Master Degree Project

UNIVERSITY OF SKÖVDE

Cybersecurity Education in Swedish Lower Secondary Schools: An Interview Study with Teachers

Experiences, Practices and Conditions

Master's Degree Project in Informatics with a specialization in Privacy, Information and Cyber Security

Second Cycle 30 ECTS

Spring term 2026

Student: Linus Brifelt

Supervisor: Oskar MacGregor

Examiner: Ali Padyab

Acknowledgements

I would like to express my sincere gratitude to all the teachers who took the time to participate in the interviews and openly share their experiences, perspectives, and thoughts. Their willingness to participate made this study possible, and I am very grateful for the time and effort they contributed despite their already busy schedules.

I would also like to thank my colleagues for their support, encouragement, and understanding throughout the writing process. Their interest in my work and continued encouragement have been greatly appreciated throughout this journey.

I am also grateful to Graff and Birkenstein (2018) and Higson-Smith (2000), whose work provided useful guidance on academic writing and on how to structure and present the analysis in a clear and coherent manner. Their work has contributed to the overall structure and presentation of this thesis.

Finally, a special and heartfelt thank you goes to my supervisor, Oskar MacGregor, who has been an invaluable source of support throughout the entire process. His guidance, thoughtful feedback, encouragement, and willingness to discuss ideas and challenges along the way have been greatly appreciated. His support has helped me navigate both the larger questions and the smaller details that arose during the work, and I am deeply grateful for the time and commitment he has dedicated to helping me bring this thesis to completion.

ABSTRACT

Cybersecurity has become an increasingly important societal issue as children and young people spend a growing part of their everyday lives in digital environments. While previous research has largely focused on students' cybersecurity knowledge and awareness, fewer studies have examined how teachers themselves perceive and implement cybersecurity-related education. The aim of this study was therefore to explore how cybersecurity-related teaching is currently practiced in Swedish municipal lower secondary schools and how teachers describe their instructional practices, resources, competence, and conditions for teaching the subject.

The study employed a qualitative research approach, beginning with a small-scale systematic literature review of previous international research on cybersecurity education. The findings from the review informed a subsequent empirical phase involving semi-structured interviews with eight teachers from seven municipal lower secondary schools in the Skaraborg region of Sweden. The interview data were analyzed using thematic analysis.

The findings suggest that cybersecurity-related topics are present in all participating schools but are rarely taught as a clearly defined or systematic subject area. Instead, cybersecurity-related issues are often integrated into broader teaching on source criticism, social media, privacy, artificial intelligence, online fraud, and digital responsibility. Teachers generally described high levels of engagement with the topic but also identified challenges related to limited time, unclear curricular guidance, uneven access to teaching materials, and varying levels of confidence regarding various aspects of the subject, many of which also reflected findings from the international research included in the systematic literature review.

Overall, the study indicates that cybersecurity education in Swedish lower secondary schools is addressed more indirectly than directly. While cybersecurity-related topics are addressed in practice, their implementation often depends on local priorities, individual teacher initiatives, and informal organizational structures rather than systematic educational planning.

Keywords: cybersecurity education, digital competence, lower secondary school, teachers, cybersecurity awareness, semi-structured interviews

Table of Contents

1. Introduction 1
1.1 Problem definition 2
1.2 Research Aims and Motivation 3
1.3 Research Questions 4
1.4 Delimitations and Scope 4
1.5 Thesis Structure 5
2. Background 6
2.1 Preliminaries and Central Concepts 6
2.1.1 What is Cybersecurity? 6
2.1.2 Common Cybersecurity-Related Topics 7
2.2 Swedish Cybersecurity Awareness Initiatives 9
2.2.1 The Swedish Civil Defence and Resilience Agency (MCF) 9
2.2.2 The Swedish Federation of Young Scientists 9
2.2.3 The Swedish Internet Foundation 10
2.2.4 The Security Check 11
3. Previous Research: Systematic Literature Review 13
3.1 Literature Search Strategy 13
3.1.1 Database Selection 13
3.1.2 Boolean Operators and Search Terms 14
3.1.3 Search Criteria 14
3.2 Literature Search, Screening Process and Supplementary Articles 15
3.3 Thematic Coding Process and Identified Themes 17
3.4 Thematic Analysis 19
3.4.1 Limitations in the Delivery of Education 19
3.4.2 Access to (and quality of) Teaching Resources 20
3.4.3 Teachers' Knowledge, Confidence and Professional Development 21
3.4.4 Governance, Curriculum and Organizational Frameworks 22
3.4.5 Pedagogical Approaches and the Teacher's Role 23
3.4.6 Thematic Analysis Summary 24
3.5 Thematic Foundation for Interview Study 25
4. Research Methodology 26
4.1 Qualitative Research Approach 26
4.2 Semi-structured Interviews 26

