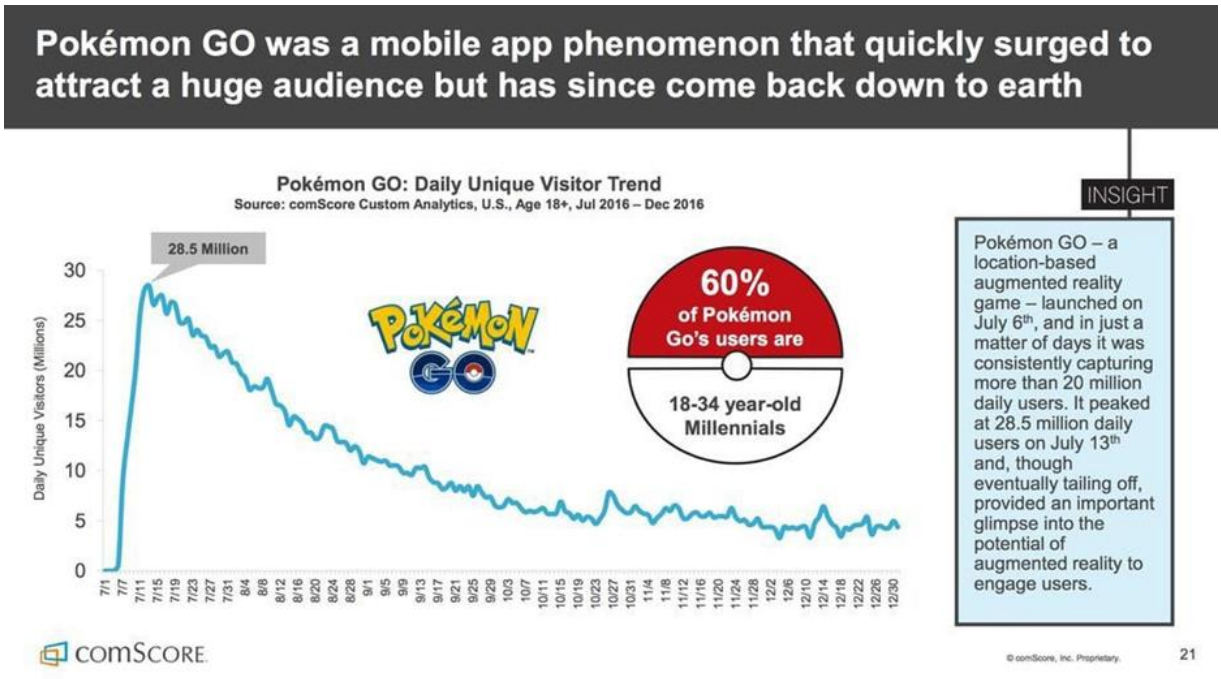

Figure 26. The userbase of Pokémon Go mobile game within the United States.[63]

4.3.3 Perspectives on the viability of ICT and cybersecurity as a school subject

As mentioned in the chapter 2.1.2, the BIK+ strategy aims to make the internet safer for children, but at the same time, push toward ICT and cybersecurity education within the EU countries to bring more awareness to major issues and concerns mentioned in chapter 2. However, it might be only a matter of time before ICT and cybersecurity education becomes a stable part of education, so asking interviewees whether they would mind ICT or cybersecurity as its own school subject, whether it would be too overwhelming for the students, and how would they implement the education into the curriculum would give some insight on how it could be done in the future curricula.

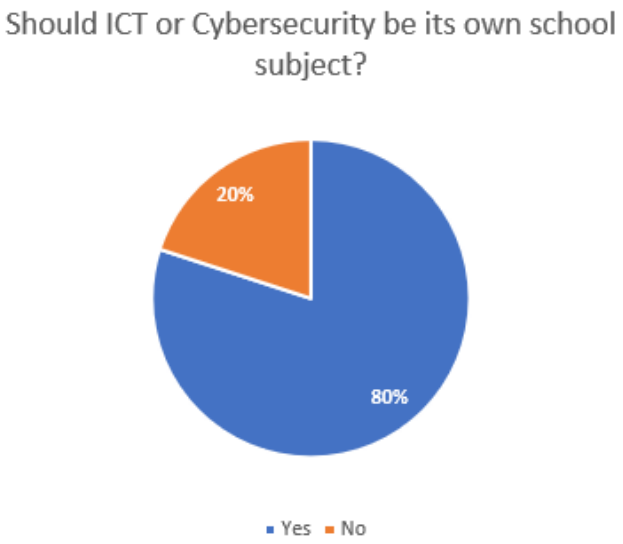

Figure 27. Interviewee's perspective whether ICT or cybersecurity should be its own school subject.

As seen based on the interviewees' answers, most thought that it would be a suitable subject in schools; however, one teacher and one cybersecurity professional mentioned that perhaps it does not necessarily need to be its own subject, rather it should be a premade package that the teachers could teach, as previously mentioned in chapter 4.2.1. Implementing a robust ICT and cybersecurity program into a school day which is already long and sharing space with other academic subjects could be a complex challenge. This though begs the question: how could a better ICT and cybersecurity education be implemented without overburdening the students it seeks to educate?

Asking teachers, the question of what subject they would switch for ICT or cybersecurity as a school subject gave a variety of answers. Some thought that it would not

matter if some of the optional studies were left out, as most students do not tend to choose automatic data processing (known as ATK in Finnish) as an optional study anymore, as they use electronic devices in schools constantly. However, some thought that subjects such as study guidance and health education could be split and spread out over the grades more and put the teaching of ICT and cybersecurity there due to overlapping in the subject. One teacher mentioned that teaching Christianity might not be so relevant, so that could be split into part, or changed to ethical thinking, and get some ICT or cybersecurity teaching time could be salvaged from that.

Some teachers had a vastly different idea. Instead of removing a subject completely, they instead suggest it should be melded to be a part of other studies: as an example, making documentations could be part of the language subjects, while the other parts of ICT and cybersecurity could be included in other classes, depending on what topic fits the best for that specific subject. This way some of the repetitive studies from, for example, health studies and study guidance could be lessened to instead involve topics such as mental health, the internet's role in mental health, internet etiquette, and how it could be used to teach students how essential government websites, such as social insurance institution of Finland (Kela) to apply for something that might be relevant for the students in the future.

Most of the interviewees agreed that the school subject that should be introduced is ICT, instead of cybersecurity, as they felt cybersecurity is an important part of the education but teaching it only would be less beneficial for the children in the long run. After all, as mentioned in chapter 4.2.1 and chapter 4.2.2, students and parents still lack basic skills needed to fully utilize ICT for their benefit.

However, the teachers did not think ICT would be too overwhelming as its own school subject if it is thought out well — that is, when subjects are taught at appropriate grades, and when education is structured in an interesting and motivating way for students. There were concerns about the educational material being too repetitive to be taught weekly, so there was a suggestion that subjects could be taught for half a semester. However, if education was melded into other school subjects, that would remove the issue, and perhaps make it more interesting and motivating for the students to have ICT implemented in a fun and interesting way among various subjects.

4.3.4 Exploring ways to make leaning of cybersecurity interesting for children and adolescents

Another big question, how to make education fun for students. Asking for the teachers' and cybersecurity professionals' opinions on the matter of what they would enjoy could be utilized in making the teaching material more interesting and entertaining. The question was to find out if there was a solution to making the education more interesting, but at the same time entertaining for them, and if it could be utilized with the existing and future materials to be easily integrated into the education, without burdening the teachers too much.

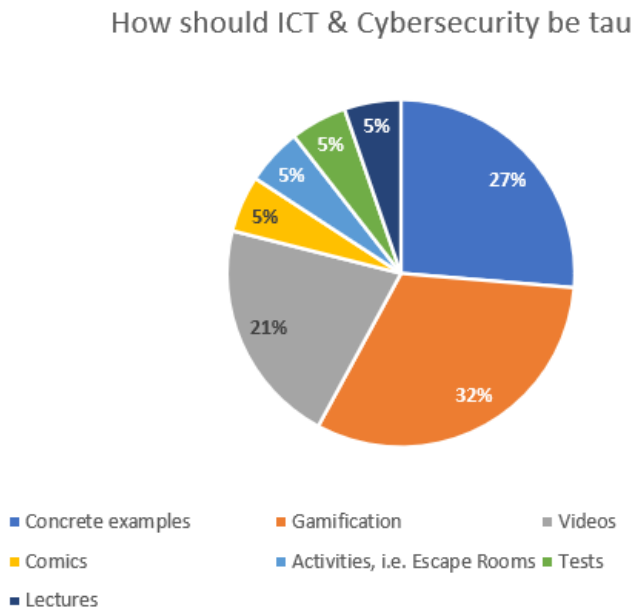

Figure 28. Interviewee's thoughts about how ICT and cybersecurity should be taught.

The interviewees thought that gamification was most relevant to making classes more fun and engaging. However, education should be done through concrete examples to give students a realistic feel of causal connections that could happen if they end up doing something. If they had a way to experiment on some things that could happen without endangering themselves, it could give them a better understanding of some concerns and issues that parents and teachers have regarding the usage of the internet.

There were plenty of mentions that the daily utilization part of ICT should be part of the education as well, be it by repetition and utilization of different types of tests and quizzes to test out the students' knowledge about certain topics. But also, the usage of different types of videos and media to teach these types of topics need to be interesting, yet short enough to digest the information from, instead of long and monotonous slideshows.

Topics that were emphasized by some of the interviewees were the importance of changing passwords, what happens to your personal data when it is used, what happens if one would google their own name, using various documentaries and games that give them concrete examples, as mentioned earlier; however, this should be done in a “mediasexy” (something that is talked in the media and general public at the moment) way to ensure that the existing material could be used in the future as well.

However, it was mentioned multiple times that the different means to make education more fun as its own is not enough. As an example of gamification, one professional mentioned that the player is just playing the game and might not even understand the topics and contexts that the game is trying to teach if the game is not integrated effectively into the educational syllabus: gamification without supporting material is not enough. The basics of ICT and cybersecurity education should come first, then stack more topics on top of that when they have understood the basics. Different ways that the topics mentioned by the interviewees and education could be combined will be discussed in chapter 5.

5 Discussion

In this chapter, the findings from the empirical data have been introduced, thus the aim of the chapter is to introduce plausible explanations and discussion about the current state of the cybersecurity education and the education system. This chapter has been divided into three subchapters based on the research questions introduced in chapter 1.2.

Chapter 5.1 presents the results from the empirical findings concerning what type of education is enough to provide children and adolescents essential cybersecurity education. Chapter 5.2, on the other hand, presents the results from the empirical data findings that could help with making cybersecurity education more engaging. Lastly, chapter 5.3 goes over the limitations of the thesis, and future research that can be done regarding the topic and issues presented in the thesis.

5.1 What is enough

The solution for cybersecurity and ICT education issues might seem simple by simply adding ICT or cybersecurity as a part of the education system and the curricula, but it is a multifaceted issue that will require much of discussion, inspection, planning, and further education for parents, teachers, and organizations. There should be and needs to be more cooperation done between teachers, the Ministry of Education and Culture, and cybersecurity professionals and specialists. As seen from the interviews, both teachers and cybersecurity professionals want the best for the future of the education, and their answers aligned with each other, therefore it should be noted that despite the cybersecurity professionals not having experience working with minors, they can still provide insight and expertise to rising technological changes and phenomena that might happen in the future to keep both the organizations and the education system up to date of which topics should be thought about in the creation of future and updated educational materials.

However, the current state of cybersecurity education in schools is currently not enough. Despite it being briefly mentioned in the school curricula, as seen in chapter 2.2. The lackluster state of cybersecurity education was reinforced by both the teachers and cybersecurity professionals that were interviewed. As mentioned by Vihreä Varis, as seen in chapter 4.1.3, the problem with the current curricula is:

> *"The current school curriculum was finished in 2016, and they started forming it since 2010-2011, the world was way different back then. Of course, it has some digitalization baked in, but it is badly behind. In the curriculum, they have mentioned all the things of digitalization, and they were already acknowledged then, but they are not actually in the curriculum."*

As seen from the interviewee's answer, the planning for the curricula started years prior to it being finished, meaning that the technology can take huge leaps during the time of the planning process of the curriculum. As seen with the smartphones, when they started becoming popular, as in 2014, there were 1,75 billion estimated smartphone users worldwide, transforming the ways of how people communicate with each other, and how businesses operate. [64]

There are, of course, yearly checkups regarding the subjects taught in schools. However, as ICT nor cybersecurity are a core part of the curricula yet, they are not being investigated regarding how schools should tackle some of the issues mentioned in chapter 4.1.2, as they can have long lasting effects on the development of students' mental health, self-image, and confidence. As seen in chapter 2, topics, and issues such as cyberbullying are a growing issue, due to the advancement of technology, and the anonymity that comes with it, yet the current curriculum does not tackle the issue of it.

However, some of these topics regarding cyberbullying and content related issues could be avoided by encouraging them to discuss their concerns and experiences, as well as teaching that they should not believe everything they see on the internet, as mentioned by Kesäheinä in chapter 4.2.1. Kesäheinä highlights the importance of discussion that is more about talking about their feelings and thoughts, rather than making them feel guilty for seeing something, even when sometimes, they have no say in what they see on the internet. That should be taken into consideration when creating the teaching material, that no matter how hard of a topic something can be, it can be discussed about different topics and issues.

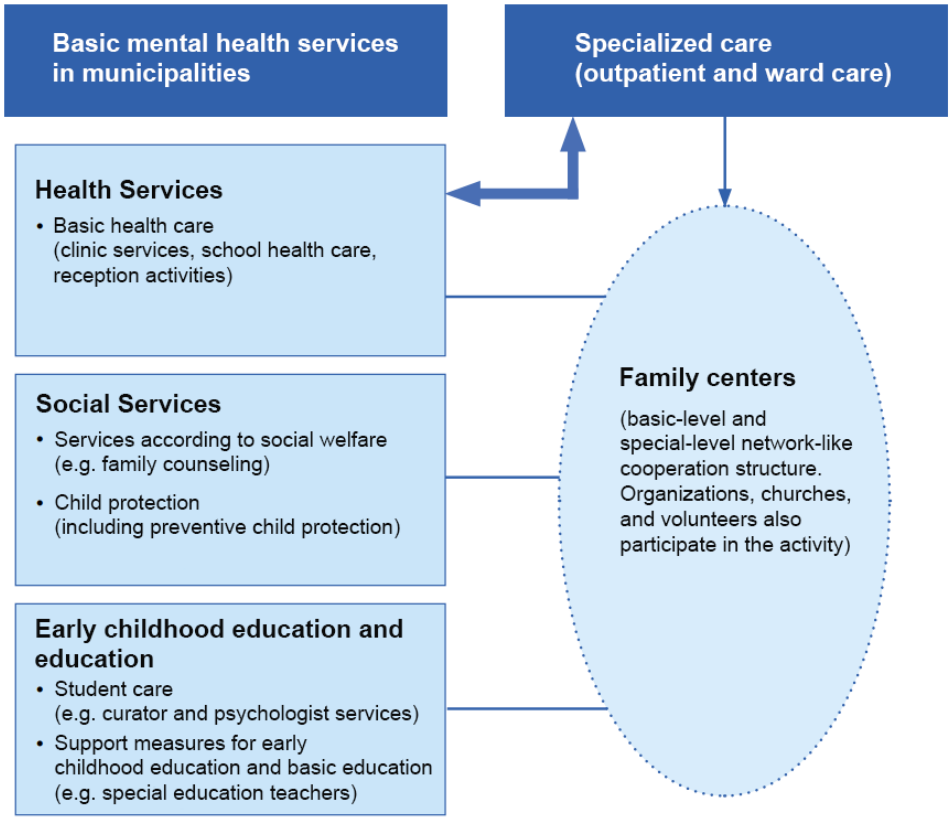

Figure 29. Different mental health services provided by the Finnish municipalities.[65]

However, some of these topics can feel hard for children and adolescents to talk about with adults. The issue stems from the lack of trust from them, which can lead them to hiding things and issues they might be having, due to feeling ashamed or scared how the adults would react. This was especially apparent during the COVID-19 pandemic, where children and adolescents felt more loneliness, anxiety, and depression, leading them to seek help by themselves from different crisis phones and crisis chat services to talk about their issues anonymously. The number of phone calls to these types of services rose by 40%, and the number of chats rose by 60% during 2020 [66]. It remains to be seen how the potential future ban of mobile phones at schools will affect students, as they are slowly getting back to the normal school environment after getting used to spending most of their days at home and on their electronic devices that were provided by the schools. Although they have only mentioned that this was to prevent them from getting distracted or disrupting the classes, it might give a reason for the students to socialize with each other, rather than spend their time on their phones and other devices.