4.3 Selection / Sampling Group 28
4.4 Data Analysis: Thematic Coding 29
4.5 Validity, Reliability and Bias (Trustworthiness) 29
4.6 Data Collection 31
4.7 Interview Coding Process 32
5. Results 33
5.1 Delivery of Education 34
5.2 Teaching Resources and Teaching Methods 37
5.3 Teachers' Knowledge, Confidence and Professional Development 39
5.4 Governance, Curriculum and Organizational Frameworks 43
5.5 Teachers' Overarching Role and Ideal Pedagogical Approaches 46
5.6 Thematic Analysis Summary 49
6. Discussion 50
6.1 Reflections on the Results and Methodological Considerations 50
6.2 Findings in Relation to Previous Research 52
6.3 Ethical and Societal Aspects 54
6.4 Reflections on the Research Process 55
6.5 Future Work 56
7. Conclusion 57
References 58
Appendices 63
Appendix A – Semi-Structured Interview Guide and Research Questions (translated from Swedish to English) 63
Appendix B – Information for Research Participants (translated from Swedish to English) 67

1. Introduction

In today's increasingly interconnected and digitized society, the need to protect sensitive and personal information is of crucial importance. Rapid technological development has, in many ways, improved our everyday lives, but it has also introduced new risks and vulnerabilities. This is particularly true for children and adolescents, who today grow up in a digital environment that is a natural and integrated part of their daily lives. In 2024, virtually all children aged 8–19 in Sweden use the internet, and 96% do so daily (Internetstiftelsen, 2024). This extensive digital presence means that children encounter both opportunities and risks at a very early age. They use the internet for schoolwork, communication, entertainment, and social interaction, often without fully understanding the potential threats in digital environments.

At the same time, both national and international reports indicate that cyber-related crime targeting minors has increased significantly. According to a report from the Global Cybersecurity Forum (GCF), as many as 72% of the world's children have at some point been affected by cyber-related abuse or crime (Panhans et al., 2022).

In the United Kingdom, a study conducted by Censu on behalf of the UK Safer Internet Centre (UKSIC) in connection with Safer Internet Day 2025 surveyed more than 2,000 children and adolescents aged 8–17 (Cawthorne, 2025). The results show that almost half of the participants report having been exposed to online scams at some point. The survey also shows that exposure to scams is a regular part of young people's online lives, with as many as 79% of children and adolescents stating that they encounter scam attempts at least once a month, of whom almost half (45%) at least once a week and 20% every day. These scams often involve false promises of free access to games or exclusive features, aiming to trick users into handing over personal information or their parents' credit card details (Cawthorne, 2025).

Research suggests that a key reason for this vulnerability is that children often have limited ability to anticipate the risks and consequences of their digital behaviors and choices (Quayyum et al., 2021). Similar concerns are highlighted by the Swedish awareness initiative "The Security Check", which identifies children and adolescents as a particularly vulnerable group, as they often lack both experience and the skills needed to recognize and resist fraudulent online behavior (Säkerhetskollen, 2024).

School plays a central role in preparing children to participate in a digitized society. The Swedish National Curriculum for Compulsory School, Preschool Class and School-Age Educare (commonly known and abbreviated Lgr22) states that students should be given opportunities to develop the skills needed to navigate the digital world. This includes not only using digital technology but also adopting a critical and responsible approach to it. The Swedish curriculum (including its official English translation) explicitly states (Skolverket, 2024, p. 8):

> Schools shall help pupils to develop an understanding of how digitalization affects the individual and societal development. All pupils shall be given the opportunity to develop their ability to use digital technology. They shall also

> be given the opportunity to develop a critical and responsible approach to digital technology, so that they are able to recognize opportunities, understand risks and evaluate information (Skolverket, 2024, p. 8).

At the same time, there are limited guidelines on how to implement these objectives in practice, particularly regarding cybersecurity-related education. This lack of practical direction becomes even more concerning in light of the results from the International Computer and Information Literacy Study 2023 (ICILS), presented by the International Association for the Evaluation of Educational Achievement (IEA) and reported in Sweden by the Swedish National Agency for Education (SNAE). The study shows that approximately 40% of Swedish eighth-grade students lack basic digital competence (Skolverket, 2023).

Anna Castberg, Chief Analyst at SNAE, commented on the findings in an interview with Swedish Radio. She emphasized it is concerning that many students lack basic computer skills and noted that frequent smartphone use does not necessarily translate into the ability to evaluate online information critically. As she explained, "you can spend a lot of time in front of a computer without developing the ability to evaluate the information you read" (Sveriges Radio, 2024, author's translation). [1]

Based on the results of the ICILS study, the IEA emphasized in an interview with the Swedish news agency TT that today's students require considerably more structured teaching in computer and information literacy and that it is no longer realistic to assume that children and adolescents will independently develop the digital skills required to navigate online environments safely (Wallström, 2024). This perspective is echoed by the Swedish Internet Foundation, which argues that schools need to equip students with the knowledge and skills required to critically evaluate information and navigate digital environments in a safe and responsible manner (Internetstiftelsen, 2025a).

1.1 Problem definition

Despite the growing importance of cybersecurity education in schools, there appears to be limited knowledge of how it is implemented in Swedish lower secondary education from the perspective of teachers. Although the Swedish curriculum emphasizes students' digital competence and responsible use of digital technology, it provides limited explicit guidance on cybersecurity education. Consequently, there is a need for a better understanding of how teachers interpret these curricular expectations, the challenges they encounter, and the factors that influence the implementation of cybersecurity-related teaching in Swedish classrooms.