And as seen in chapter 4.2.1, cyberbullying and mental development issues are one of the most mentioned issues that the interviewees have. Work is being done to tackle this issue,

as mentioned by the professional Vihreä Varis in chapter 4.2.2; big Finnish cities such as Pori, Turku, and Helsinki are trying to tackle this problem by providing and creating teaching materials for education purposes that will be introduced in the future. But as mentioned by them, it brings another major issue where big cities are working on materials, but some municipalities are putting no effort into the work, or are working on their own projects, which brings the question; how will they ensure that every single student gets the same level of education in smaller cities and municipalities to avoid creating inequality between municipalities and schools that might have less funding than others? That is another problem that needs to be solved.

5.2 How to make learning fun

As for the teaching materials and guidelines created for teachers on how the materials should be taught, they must be made in a way that are fun for both the teachers and the students. As Vihreä Varis mentioned in chapter 4.2.2 for the plan of instructions:

> *"The best way that we have found is that we create teaching materials for teachers, the type of teaching material that the teachers can teach through that, and we give them instructions how to teach them. This does not vary from teaching, for example, mathematics, the teacher gets a math textbook to teach from. Of course, the teacher knows how to teach it, but we give them a teaching plan."*

If instructions are just slides for teachers to read, it might be dull and demotivating for them to teach the material— and if the material is unengaging for the teachers, then it is likely their teaching of said material will be similarly unengaging for students. This is why material should be thought out in a way that would make the teachers feel interested in learning about the topics that they might not know so much about— this could be helpful with the teachers' updating training sessions as well. The educational materials that are made interesting for children can be made interesting for teachers and parents at the same time, utilizing the same methods mentioned in chapter 4.3.4.

Of course, there are many already existing teaching materials ranging from literature, videos, and games that could be used in educational purposes. However, it must be noted that due to them being in mostly in English, it can hinder some students', parents', and teachers' ability to learn, as some might not be so fluent with the language, especially when it comes to technical terms. However, this could be overcome by melding ICT and cybersecurity

education into different school subjects such as English classes, as it was noted in the chapter 4.3.3. This would be a potential way to learn some of the technical terms that they will hear on the internet, and most likely hear during their work life or later studies.

Gamification is an emerging trend that has been utilized in many places ranging from businesses, in-service management, health, and education [67]. The term gamification refers to the use of game mechanics in non-gaming contexts, or in other words, creating "gameful experiences" [68]. Gamification has been used for years, and is still used by many organizations and businesses to bring more engagement for their customers and employees by hiding game mechanics into their systems or applications that they present for their customers and employees. This can promote learning, employee performance, and customer engagement. The attraction for gamification lies within its potential to strengthen engagement, change people's behavior, and support innovative thinking. Gamification techniques can be also used in variety of educational contexts and subject areas and can be used to promote behaviors such as collaboration, self-guided studying, and creativity. [69]

Some researchers believe that video games can be utilized with education as well, even suggesting that certain video games could be given to play as homework, [70] despite it not yielding any significant results regarding cognitive skills. Indeed fast-paced computer game playing can only serve to foster highly specific skills that do not transfer. Despite this, it should be noted that "Kids learn from more positive, useful things for their future from their computer games than they learn in school." [71]

However, the transfer involves the ability to take what someone has learned in one context and then apply the learned knowledge to solve another problem or learning it in a new context. Transference is at the core of learning, and it has been a core part in both education and psychology. Educational experiences often present multimedia learning scenarios by presenting instructional materials that involve both words (written or spoken) and pictures (graphics, animations, or video). Figure 30 demonstrates a model of how learning works in different types of multimedia learning situations based on three basic principles of learning [72]:

- Dual channel principle
    - People have separate channels for processing visual and verbal material
- Limited capacity principle

- People can only process a small amount of material in each channel at one time

- Active processing principle
  - Deep learning occurs when people engage in active cognitive processing during learning

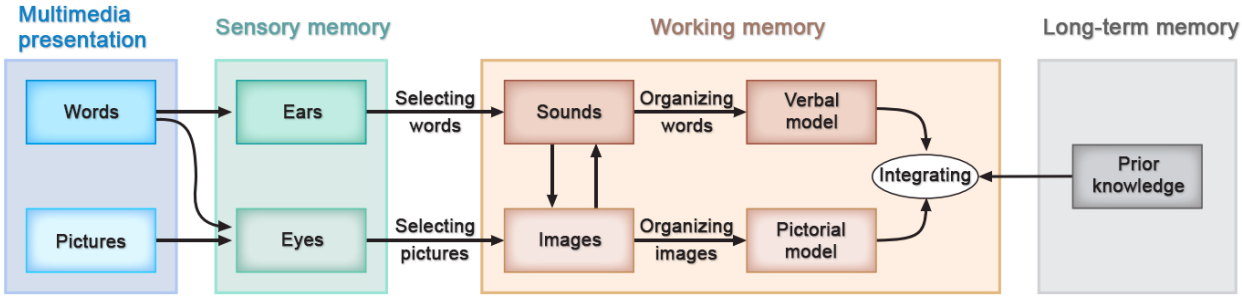

Figure 30. Cognitive model of multimedia learning. [72]

Despite the games themselves not providing any significant results in a short period of time, they have shown promising features that could be used to change the effect of the games and other types of media on learning as seen in table 2. Even if video games might not be the future of education, these results can still be utilized within the suggestions made by the interviewees in chapter 4.3.4.

Feature	Description	Experiments in which the effect is observed	Effect size
Modality	Use spoken text.	9 out of 9 experiments	1.4
Personalization	Use conversational language.	8 out of 8 experiments	1.5
Pretraining	Provide pregame information	7 out of 7 experiments	0.8
Coaching	Provide in-game advice and feedback	12 out of 15 experiments	0.7
Self-explanation	Prompt players to explain or reflect	13 out of 16 experiments	0.5

Table 4. Five promising features of computer games in education. [72]

One of the key areas mentioned by the interviewees was teaching through the usage of concrete examples that children could relate to be it through different types of media available for them. However, it needs to be thought out what would be the best way for them to learn about these things, as video games could be utilized, but it might not feel as personal or relatable in the eyes of the children. Hence the usage of concrete examples should be done through videos and other types of media.

Some interviewees wanted to raise awareness of some of the issues mentioned in chapter 4.1.2 without putting the children and adolescents at risk. This could be done with interactive media, which is a method of communication in which the output from the media comes from the input of the user.

Interactive films have been quite popular since the 1980s, such as Dragon's Lair, in which one or more viewers can interact with the film and influence the events that unfold in the film. This can be done through the gaming term quick-time events (QTE), in which the player performs an action on the controller device after an on-screen prompt. In the 2010, streaming services such as Netflix have been introducing interactive films, be it through animation or live-action movies.

One of the interactive experiences that Netflix released in late 2018 was a port of Minecraft: Story Mode made by the video game developer Telltale Games, changing the user interface (UI) and user experience (UX) to be more suitable to be played on a television remote or a mouse, instead of a video game controller.

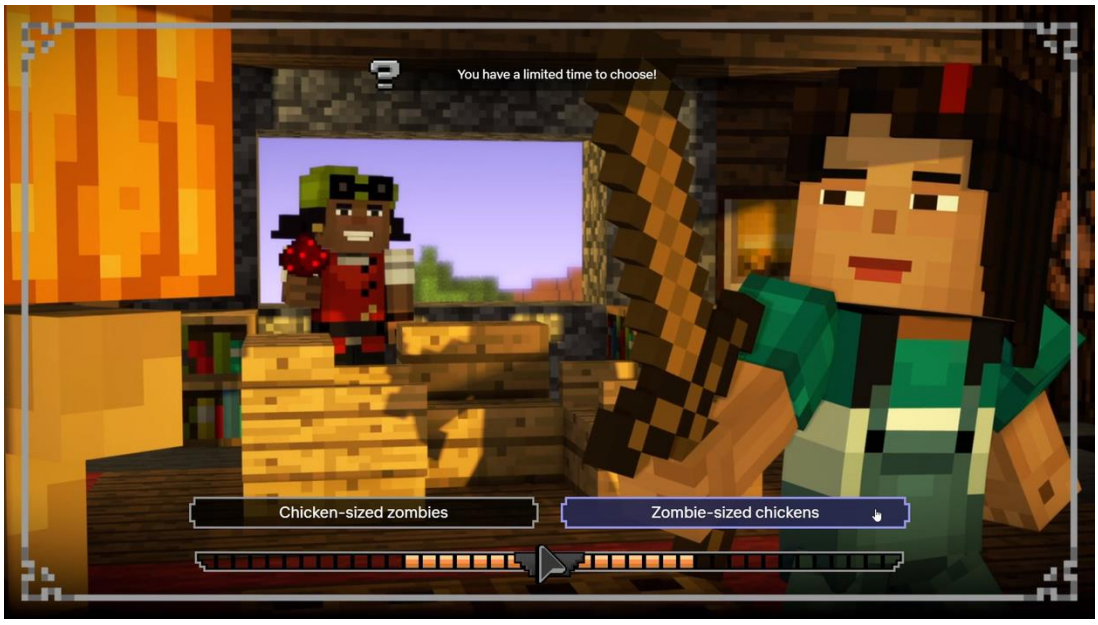

Figure 31. User interface of Minecraft: Story Mode in the Netflix release. [73]

Another interactive movie that Netflix released in 2018 was the Black Mirror: Bandersnatch, where the viewer makes the choices and decisions for the main character in a non-linear movie with five different endings. The movie presents the viewers with simple A or B choices that end up branching the story in different ways.