Internationally, several studies have examined how cybersecurity and digital security awareness can be taught in primary and lower secondary education. Much of this research focuses on students' cybersecurity-related knowledge, attitudes, and online behaviors, as well as on evaluating educational interventions, such as

[1] – Man kan ju sitta mycket framför en dator utan att få en förmåga att värdera den informationen man läser. Anna Casterberg, Statens Skolverk.

pedagogical models, frameworks, games, and technical tools designed to improve cybersecurity awareness and promote good cyber hygiene (Saglam et al., 2023; Arishi et al., 2024). In comparison, there seem to be significantly fewer studies specifically examining teachers' perspectives, including their competence, available resources, time constraints, and the challenges they face when teaching cybersecurity-related topics.

Blažič and Blažič (2022) reported in a 2022 survey of students, parents, and teachers at European schools, that only 29% of students felt they received sufficient cybersecurity education. At the same time, 55% of teachers stated that they did, in fact, teach the subject. Still, a majority of them emphasized that limited time, often only a few hours per year, along with a lack of high-quality and fit-for-purpose educational materials, made it difficult to conduct teaching effectively.

A similar survey study was conducted in Bahrain, focusing on teachers and guardians (Ayyash et al., 2024). Of the 93 teachers who participated in the study, 64% stated that schools have a responsibility to increase students' cybersecurity awareness. Still, many simultaneously reported insufficient lack of sufficient resources, adequate time, and support to carry out this work. Regarding tools, teachers reported that instruction most often relies on narrative, problem-solving, and video-based methods, but that these methods are unevenly distributed and cannot always be implemented consistently due to time pressure and limited teacher competence (Ayyash et al., 2024).

1.2 Research Aims and Motivation

This study aims to examine how cybersecurity-related topics are integrated into teaching practices in Swedish municipal lower secondary schools. While previous research has examined cybersecurity education across a range of international contexts, there appears to be a lack of corresponding research focusing on Swedish lower secondary schools, particularly from the perspective of teachers. Investigating the Swedish context is of particular interest because the national curriculum emphasizes students' digital competence and responsible use of digital technology, while providing limited explicit guidance on how to incorporate cybersecurity-related topics into teaching. The purpose of this study is therefore to develop a clearer understanding of whether and how cybersecurity-related topics are integrated into teaching, as well as how teachers perceive their competence, available time, and access to pedagogical resources. By exploring both current practices and the challenges identified by teachers, the study seeks to provide insights into the opportunities and obstacles associated with teaching these issues in a systematic manner.

Another important motivation is that students aged 13–16 (i.e., at lower secondary level) are at a stage where their digital habits, behaviors, and risk awareness are still developing (Erukulla, 2026). At this age, many students begin to engage more independently with digital platforms such as social media, online gaming, and communication services, often without direct supervision. This increased exposure makes them particularly vulnerable to threats such as phishing, online scams, privacy violations, and social engineering (Erukulla, 2026).

While this increased independence may expose students to greater risks, it also creates opportunities for schools to support the development of safe and responsible digital habits. This focus is further supported by the Swedish national curriculum (Lgr22), which emphasizes that students should develop a critical and responsible approach to digital technology and an understanding of digital risks (Skolverket, 2024).

The geographical scope of the study was limited to municipal lower secondary schools in the Skaraborg region. In addition to being feasible within the timeframe of a master's thesis, Skaraborg includes both urban and rural municipalities, providing the opportunity to capture perspectives from a range of school contexts. Although the findings cannot be generalized to all Swedish schools, they may provide insights that are relevant to municipalities with similar educational conditions and contribute to the limited body of research on cybersecurity education in Swedish lower secondary schools. The larger number of secondary schools also provided a wider pool of potential participants if some schools would have declined to take part in the study.

An additional rationale for focusing on lower secondary education was informed by insights from the author's previous bachelor's thesis (Brifelt & Karlsson, 2023), which partly examined teachers in upper secondary schools. Teachers who participated in that study informally suggested that a greater focus on lower secondary education could yield additional insights, as teaching at this level often allows greater flexibility in lesson planning and content delivery than at upper secondary education, where instruction is more closely tied to specific programs and subject specializations. Although these observations were informal, they contributed to the decision to focus on lower secondary education in the present study.

1.3 Research Questions

To address the aim of the study, the following research questions were formulated:

- RQ1: How is cybersecurity-related teaching currently practiced in Swedish municipal lower secondary schools (grades 7–9) with a focus on the Skaraborg region?
- RQ2: How do teachers describe their instructional practices, available resources, competence, knowledge, and the conditions under which they teach cybersecurity-related topics?

These research questions guided both the design of the interview study and the subsequent thematic analysis presented in later chapters.

1.4 Delimitations and Scope

The study is delimited to publicly run municipal lower secondary schools in Sweden, specifically focusing on grades 7–9 (students typically aged 13–16). As mentioned previously, the geographical scope was limited to the Skaraborg region.

The study was also delimited in terms of participant roles, focusing exclusively on teachers. Perspectives from other stakeholders, such as school leadership or students, were not included.

In terms of data collection, the study was delimited to semi-structured interviews. Other methods, such as classroom observations or document analysis, were not included, since the focus was on gathering insights from participants' own experiences and perspectives (see Chapter 4). At the same time, some flexibility was allowed during the interviews. If participants chose on their own initiative to show or explain tools or materials they used in their classroom teaching, they were encouraged to do so. Such information was treated as additional context and did not alter the study's overall methodological approach.