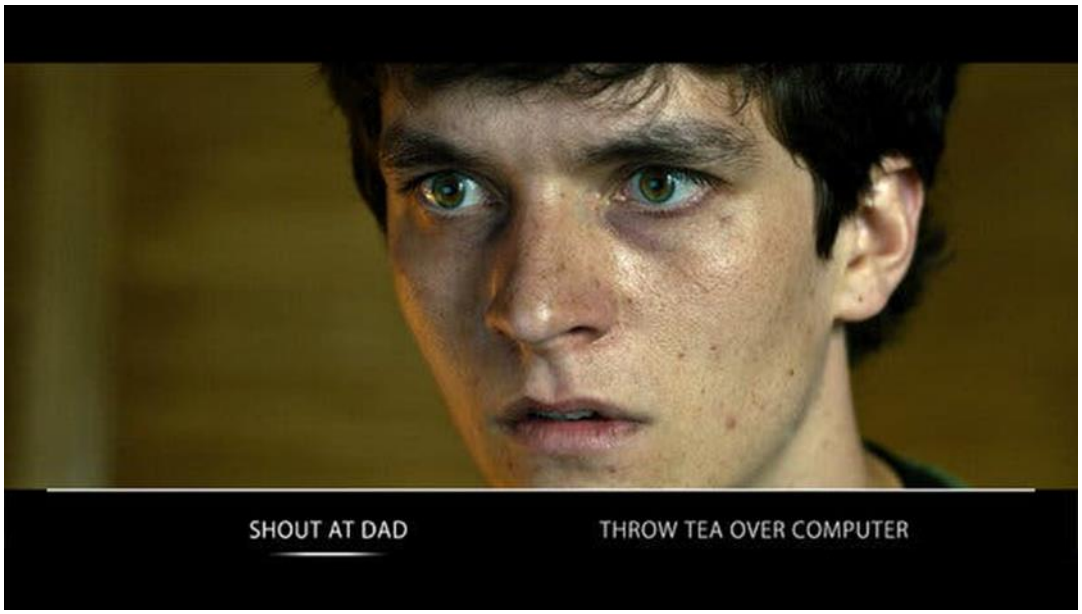

Figure 32. A or B choice the viewer must choose for the main character Stefan. [74]

However, since Black Mirror presents so many different choices for the viewer, it might not be the best way to present educational material. But regardless of that, the interactive media idea could be utilized by combining concrete examples and educational materials for the students.

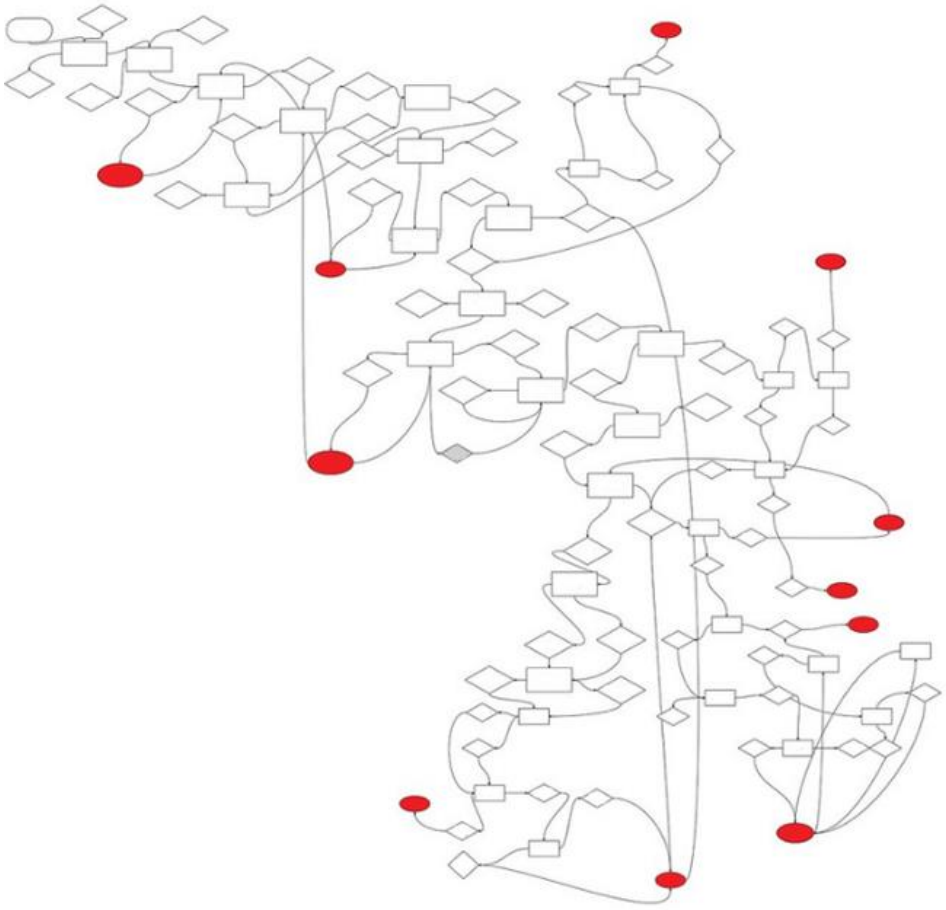

Figure 33. An example flowchart of choices in Black Mirror: Bandersnatch. [75]

The way both Minecraft: Story Mode and Black Mirror: Bandersnatch handle narrative branching and storytelling is very similar to visual novels, which is a form of digital interactive fiction. Some of these games involve some type of gameplay or puzzle elements that the player must complete to progress the story.

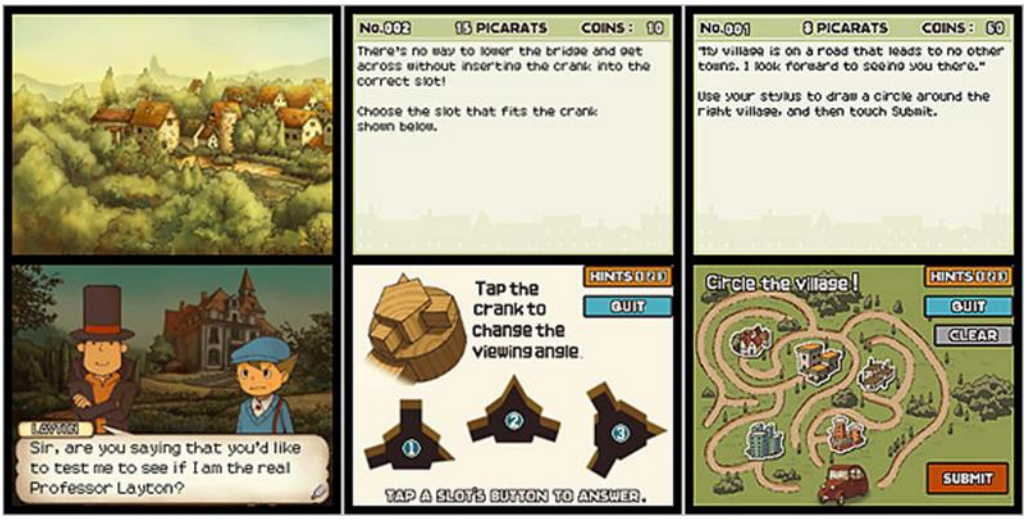

Figure 34. Scenes from Professor Layton and the Curious Village. [76]

These examples are quite fitting for what the interviewees were discussing, from being interactive, interesting, and giving the potential to express concrete examples of the potential dangers and issues regarding cybersecurity and ICT. The possibilities are limitless; however, it should be noted that to make the interactive media educational, the materials within them need to be easily digestible depending on the age group that the interactive media has been made for. And of course, they need to be created by people with the sufficient knowledge, ability, and budget.