The scope of the study was considered sufficiently broad to allow for meaningful analysis and discussion, while remaining manageable within the time constraints of a thesis study.

1.5 Thesis Structure

The remainder of this thesis is organized as follows. Chapter 2 provides the background to the study by introducing central concepts related to cybersecurity and presenting a selection of Swedish cybersecurity awareness initiatives relevant to the research context. Chapter 3 presents a small-scale systematic literature review of previous international research on cybersecurity education. Given the limited research identified in the Swedish context, the review was conducted to establish the current state of knowledge, identify recurring themes and research gaps, and provide a research-based foundation for the interview study. The findings from the review also informed the development of the interview guide used in this study.

Chapter 4 describes the research methodology, including the qualitative research approach, the use of semi-structured interviews, participant selection, data analysis procedures, and considerations related to validity and reliability (trustworthiness). The chapter also outlines the data collection process and the practical implementation of the study, including examples from the thematic coding applied to the interview results.

Chapter 5 presents the results from the interview study and provides an analysis of the empirical material. Chapter 6 discusses the findings and results in relation to previous research, reflects on the chosen methodology, and addresses the ethical and societal implications of the study. The chapter also suggests directions for future research. Finally, Chapter 7 concludes the thesis by summarizing the main findings and outlining the study’s contributions.

2. Background

This chapter introduces the background necessary to understand the research topic and its objectives. It provides essential context for the thesis and outlines key aspects related to the subject.

2.1 Preliminaries and Central Concepts

2.1.1 What is Cybersecurity?

The EU Cybersecurity Act defines *cybersecurity* as the activities required to protect network and information systems, their users, and others affected by cyber threats (European Court of Auditors, 2022). It is closely connected to *information security*, which is commonly structured around the principles of *confidentiality*, *integrity*, and *availability* (the CIA triad). Confidentiality refers to protecting information from unauthorized access, ensuring that only authorized users can access data. Integrity concerns maintaining the accuracy and completeness of information, ensuring it has not been altered or manipulated. Availability refers to ensuring that systems and information are accessible when needed (Pfleeger et al., 2015).

Similarly, the European Union Agency for Cybersecurity, abbreviated ENISA, frames cybersecurity as a broad socio-technical domain that includes technical controls, organizational processes, and human behavior (European Court of Auditors, 2022). ENISA further introduces the concept of *Cybersecurity Culture* (CSC), emphasizing how knowledge, attitudes, and values shape individuals' security-related behavior (ENISA, 2017).

From an industry perspective, Cisco defines cybersecurity as the protection of systems, networks, and applications against digital attacks, emphasizing that effective cybersecurity requires integrating people, processes, and technology (Cisco, n.d.-a). Cisco also uses the term interchangeably with *IT security* (Cisco, n.d.-b).

In an academic context, Ayyash et al. (2024) describe cybersecurity as a relatively recent concept that has become increasingly important in modern society and has gained significant attention in recent years. Cybersecurity can be understood as a set of processes, resources, and structures aimed at protecting the digital environment.

Similarly, Quayyum et al. (2021) describe cybersecurity as encompassing tools, policies, and educational efforts that help protect digital environments, as well as the digital assets of both individuals and organizations. The authors also present terms such as *cybersecurity*, *digital security*, *online safety*, *internet security*, and *information security* as closely related or synonymous concepts used to describe how security challenges in digital environments are addressed. At the same time, they emphasize that cybersecurity is a broad concept that can be applied across different contexts.

Taken together, these definitions demonstrate that there is no single, universally accepted definition of cybersecurity. Rather, the concept encompasses a broad range of technical, organizational, and human aspects of protecting digital environments. While the terminology varies across policy documents, industry, and academic literature, the concepts are closely related and often overlap.

In this thesis, *cybersecurity* is used as the primary term throughout the analysis and discussion. The study adopts the definition proposed by the European Court of Auditors (2022) as its conceptual foundation, and incorporates ENISA's concept of *Cybersecurity Culture*, which emphasizes both the technical and human dimensions of cybersecurity. Accordingly, cybersecurity is understood to encompass not only the protection of digital systems and information but also the knowledge, behaviors, and educational practices that enable individuals to recognize, understand, and manage cybersecurity-related risks. Within the context of this study, the term therefore includes the broad range of cybersecurity-related topics presented in the following section.

However, during the interviews, participants were also free to use related terms such as *digital security*, *IT security*, or *internet security*, as these may be more familiar in school contexts. This was clarified both in the interview invitations and at the beginning of each interview. The use of the term *digital security* was also further motivated by its closer alignment with the concept of digital competence in the Swedish national curriculum (Lgr22), making it potentially more familiar and contextually relevant to participants (Skolverket, 2024). For consistency, however, *cybersecurity* is used as the primary term throughout the written analysis and report.

2.1.2 Common Cybersecurity-Related Topics

The categories presented in Table 1 represent common aspects of cybersecurity, covering both technical aspects and human behavior. Most of these areas are based on definitions provided by Quayyum et al. (2021) and educational materials provided by Cybersecurityacademy.se. These aspects are grouped based on their general area of relevance but should not be interpreted as a ranking or order of priority. Instead, they serve as illustrative examples rather than a complete overview of the field. The purpose of presenting these areas is to provide a general understanding of the types of topics commonly associated with cybersecurity.

Table 1

Common Aspects Within Cybersecurity

Cybersecurity-related topics	**Description**
Social and societal aspects	
Source criticism and disinformation.	The ability to critically assess the credibility of online information.
Digital footprints.	Persistent traces of online activity that may impact privacy and reputation.

Sharing on social media.	The importance of reflecting before sharing personal information, images, or opinions.
Echo chambers.	Algorithm-driven reinforcement of existing beliefs, limiting exposure to diverse perspectives.
Cookies and targeted advertising.	Tracking technologies used to personalize content, sometimes including misleading or fake advertisements.
Cyberbullying.	Harassment or harmful behavior conducted through digital platforms
Grooming.	Manipulative behaviors targeting minors in online environments.
Privacy.	The right to control personal information and how it is collected, used, and shared.
Fraud and manipulation	
Phishing and scams.	Fraudulent messages attempting to obtain sensitive information such as passwords or financial data.
Fake profiles.	Accounts impersonating others to build trust or manipulate users.
Deepfakes and AI manipulation.	Synthetic media that challenges the reliability of digital content.
Clickbait and misleading content.	Content designed to manipulate users into clicking or believing exaggerated claims.
Investment scams.	Fraudulent schemes promising unrealistic financial returns.
Romance scams.	Exploitation of emotional relationships, usually for financial gain.
Technical aspects	
Encryption.	Protecting information by making it unreadable to unauthorized users.
Strong passwords	A foundational measure for preventing unauthorized access
Two-factor authentication (2FA):	Strengthening authentication through multiple verification factors.
Secure use of public networks	Awareness of risks associated with unsecured connections.
Viruses / Malware	Recognize malicious software and how to handle them.

2.2 Swedish Cybersecurity Awareness Initiatives

Several Swedish organizations offer initiatives and educational resources aimed at strengthening cybersecurity awareness and safer digital behavior across Swedish society, including materials relevant to schools and educators. To provide context for this study, this section presents examples from the Swedish Civil Defense and Resilience Agency (Myndigheten för civilt försvar, MCF), the Swedish Federation of Young Scientists (Förbundet Unga Forskare), the Swedish Internet Foundation (Internetstiftelsen), and the Security Check (Säkerhetskollen). These initiatives provide a broader picture of the resources available in the Swedish educational context and are also referred to in other parts of the thesis.

2.2.1 The Swedish Civil Defence and Resilience Agency (MCF)

MCF, formally known as the Swedish Civil Contingencies Agency (MSB), is a Swedish government authority responsible for strengthening society's ability to prevent, prepare for, and manage crises and emergencies. The agency works with areas such as civil preparedness, crisis management, information security, and the protection of critical infrastructure.

An important part of MCF's mission is to strengthen cybersecurity in Sweden by developing guidelines, educational materials, and training programs on information security for government agencies, companies, and the general public. The agency also supports organizations in their security efforts and promotes safer digital behavior through national information campaigns. One example is the campaign *Think Security* (*Tänk säkert*), a yearly national initiative aimed at helping citizens adopt safer digital habits in everyday life. The campaign highlights simple but effective practices such as using unique passwords, enabling multi-factor authentication, regularly updating devices and software, and recognizing common online threats (MCF, 2025).

While the agency also targets young people and provides some school-related materials, much of its contribution to cybersecurity education in schools is carried out through collaborations with partner organizations, particularly the initiative cybersecurity.se, which is described in the following section.

2.2.2 The Swedish Federation of Young Scientists

The Swedish Federation of Young Scientists (Förbundet Unga Forskare) is a Swedish non-profit youth organization founded in 1977 that promotes interest in science, technology, engineering, and mathematics (STEM) among adolescents. Through competitions, educational initiatives, and collaborations with schools and other organizations, the organization encourages curiosity and engagement with scientific topics both within and beyond the traditional classroom environment. Over the decades, the organization has played an important role in strengthening youth engagement in STEM fields across Sweden and continues to develop programs that make science more accessible to new generations of students (Unga Forskare, n.d).

In the autumn of 2019, the organization, in collaboration with MSB (now MCF) and the multinational technology company IBM, launched the initiative "Are You Secure? #290CyberSecurity" ("Är du säker?") - a nationwide information campaign aimed at Swedish lower and upper secondary schools focusing on information security awareness, promoting responsible use of the internet and linking digitalization to the United Nations Global Sustainability Goals (Unga Forskare, 2019). The project initially offered in-person educational sessions at schools but quickly transitioned to digital seminars due to the COVID-19 pandemic. Teachers were also provided with educational materials for use in future lessons. By the autumn of 2021, the initiative had reached schools in all of Sweden's 290 municipalities.

In the following years, the project expanded significantly and evolved to include the web platform cybersecurityacademy.se, which today provides free lesson plans and teaching materials for all school-age groups, from primary school to upper secondary education. The platform also offers pedagogical support, allowing educators to visit schools and assist teachers in delivering lessons on various cybersecurity topics. Importantly, the initiative not only focuses on technical cybersecurity concepts, but also addresses everyday digital safety issues including digital footprints, responsible social media use, cyberbullying, and online scams in games and other digital environments (cybersecurityacademy.se, 2025).