The interactive media could resemble movies that combine some the smaller key areas mentioned in the chapter 4.3.4. The interactive media could, on the other hand, resemble visual novel-type games, featuring small tests and sequences to further the education and entertainment of the players. Despite games not influencing the skills of the player's cognitive abilities, however, well written stories can be memorable even after decades as we have seen with some movies, literature and video games that are still remembered for their stories. The United Kingdoms has put a lot of effort into their edutainment industry by providing students with free online study support resources with BBC Bitesize. They have done this by providing different alternative ways to study, through games and interactive media. [77]

If this was done on the education side of things, written stories with the combination of concrete examples and potential gamification aspects could be utilized to change the interactivity in learning cybersecurity and ICT in education, rather than solely relying on written materials that the students must read and study through. This with the combination of having students talk about the learning material and how it makes them think and feel could also be used as a bridge for teaching them that even harder topics can and should be discussed

about, as mentioned in chapter 4.2.1. Thought provoking material can be the difference between how seriously parents, teachers, children, and adolescents take cybersecurity and ICT education, as it was mentioned in chapter 4.1.2 that currently some parents lack the care or knowledge to prepare their children for the potential dangers of cybersecurity.

This is why some thought provoking and maybe even provocative material is needed to create more buzz and discussion regarding how people's personal data, private information, and security is handled on the internet, and how it can affect them for the rest of their lives, and why cybersecurity and ICT education is important for the current and future generation, despite them being considered 'diginative'. Even if the learning materials and learning methods might need to be thought provoking, they can at the same time be made fun and enjoyable.

5.3 Limitations and future work

As seen in chapter 3, all methodological choices used in this research thesis have been rationalized. Additionally, chapter 3.3 addressed the trustworthiness and authenticity of this research. Moreover, to conduct this research, multiple number of publications were read and, additionally, referred in this final thesis. However, there are natural limitations considering the research, and thus, these limitations are addressed in this subchapter. Furthermore, there are future research suggestions made from the perspective of the limitations of this thesis.

First, it is important to note that this thesis has not been written by an IT or information security expert, and thus, most of the practical solutions and education within businesses and organizations, and how they differ from school education have been left for the reader's responsibility and further reading. Therefore, the focus of this research is mainly on the aspect of cybersecurity within the Finnish education system with suggested additions regarding what, when and how it should be taught. In addition, the information obtained from the empirical findings and previous research reflect the time of writing this thesis and might change in the future.

Moreover, as mentioned in chapter 3, the study's results are based on the opinions of limited number of interviewees, thus they are not mean to reflect every single teacher and cybersecurity expert's opinion. Instead, the result aimed to gather different opinions why the Finnish education system needs to be changed in the future and give different suggestions how it could be done to be more enjoyable for everyone involved in it, be it students, teachers,

and parents. Hence, the purpose is not to argue that different cities' curricula are worse than others. Instead, it should be interpreted and applied in ways that would avoid inequality in different Finnish municipalities.

Another limitation this study contains is that the empirical data cannot be applied to directly to the Finnish education system and learning materials due to differences between laws and regulations of different countries involved in the research of the empirical data. Therefore, it would be interesting to examine if there are clear differences or patterns in the education of cybersecurity depending on the laws and regulations of different countries. Furthermore, it could be studied how different EU countries handle their ICT and cybersecurity education, and how the information could use to develop the ICT and cybersecurity education in Finland.

Finally, at the time of finishing this research, the Finnish government has not concluded whether they should ban the usage of smartphones at schools, and how it could affect the future of the ICT and cybersecurity education in Finland. The experts they have interviewed are claim that they can be used in a useful way in a supervised manner, but when other types of education are used, they should be put away. This can be beneficial, as mentioned by the experts, since students are recognizing that smartphones can be distracting during classroom, especially because children in Finland get smartphones much easier than any other country. [78]

However, schools and the government must ensure that parents are can and are able to contact their children during the school day one way or another, even if the ban of smartphones would limit the usage of social media and allow the children to focus on schoolwork. One expert mentioned that the mere presence of a smart phone on a child's desk can negatively impact concentration and weaken school performance, due to the presence of smartphones encouraging multitasking. [79] It will be interesting to see whether the ban of smartphones will affect school performance, and would it be more exciting and interesting for students to use different types of technologies to study as discussed in chapter 5.2.

6 Conclusion

In the beginning of this thesis, it was mentioned that the digitalization and modernization of the world has integrated IT devices as part of the minor's daily lives and education. Therefore, the research questions were formulated to study the currently existing literature and educational materials regarding ICT and cybersecurity, and to find out what teachers and cybersecurity professionals thought about what, when, and how cybersecurity should be taught to them and inspect the existing curricula to find out what types of teaching methods are currently used in four big cities in Finland. The research's focus was to inspect the existing studies and literature and compare them to the opinions and thoughts of the teachers and cybersecurity professionals. This was done to find out consistencies and differences between the two. In addition, the results covered various suggestions on how ICT and cybersecurity education could be made better in the future, and how this could be achieved.

In this chapter, the study's findings are raised on a higher level, and thus, the scientific and practical implications of conducting the research have been discussed. First, as being a master thesis, subchapter 6.1 will present the scientific or theoretical contribution of the research. The aim of the subchapter is to address how the study's results support the existing literature. Subchapter 6.2 presents practical contributions this study's results offer. The practical contributions are mainly directed towards the education of students' school curricula, however, some contributions toward the education of parents and teachers are also provided.

6.1 Theoretical contributions

Contrasting the findings of the study in chapter 4 against the existing literature and related studies presented in chapter 2, it could be concluded that the study's findings support the existing research and literature. The main key areas found in the study that were supported by the literature were; educational materials should be created and presented while keeping in mind the age categories that the materials are made for, the education of ICT and cybersecurity should be started when a minor is given an electronic device for the first time, and the educational material should be presented in a way that is the most appropriate for the certain age categories. Hence, the empirical findings underlined the importance of cybersecurity education, especially regarding the five risk categories that should be kept in mind when creating and presenting the educational material. This is to prepare them to the

current, shifting, and evolving dangers that the internet can bring. However, to do this, the level of education and the educational materials must be updated to be suitable for modern needs.

Due to the empirics of the study being formulated from the currently existing materials as of writing this thesis, it is rather difficult to know whether some of the suggestions made on this thesis have already been thought about in the future studies. However, one theoretical contribution would be that the education of ICT and cybersecurity is a multi-layered issue, which on its own cannot be solved by educating students. For education to be functional in the future, there must be steps taken to educate parents and teachers too regarding the complex issues that ICT and cybersecurity can bring. Another issue that needs to be addressed is the fact that they are considered 'diginative' due to them being raised in a modern cyber focused society. However, it needs to be noted that they know the entertainment side well, but they are not so well versed with the utilization of ICT for their own benefit. Of course, issues such as cyberbullying and its effect on the children and adolescents' mental health has been well written about in the existing literature, as mentioned in chapter 2.

It needs to be noted how little children and adolescents are encouraged to speak out about the issues they are facing, especially in Finland. The effects and prevention methods of issues that might harm mental development, such as cyberbullying, were almost non-existent in any of the existing curricula that were inspected for this study. This can lead to inequality in some of the municipalities and cities of Finland, if not addressed.

As for the BIK+ EU strategy, the European Union has failed to advertise and forward the information of their newly updated EU strategy to their member countries, and especially to the target audience: children. If neither cybersecurity professionals nor teachers have heard of the EU strategy, how likely is it that children have heard about it? The EU strategy would be beneficial for children in the EU member countries and outside of Europe, just like the GDPR, if EU had put more resources into forwarding the information. The strategy could be used as a framework for creating more safe spaces for children within the internet, while at the same time, bring more opportunities to European businesses to build different business opportunities to slowly shift away from having to rely on foreign countries to handle and process the data of European citizens.

6.2 Practical contributions

Contrasting the findings of the study in chapter 4 against the existing literature and related studies presented in chapter 2, it needs to be noted how aware the teachers and cybersecurity professionals are of the existing issues, and how they would wish them to be tackled.