The organization also maintains a continuously updated record of schools that have requested access to the web platform or ordered their educational materials. Consequently, the organization was contacted during the planning phase of this study to determine whether any lower secondary schools in the selected region had previously engaged with its resources. Further information on this, together with additional details regarding the sampling process, is presented in Chapter 4: Research Methodology subsection 4.3: Selection / Sampling Group.

Overall, the initiatives from the Swedish Federation of Young Scientists represent an effort to strengthen digital awareness and cybersecurity knowledge among young people in Sweden, while supporting schools in preparing students for an increasingly digital society.

2.2.3 The Swedish Internet Foundation

The Swedish Internet Foundation (Internetstiftelsen) is an independent organization that works to ensure that the internet in Sweden remains stable, secure, and accessible to everyone. The organization was established in 1997 when the need arose for a clearly defined actor responsible for managing Sweden's top-level domain .se. Today, the Swedish Internet Foundation is responsible for operating and administering the top-level domains .se and .nu. (Internetstiftelsen, n.d).

In addition to its technical responsibilities, the foundation works to increase public knowledge about the internet through educational initiatives, guides, and reports on digital development and security. One example is the annual report *The Swedes and the Internet* (*Svenskarna och internet*), which analyzes how people in Sweden use the internet and how digital trends and behaviors evolve over time. (Internetstiftelsen, 2025b)

For several years, the foundation has been one of the organizations participating in MCF's national campaign *Think Security* (*Tänk säkert)*. Through this initiative, the foundation provides educational resources designed to help individuals become more secure and informed internet users. These include short courses and practical guides on recognizing phishing emails, protecting electronic identification (e-ID), creating strong passwords, and identifying common online scams such as fraudulent SMS messages, fake webshops, and deceptive phone calls.

The Swedish Internet Foundation also provides guidance for individuals who may already have been affected by online fraud, including advice on how to respond to suspicious links, fraudulent purchases, or scam calls claiming to come from government agencies. In addition, educational articles explain common cyber threats such as romance scams, investment fraud, and the growing use of artificial intelligence in online scams. Together, these efforts reflect the foundation's broader mission to promote a secure and well-functioning internet while strengthening public awareness of digital technologies and online security.

2.2.4 The Security Check

The Security Check (Säkerhetskollen) is a Swedish online service designed to help individuals and organizations better understand and improve their digital security. The service is provided free of charge by the Swedish Theft Prevention Association SSF (Stöldskyddsföreningen). It was introduced as a web service in the early 2010s, a period when cybercrime, data breaches, and online fraud were rapidly increasing, while many people still lacked the basic knowledge needed to protect their accounts and personal information online. The service is aim make cybersecurity easier to understand for everyday internet users and help them recognize risks that could lead to fraud or account takeovers (Säkerhetskollen, n.d).

One of the main features of the service is the ability to check whether an email address has been exposed in known data breaches. The Security Check also continuously monitors and maps new fraud methods used by cybercriminals. The service explains how these scams work and provides practical advice on recognizing and avoiding them before becoming victims. In addition, it offers simple security tests, guides, and educational material about online threats such as phishing, identity theft, and scams. It also includes information for parents, helping them understand the risks their children may encounter online and how to talk to them about safe internet use.

Furthermore, SSF, in collaboration with the Swedish Federation of Young Scientists, has contributed to the development of *Nätklok*, a free and interactive learning platform primarily aimed at children and adolescents. The resource is designed for use both in classrooms and at home. It includes quizzes and exercises to strengthen users' understanding of digital safety topics, including social media, passwords, online scams, and digital footprints. The service is available in both Swedish and English (Säkerhetskollen, 2025).

As demonstrated, several initiatives in Sweden aim to strengthen cybersecurity awareness and promote safer digital behavior among children, young people, educators, and the general public. These initiatives also demonstrate the growing availability of educational materials that schools can draw upon to support cybersecurity-related teachings. However, the existence of such resources does not necessarily reflect their actual use in schools or how, or to what extent, cybersecurity-related topics are addressed in everyday classroom practice, how teachers approach the subject, what content is prioritized, and what opportunities or challenges they encounter. To situate these questions within the broader research landscape, the following chapter therefore examines previous international research on cybersecurity education to establish the current state of knowledge, identify key research themes and gaps, and provide a foundation for the subsequent interview study.

3. Previous Research: Systematic Literature Review

This chapter presents a small-scale systematic literature review (SLR) focused on prior research related to cybersecurity education in primary and secondary school settings, with particular attention to teachers' perspectives, conditions, and challenges. By identifying and reviewing relevant research in the field, the review aimed to strengthen the study's theoretical foundation and provide a basis for the subsequent interview investigation.

In contrast to a traditional background section, the review follows a more structured and systematic process for selecting and analyzing prior research. As a result, it goes beyond a general overview and can be regarded as a small study in its own right. For this reason, it is presented as a separate chapter rather than being incorporated into the background section. Presenting the review independently also enhances transparency and makes it easier to highlight key findings and identify research gaps, thereby further justifying the relevance of this SLR.

The methodological approach for this SLR is primarily based on recommendations and guidance from *Handbok för systematiska litteratur- och dokumentstudier inom samhällsvetenskapen* by Funck and Karlsson (2021), with particular emphasis on strategies for searching and selecting academic articles. In addition, Oates's (2006) book *Researching Information Systems and Computing* later served as the methodological foundation for the thematic coding of the selected articles.

3.1 Literature Search Strategy

This section describes the literature search strategy used to identify relevant research for the SLR. It outlines the selection of the academic database, the Boolean operators and search terms used, as well as the criteria applied to guide the selection of relevant articles.

3.1.1 Database Selection

In more comprehensive literature reviews, it is common practice to search multiple academic databases during the initial phase. This approach helps researchers gain an overview of the existing body of research and assess whether a sufficient number of relevant and high-quality articles are available in the chosen field (Funck & Karlsson, 2021). However, since this literature review is of a more limited scope, only one academic database was initially selected, namely Scopus. Scopus was selected because of its broad coverage and high quality, containing approximately 29,000 active scientific journals and around 13 million peer-reviewed conference papers. An additional reason for this choice is that the database not only includes articles published directly in Scopus but also aggregates content from other well-known databases, such as IEEE Xplore, ScienceDirect, SpringerLink, and many others (Feldner, 2025). This makes Scopus a suitable and efficient database for conducting a limited literature review.

3.1.2 Boolean Operators and Search Terms

Funck and Karlsson (2021) emphasize the importance of using appropriate Boolean search terms and carefully selecting keywords. When searching for and selecting articles, it is not only the choice of academic databases that matters, but also how the searches themselves are conducted. To efficiently identify relevant articles, so-called Boolean search terms, also referred to as operators, such as AND, OR, and NOT, are commonly used. These make it possible to combine multiple keywords or to narrow down search results. The keywords themselves naturally play a crucial role, and it is therefore appropriate to base them on key concepts from the study's research question and inclusion criteria. Based on this, several relevant keywords can be identified and used in different combinations to increase the likelihood of finding suitable articles. In addition, parentheses can be used to group related search terms and clarify the relationship between different Boolean operators, thereby enabling more structured and precise searches.

The following Boolean search and keywords were used:

TITLE-ABS-KEY ((cybersecurity AND education AND ("middle school*" OR "secondary school*" OR "elementary school*" OR "K-12") AND teach*) OR (cybersecurity AND school* AND (teacher* OR extracurricular)) OR (cybersecurity AND school* AND ("systematic review" OR "systematic literature review")) OR ("digital safety" AND "elementary school*" AND teacher*)) AND PUBYEAR > 2018 AND PUBYEAR < 2026 AND (LIMIT-TO (LANGUAGE, "English") OR LIMIT-TO (LANGUAGE, "Swedish"))

3.1.3 Search Criteria

In addition to Boolean operators, Funck and Karlsson (2021) stress the importance of adopting a structured and systematic approach from the very outset of the academic database search process by clearly defining inclusion and exclusion criteria. This is essential to ensure that the identified research articles are high-quality and directly relevant to the study's aims and research questions.

The search criteria used during the literature study are presented in Table 2. The criteria are divided into inclusion and exclusion criteria, which were applied at different stages of the search and screening process. Some of the inclusion criteria were applied during the database search, while the full set of inclusion criteria was used during the subsequent title screening. The abstracts of the remaining records were then reviewed to assess their relevance to the study, followed by a more detailed eligibility assessment using the exclusion criteria.

Notably, the language criteria and the publication period criteria were applied both directly in the Boolean database search and again during the subsequent screening process to ensure that all selected studies met these requirements.

Table 2
Search Criteria

Inclusion criteria	Exclusion criteria
Relevant educational population and context. Studies addressing teachers and/or students were included to ensure relevance to the study's educational focus.	**Publication period**. Studies published outside the period 2019–2025 were excluded to maintain a focus on recent research, particularly given the rapid development of cybersecurity.
Language. Studies published in English or Swedish were included to provide access to both international and Swedish research.	**Lack of full-text access.** Studies were excluded when the complete text could not be accessed, including articles behind a paywall or otherwise requiring restricted access.
Peer-reviewed. Only peer-reviewed studies were included to ensure that the research had undergone academic review.	**Irrelevant focus despite initial search relevance.** Studies were excluded when closer examination showed that cybersecurity was mentioned but not addressed within an educational context.
Publication type. Journal articles and conference papers were included to ensure that the studies were published within an academic context.	**Population or educational level outside the scope.** Studies focusing exclusively on populations outside the relevant educational context were excluded.
Database availability. Studies identified through academic databases accessible via the University of Skövde.	**Insufficient academic rigor.** Studies were excluded when the methodology, implementation, or results were insufficiently described to allow adequate assessment.

3.2 Literature Search, Screening Process and Supplementary Articles

The literature search and screening process was conducted in February 2026. The search and screening process is presented in Table 3 and follows a flowchart structure proposed by Funck and Karlsson. To improve readability and conserve space, the procedure is presented as a table rather than as a graphical flowchart. In addition, step 5 was added to account for the practical scope and time constraints of this master's thesis.

Table 3
Screening Process

Steps	Description	Number remaining
Step 1: Identification	203 records were identified through the database searches. 2 duplicates were removed.	201 records
Step 2: Inclusion and title screening	The identified records were screened according to the inclusion criteria and by reviewing their titles.	104 records
Step 3: Abstracts screening	The abstracts of the remaining records were reviewed to assess their relevance to the study.	62 records
Step 4: Eligibility assessment	The remaining articles were assessed in greater depth for eligibility using the exclusion criteria.	35 articles
Step 5: Scope-based selection	Due to the scope of this master's thesis, 19 eligible articles were selected, prioritizing studies in which teachers' perspectives were clearly represented.	19 articles
Step 6: Analysis	The final articles were included in the literature review and analyzed in full.	19 articles

In addition to the initial 19 articles identified through the primary database search, two further articles were later included following a manual search of the reference lists of the selected studies (backward citation searching), resulting in a total of 21 articles included in the final analysis. These two articles later added are marked with an asterisk (*) in Table 4.