However, as was mentioned in chapter 6.1, the study's findings suggest beginning with learning material. The learning material must be made for different age categories in mind, instead of putting minors into a single category. Despite it being hard to definite what is a child, as seen in chapter 2.1.1, dividing the created material into categories would eliminate some issues, where the materials can be adjusted for the needs of the age category, versus against a compilation of materials where teachers must pick and choose from. This also would eliminate the concerns that teachers had regarding educational material being too scattered. And if the teachers had guidelines on how to teach the material, it would be beneficial for them, and the students as well, eliminating the concerns regarding being unable to teach the material they are unsure of.

As for the teaching method, there are multiple types of teaching methods that could be used in ICT and cybersecurity education, however, some type of gamification and media through concrete examples that the age category can relate to would be the most beneficial for them. As the interviewees emphasized, the learning must be made in a way that is not condescending for them and should avoid feeling like they are feeling scolded. Rather, the education should include students also speaking about harder to talk topics to learn that everything can be talked and discussed about, no matter the topic.

As for different places to start the teaching from, the interviewees thought that starting from the basics of ICT and cybersecurity safety and usage would be the most beneficial. However, it must be noted that internet etiquette, and media literacy education were emphasized at a young age. This would help the child and adolescent to understand the difference between disinformation, misinformation, and correct information. As for internet etiquette, it would be another step to prevent cyberbullying, and learning about what ethically poor behavior on the internet can do to both the victim and the perpetrator.

The most important note from the study is that there must be steps taken to prevent students becoming inequal due to the cities and municipalities handling their ICT and cybersecurity education without guidelines or frameworks to work on. To prevent them from

being stuck in their own bubble, cooperation between municipalities and cities should be done. However, simply doing that might not prevent the inequality, as the teachers still lack ICT and cybersecurity as a part of their own studies in universities, which is later fixed with voluntary updating training. This is only a temporary fix that will work for a while, but it will not prevent the inequality the students might be caused to feel, due to the teachers lacking the knowledge and training on how to teach these types of subjects. Most of the conclusions the interviewees came to be the usage of different types of media, gamification techniques as a part of the education, and the usage of concrete examples that they can relate to and learn the most out of.

6.3 Revisiting objectives and outcomes

The digitalization and modernization of the world has integrated IT devices as part of minor's daily lives and education. The rising need for technological literacy after COVID-19 has brought up concerns regarding their knowledge about cybersecurity, especially considering the amount which they are now dependent on technology, and the cybersecurity threats in such an environment. The importance of cybersecurity and ICT education has grown significantly over the past couple decades, as technology takes huge development leaps within years, and these concerns can be seen in already existing cybersecurity literature and studies regarding them, as they have summarized the risks into five different categories: content risks, contact risks, children targeted as consumers, economic risks, and online privacy risks. However, these are only the main categories of concerns, which then are divided into subcategories (see figure 3-5).

As for the cybersecurity education level in Finland, the Finnish cities' curricula mention ICT as a part of it, elaborating what skills and knowledge the students will acquire during the years, however, cybersecurity was not mentioned in almost any of them. The objective was to find out whether cybersecurity should become a part of the Finnish curricula, when should the education of cybersecurity be started, what materials regarding cybersecurity should be taught, and how cybersecurity should be taught for children and adolescents.

The research was based on a qualitative research methodology method, which combines both qualitative and quantitative research methods to create a research outcome than either method would be able to individually. The literature review serves as quantitative research for understanding the current state of cybersecurity teaching in education, what types of information and material are available for teaching purposes, and how up to date the

materials are. As for the qualitative case study, it complements the literature review by collecting firsthand information through interviews from five cybersecurity professionals and five teachers.

The interview questions were divided into three different categories. The categories have three different chapters based on the research objectives of the thesis to help draw out the conclusions in a categorized manner, as the research objectives cannot be summarized within one single category. Furthermore, the categorization of the research objectives has been further divided into different subcategories to help with the analysis and conclusions regarding each category. In addition, the study's results offered several different suggestions on what type of education is enough for students of different age groups, and how can the education and learning be made fun.

The first research question has been divided into when children and adolescents should be taught cybersecurity. The question has been divided into three categories. Monitoring of them, which goes into more into the concerns regarding the monitoring and methods used to monitor, and how it should be done according to the interviewees. To this, the monitoring should be done per age category, to build a healthy relationship and trust between the parents, teachers, and children. However, the monitoring should be done mostly by the parent, as mentioned by the cybersecurity experts that it might otherwise break the privacy rights of minors if it were to be done by a teacher. Internet safety and concerns goes further into detail what areas are the most concerning regarding their internet usage, and why. There were many different types of issues mentioned by the interviewees, however, the most prominent key areas mentioned were content related risks, mental development issues, cyberbullying, and sexual solicitation. In addition to the two, the last subcategory goes into detail about how and when should they be aware of the concepts of cybersecurity and to what extent. The teaching should begin once the minor is given the electronic device that can connect to the internet— however, it should be ensured that the education regarding this should be done on the level that the minorwill understand.

The second research question has been divided into two subcategories. The first subchapter goes further into detail what type of materials and information teachers would like to see being taught in the future. However, the teachers emphasized the importance of internet etiquette and media literacy skills, as they mentioned how the students know and understand the entertainment side of technology but are lacking on the utilization side of technology. As

for the media literacy skills, they emphasized how important it would be for children and adolescents to understand the difference between disinformation, misinformation, and clean information, as the wrong type of information can spread like wildfire among the students. As for the second subchapter, it goes further into detail what type of information cybersecurity professionals think should be taught to them at schools. They emphasized the importance of making the education fun, rather than being monotonous and repetitive, also emphasizing the importance of cooperation between different types of organizations and professions, as the knowledge from both could be used to create a more competent and complete educational material package for schools to teach.

Finally, regarding the third research question, the category has been divided into four different subchapters. The first subchapter goes further into detail about the knowledge of the interviewees regarding BIK+. However, almost none of the interviewees have heard about the strategy, but thought it was a good idea, but the execution of distributing the information regarding it was done poorly. The second chapter went further into detail regarding whether children enjoy using electronic devices at school, how they use their electronic devices outside of schoolwork. According to the interviewees, some students enjoy them, but there has been a certain level of fatigue regarding the constant use of electronic devices at school. However, the children do enjoy using their devices for communication, various types of entertainment, and social media. The third subchapter goes into detail whether ICT or cybersecurity as its own subject would be viable. Regarding this, most interviewees thought that it should be ICT first, and cybersecurity as a part of the ICT education. As for how the education should be done, ICT education could replace some of the elective studies or be melded into other subjects as a part of them. As for the last subchapter, it went further into detail and thoughts of teachers and cybersecurity professionals on how to make the learning of ICT and cybersecurity more fun for students.

7 References

[1] N. Lau, R. Pastel, M. R. Chapman, J. Minarik, J. Petit, and D. Hale, “Human Factors in Cybersecurity – Perspectives from Industries,” Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 62, no. 1, pp. 139–143, Sep. 2018, doi: 10.1177/1541931218621032.

[2] V. N. Mathoosoothenen, J. S. Sundaram, R. A. Palanichamy, and S. N. Brohi, “An Integrated Real-Time Simulated Ethical Hacking Toolkit with Interactive Gamification Capabilities and Cyber Security Educational Platform,” in Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence, Jakarta Indonesia: ACM, Dec. 2017, pp. 199–202. doi: 10.1145/3168390.3168397.

[3] A. Nagarajan, J. M. Allbeck, A. Sood, and T. L. Janssen, “Exploring game design for cybersecurity training,” in 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), Bangkok: IEEE, May 2012, pp. 256–262. doi: 10.1109/CYBER.2012.6392562.

[4] F. Giannakas, A. Papasalouros, G. Kambourakis, and S. Gritzalis, “A comprehensive cybersecurity learning platform for elementary education,” Information Security Journal: A Global Perspective, vol. 28, no. 3, pp. 81–106, May 2019, doi: 10.1080/19393555.2019.1657527.

[5] Zhang-Kennedy, L., Yomna, A., & Sonia, C. (2017). Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. International Journal of Child-Computer Interaction, 13 (2017), (pp. 10-18).

[6] L. Zhang-Kennedy, Y. Abdelaziz, and S. Chiasson, “Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy,” International Journal of Child-Computer Interaction, vol. 13, pp. 10–18, Jul. 2017, doi: 10.1016/j.ijcci.2017.05.001.

[7] C. Grace, “Facebook Data Breach 2021 Exposes Personal Info of 1.5 Billion Users: 2 Tools to Check If Your Data Have Been Leaked,” iTech Post, Oct. 07, 2021. https://www.itechpost.com/articles/107257/20211007/facebook-data-breach-2021-exposes-personal-info-1-5-billion.htm.

[8] C. Price, “Roblox security issues expose 100 million users, claims Cybernews,” Tech Digest, Apr. 28, 2021. https://www.techdigest.tv/2021/04/roblox-security-issues-expose-100-million-users-claims-cybernews.html.

[9] “Scams and What to Look out for.” https://discord.com/safety/common-scams-what-to-look-out-for.

[10] “Older people targeted by ransomware while young adults fall for TikTok scams,” SecurityBrief New Zealand, 2022. https://securitybrief.co.nz/story/older-people-targeted-by-ransomware-while-young-adults-fall-for-tiktok-scams

[11] The Global Cybersecurity Forum, “GCF-2022-Book-English.pdf,” 2022. https://globalcybersecurityforum.com/GCF-2022-Book-English.pdf (accessed Aug. 23, 2023).

[12] F. Quayyum, D. S. Cruzes, and L. Jaccheri, “Cybersecurity awareness for children: A systematic literature review,” International Journal of Child-Computer Interaction, vol. 30, p. 100343, Dec. 2021, doi: 10.1016/j.ijcci.2021.100343.

[13] J. C. Read and P. Markopoulos, “Child–computer interaction,” International Journal of Child-Computer Interaction, vol. 1, no. 1, pp. 2–6, Jan. 2013, doi: 10.1016/j.ijcci.2012.09.001.

[14] A. Tsirtsis, N. Tsapatsoulis, M. Stamatelatos, K. Papadamou, and M. Sirivianos, “Cyber security risks for minors: A taxonomy and a software architecture,” in 2016 11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP), Thessaloniki, Greece: IEEE, Oct. 2016, pp. 93–99. doi: 10.1109/SMAP.2016.7753391.

[15] E. W. Owens, R. J. Behun, J. C. Manning, and R. C. Reid, “The Impact of Internet Pornography on Adolescents: A Review of the Research,” Sexual Addiction & Compulsivity, vol. 19, no. 1–2, pp. 99–122, Jan. 2012, doi: 10.1080/10720162.2012.660431.

[16] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, “A Review of Using Gaming Technology for Cyber-Security Awareness,” IJISR, vol. 6, no. 2, Jun. 2016, doi: 10.20533/ijisr.2042.4639.2016.0076.

[17] I. Cullinane, C. Huang, T. Sharkey, and S. Moussavi, “Cyber security education through gaming cybersecurity games can be interactive, fun, educational and engaging,” J. Comput. Sci. Coll., vol. 30, no. 6, pp. 75–81, Jun. 2015.

[18] E. Staksrud, K. Ólafsson, and S. Livingstone, “Does the use of social networking sites increase children’s risk of harm?,” Computers in Human Behavior, vol. 29, no. 1, pp. 40–50, Jan. 2013, doi: 10.1016/j.chb.2012.05.026.

[19] A. T. Pinter, P. J. Wisniewski, H. Xu, M. B. Rosson, and J. M. Caroll, “Adolescent Online Safety: Moving Beyond Formative Evaluations to Designing Solutions for the Future,” in Proceedings of the 2017 Conference on Interaction Design and Children, Stanford California USA: ACM, Jun. 2017, pp. 352–357. doi: 10.1145/3078072.3079722.

[20] D. F. G. Aponte and D. Richards, “Managing cyber-bullying in online educational virtual worlds,” in Proceedings of The 9th Australasian Conference on Interactive Entertainment: Matters of Life and Death, Melbourne Australia: ACM, Sep. 2013, pp. 1–9. doi: 10.1145/2513002.2513006.

[21] L. K. Watts, J. Wagner, B. Velasquez, and P. I. Behrens, “Cyberbullying in higher education: A literature review,” Computers in Human Behavior, vol. 69, pp. 268–274, Apr. 2017, doi: 10.1016/j.chb.2016.12.038.

[22] C. E. Notar, S. Padgett, and J. Roden, “Cyberbullying: A Review of the Literature,” Universal Journal of Educational Research, vol. 1, no. 1, pp. 1–9, 2013.

[23] K. P. Reed, R. L. Cooper, W. R. Nugent, and K. Russell, “Cyberbullying: A literature review of its relationship to adolescent depression and current intervention strategies,” Journal of Human Behavior in the Social Environment, vol. 26, no. 1, pp. 37–45, Jan. 2016, doi: 10.1080/10911359.2015.1059165.

[24] L. Buchanan, L. Scarlatos, and N. Telendii, “Curriculum to Broaden Participation in Cybersecurity for Middle School Teachers and Students,” in 2021 IEEE Integrated STEM Education Conference (ISEC), Princeton, NJ, USA: IEEE, Mar. 2021, pp. 63–70. doi: 10.1109/ISEC52395.2021.9763930.

[25] “Tietoturva ja -suoja koulussa,” Opetushallitus. https://www.oph.fi/fi/koulutus-ja-tutkinnot/tietoturva-ja-suoja-koulussa.

[26] “Convention on the Rights of the Child,” OHCHR. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child (accessed Aug. 02, 2023).

[27] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+). 2022. Accessed: Aug. 02, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN

[28] World Health Organization, "Adolescent health." Accessed: Sep. 28, 2023. [Online]. Available: https://www.who.int/health-topics/adolescent-health

[29] "Frequently asked questions on the Convention on the Rights of the Child | UNICEF." https://www.unicef.org/child-rights-convention/frequently-asked-questions (accessed Aug. 02, 2023).

[30] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS European Strategy for a Better Internet for Children. 2012. Accessed: Aug. 02, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0196

[31] "BIK Strategy - BIK Portal - BIK Community," BIK Portal. https://www.betterinternetforkids.eu/policy/newbikstrategy (accessed Aug. 02, 2023).

[32] T. Vänni, "Perusopetuksen opetussuunnitelman perusteet 2014 luvut 1-12". https://blog.edu.turku.fi/ops2016/files/2021/02/Turun-ops-luvut-1-12_200806.pdf (accessed Aug 11.2023).

[33] E. Valtonen, "Perusopetuksen opetussuunnitelman perusteet 2014 luku 13". https://blog.edu.turku.fi/ops2016/files/2015/04/luku-13-1-2lk.pdf (accessed Aug. 11, 2023).

[34] E. Valtonen, "Perusopetuksen opetussuunnitelman perusteet 2014 luku 14". https://blog.edu.turku.fi/ops2016/files/2021/09/Turun-ops-luku-14-3-6lk_210914.pdf (accessed Aug. 11, 2023).

[35] "Tieto- ja viestintäteknologian opetuskäytön suunnitelma 2019 – 2022." https://edu.turku.fi/wp-content/uploads/2019/10/tvt-suunnitelma-2019-2022.pdf.

[36] “Perusopetuksen opetussuunnitelma.” https://peda.net/pori/perusopetus/opetus/ok22 (accessed Jun. 11, 2023).

[37] “Perusopetuksen opetussuunnitelma.” https://ops.tampere.fi/perusopetus/1/?school= (accessed Jun. 12, 2023).

[38] “Seudullinen TVT-suunnitelma 2019-2021.” https://www.pirkkala.fi/library/files/5fbf711c475a6c7d163257ee/Tampereen_seudun_tvtsuunnitelma_2019-2021.pdf (accessed Jun. 12, 2023).

[39] “Helsingin Opetussuunnitelma.” https://ops.edu.hel.fi/ops/ (accessed Jun. 13, 2023)..

[40] “Perusopetuksen Opetussuunnitelman perusteet 2014.” https://ops.edu.hel.fi/wp-content/uploads/2016/01/163777_perusopetuksen_opetussuunnitelman_perusteet_2014.pdf (accessed Jun. 13, 2023).

[41] M. Christen, B. Gordijn, and M. Loi, Eds., The Ethics of Cybersecurity, vol. 21. in The International Library of Ethics, Law and Technology, vol. 21. Cham: Springer International Publishing, 2020. doi: 10.1007/978-3-030-29053-5.

[42] “The CIA triad of confidentiality, integrity and availability,” i-SCOOP. https://www.i-scoop.eu/cybersecurity/cia-confidentiality-integrity-availability-security/.

[43] Plato, “The Ring of Gyges,” 358d-361d. https://www.plato-philosophy.org/wp-content/uploads/2016/05/gyges-a.pdf.

[44] “Google’s $400m penalty and impact of the 5 heftiest data privacy fines on 2023 ad plans,” The Drum. https://www.thedrum.com/news/2022/11/15/googles-400m-penalty-the-impact-the-5-heftiest-data-privacy-fines-2023-ad-plans.

[45] P. Formosa, M. Wilson, and D. Richards, “A principlist framework for cybersecurity ethics,” Computers & Security, vol. 109, p. 102382, Oct. 2021, doi: 10.1016/j.cose.2021.102382.

[46] D. J. Solove, Understanding privacy, First Harvard University Press paperback edition. Cambridge, Massachusetts London, England: Harvard University Press, 2009.

[47] M. A. Malina, H. S. O. Nørreklit, and F. H. Selto, “Lessons learned: advantages and disadvantages of mixed method research,” Qualitative Research in Accounting & Management, vol. 8, no. 1, pp. 59–71, Apr. 2011, doi: 10.1108/11766091111124702.

[48] J. Moriarty, Qualitative Methods Overview. in SSCR Methods Reviews. London: National Institute for Health Research School for Social Care, 2011.

[49] R. Anderson, “Thematic Content Analysis (TCA) Descriptive Presentation of Qualitative Data,” 2014, [Online]. Available: https://rosemarieanderson.com/wp-content/uploads/2014/08/ThematicContentAnalysis.pdf

[50] M. Vaismoradi, J. Jones, H. Turunen, and S. Snelgrove, “Theme development in qualitative content analysis and thematic analysis,” JNEP, vol. 6, no. 5, p. p100, Jan. 2016, doi: 10.5430/jnep.v6n5p100.

[51] “Can personal data about children be collected?” https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_en.

[52] Data Protection Ombudsman’s Office, “Consent of the data subject | Data Protection Ombudsman’s Office,” Tietosuojavaltuutetun toimisto. https://tietosuoja.fi/en/consent-of-the-data-subject.

[53] C. McCarthy, “Why teenagers eat Tide pods,” Harvard Health, Jan. 30, 2018. https://www.health.harvard.edu/blog/why-teenagers-eat-tide-pods-2018013013241.

[54] K. Miller, “Here’s What the Blackout Challenge Is, and Why It’s So Dangerous,” Health, 2023. https://www.health.com/mind-body/blackout-challenge (accessed Aug. 02, 2023).

[55] RAINN, “Grooming: Know the Warning Signs | RAINN.” https://www.rainn.org/news/grooming-know-warning-signs (accessed Aug. 02, 2023).

[56] L. Zhang-Kennedy, S. Chiasson, and P. Van Oorschot, “Revisiting password rules: facilitating human management of passwords,” in 2016 APWG Symposium on Electronic Crime Research (eCrime), Toronto, ON, Canada: IEEE, Jun. 2016, pp. 1–10. doi: 10.1109/ECRIME.2016.7487945.

[57] Ministry of Education and Culture, Finland, “New Literacies Programme - OKM - Ministry of Education and Culture, Finland,” Opetus- ja kulttuuriministeriö. https://okm.fi/en/new-literacies-programme.

[58] Opetushallitus, “Digitaalisen osaamisen kuvaukset,” ePerusteet. https://eperusteet.opintopolku.fi/#/fi/digiosaaminen/8706410/tekstikappale/8709071.

[59] L. Kolirin, “Artist rejects photo prize after AI-generated image wins award,” CNN, Apr. 18, 2023. https://www.cnn.com/style/article/ai-photo-win-sony-scli-intl/index.html.

[60] S. Barnett, “ChatGPT Is Making Universities Rethink Plagiarism,” Wired. Accessed: Jul. 17, 2023. [Online]. Available: https://www.wired.com/story/chatgpt-college-university-plagiarism/

[61] “Front page | KyberVPK.” https://kybervpk.fi/en/.

[62] P. Vanttinen, “Finland to ban mobile phones in schools,” www.euractiv.com, Jun. 27, 2023. https://www.euractiv.com/section/politics/news/finland-to-ban-mobile-phones-in-schools/.

[63] Comscore, “2017 U.S. Cross-Platform Future in Focus,” Comscore, Inc. https://www.comscore.com/Insights/Presentations-and-Whitepapers/2017/2017-US-Cross-Platform-Future-in-Focus.

[64] H. W. Lucius and J. H. Hanson, “Consumerism and Marketing in the Digital Age,” American Journal of Management, vol. 16, no. 3, Art. no. 3, Sep. 2016, Accessed: Aug. 02, 2023. [Online]. Available: https://www.articlegateway.com/index.php/AJM/article/view/1871

[65] T. Aalto-Setälä, E. Huikko, K. Appelqvist-Schmidlechner, H. Haravuori, and M. Marttunen, “Kouluikäisten mielenterveysongelmien tuki ja hoito perustason palveluissa : Opas tutkimiseen, hoitoon ja vaikuttavien menetelmien käyttöön,” 2020. https://www.julkari.fi/handle/10024/140590.

[66] S. terveysministeriön asettama työryhmä, “Lapset, nuoret ja koronakriisi : Lapsistrategian koronatyöryhmän arvio ja esitykset lapsen oikeuksien toteuttamiseksi,” Jan. 18, 2021. https://julkaisut.valtioneuvosto.fi/handle/10024/162647.

[67] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, “From game design elements to gamefulness: defining ‘gamification,’” in Proceedings of the 15th International Academic

MindTrek Conference: Envisioning Future Media Environments, Tampere Finland: ACM, Sep. 2011, pp. 9–15. doi: 10.1145/2181037.2181040.

[68] J. Koivisto and J. Hamari, “Demographic differences in perceived benefits from gamification,” Computers in Human Behavior, vol. 35, pp. 179–188, Jun. 2014, doi: 10.1016/j.chb.2014.03.007.

[69] I. Caponetto, J. Earp, and M. Ott, “Gamification and Education: a Literature Review,” Proceedings of the 8th European Conference on Games-Based Learning - ECGBL 2014, vol. 1, pp. 50–57, Oct. 2014.

[70] C. Pilegard and R. E. Mayer, “Game over for Tetris as a platform for cognitive skill training,” Contemporary Educational Psychology, vol. 54, pp. 29–41, Jul. 2018, doi: 10.1016/j.cedpsych.2018.04.003.

[71] M. Prensky, “Don’t bother me Mom, I’m learning!”: how computer and video games are preparing your kids for twenty-first century success and how you can help!, 1st ed. St. Paul, Minn: Paragon House, 2006.

[72] R. E. Mayer, “Computer Games in Education,” Annu. Rev. Psychol., vol. 70, no. 1, pp. 531–549, Jan. 2019, doi: 10.1146/annurev-psych-010418-102744.

[73] Joyrok, “Minecraft Story Mode: Netflix — Joyrok.” https://joyrok.com/Minecraft-Story-Mode-Netflix.

[74] D. Streitfeld, “‘Black Mirror’ Gives Power to the People,” The New York Times, Dec. 28, 2018. Accessed: Jul. 26, 2023. [Online]. Available: https://www.nytimes.com/2018/12/28/arts/television/black-mirror-netflix-interactive.html

[75] J.-A. Rowney, “Black Mirror Bandersnatch flowchart gives you a map for all the endings,” mirror, Dec. 31, 2018. https://www.mirror.co.uk/film/black-mirror-bandersnatch-flowchart-gives-13795928.

[76] S. Schiesel, “Taking a Virtual Leap Into a Mind-Bending, Interactive, Anime World,” The New York Times, Apr. 09, 2008. Accessed: Aug. 02, 2023. [Online]. Available: https://www.nytimes.com/2008/04/09/arts/television/09puzz.html

[77] “Find out more about BBC Bitesize.,” BBC Bitesize. https://www.bbc.co.uk/bitesize/articles/z6x992p (accessed Aug. 21, 2023).

[78] Yle News, “Citizens’ initiative seeks to ban smartphones in classrooms,” News, Apr. 18, 2023. https://yle.fi/a/74-20027680.

[79] B. Thornton, A. Faires, M. Robbins, and E. Rollins, “The Mere Presence of a Cell Phone May be Distracting: Implications for Attention and Task Performance,” Social Psychology, vol. 45, no. 6, pp. 479–488, Nov. 2014, doi: 10.1027/1864-9335/a000216.