Table 4 presents the 21 articles that were ultimately included in the systematic literature review and analyzed in full. The articles are listed in alphabetical order by the authors' last names to ensure consistency with the APA-formatted reference list.

Table 4
Articles Read and Analyzed in Full

Author(s)	Article title
* Amin et al. (2024)	Securing young minds: Analyzing primary teachers' perspectives and practices in cyber safety
Arishi et al. (2024)	Cybersecurity awareness in schools: A systematic literature review of practices, challenges, and target audiences
Ayyash et al. (2024)	Cybersecurity education and awareness among parents and teachers: A survey of Bahrain
Blažič & Blažič (2022)	Cybersecurity skills among European high-school students: A new approach in the design of sustainable educational development in cybersecurity
Childers et al. (2022)	K–12 educators' self-confidence in designing and implementing cybersecurity lessons
Hossain et al. (2024)	Empowering K–12 STEM educators: Enhancing cybersecurity awareness through professional development

Ibrahim et al. (2024)	A systematic review of K–12 cybersecurity education around the world
Lamond et al. (2025)	Teachers' perspectives and practice of cybersecurity education in primary schools
* Liu et al. (2025)	Systematic review of elementary cybersecurity education: Curriculum, pedagogy, and barriers
Lorenz (2025)	Improving cybersecurity education in schools: An assessment of the "Digitally Safer School" proposal
Lorenz & Kikkas (2020)	"Trust me, you will need it": Cybersecurity as extracurricular subject at Estonian schools
Martin et al. (2022)	Teacher and school concerns and actions on elementary school children digital safety
McLeod et al. (2024)	Comparing teacher and creator perspectives on the design of cybersecurity and privacy educational resources
Mourning et al. (2023)	Reflections of cybersecurity workshop for K–12 teachers
Pencheva et al. (2020)	Bringing cyber to school: Integrating cybersecurity into secondary school education
Prior & Ophoff (2024)	Lessons learnt from using educational phishing materials with UK primary school children
Renieri et al. (2025)	WalkthroughCyber: Teaching cyber-awareness in Montessori middle schools
Saglam et al. (2023)	A systematic literature review on cyber security education for children
Videnovik et al. (2024)	A novel methodological approach for learning cybersecurity topics in primary schools
Videnovik et al. (2025)	Using peer-learning and game-based instruction for achieving long-lasting knowledge of cybersecurity in primary schools
Xu & Li (2025)	Cybersecurity matters for primary school students: A scoping review of the trends, challenges, and opportunities

3.3 Thematic Coding Process and Identified Themes

To analyze the selected articles, thematic coding was applied. In this process, the researcher first identifies and documents recurring codes while reading and summarizing each article in full. These codes represent specific concepts, patterns, or observations found in the material related to the research questions. According to Oates (2006), thematic coding is a suitable method for identifying patterns in texts, as it is not strictly tied to any specific theory.

As the analysis progresses, related codes are compared and grouped together to form broader themes. In this way, themes are not predefined but emerge inductively from the data. When a new code is identified for the first time, it is documented and later assessed in relation to existing codes. If several articles contain codes that can be combined under the same broader concept, these are consolidated into a common theme and included in the subsequent analysis.

Table 5 presents the themes identified through the coding process. The table is divided into themes and the associated codes used to identify said themes, as well as the authors in whose works these codes and subsequent themes were

identified. The table thus provides a clear overview of how the different themes occur within the material and how they are related to one another.

Originally, the plan was to exclude themes identified only from codes originating in a single article. The rationale behind this was to ensure that the identified themes had clear support across multiple studies and are therefore relevant to the subsequent analysis (Oates, 2006). During the coding process, however, it became evident that all identified codes and subsequent themes appeared in more than one article. As a result, no themes needed to be excluded, and all were included in the final analysis.

Table 5
SLR Thematic Coding Results

Theme	**Associated codes**	**Article authors**
1: Limitations in the delivery of education.	• Cybersecurity is given limited space in teaching. • Integrated sporadically into other subjects. • Taught on specific occasions. • Cybersecurity as a project or voluntary subject. • Lack of long-term progression.	Arishi et al. (2024), Blažič & Blažič (2022), Ibrahim et al. (2024), Liu et al. (2025), Lorenz & Kikkas (2020) Martin et al. (2022), Prior & Ophoff (2024), Renieri et al. (2025), Saglam et al. (2023), Videnovik et al. (2024), Xu & Li (2025)
2: Access to (and quality of) teaching resources	• Lack of pedagogical grounding and age-appropriate materials. • Dependent on individual teacher capacity. • Outdated educational materials. • Materials perceived as overly technical. • Need for accessible materials. • Materials developed collaboratively with researchers in specific projects.	Amin et al. (2024) Arishi et al. (2024), Ayyash et al.(2024), Childers et.al (2022), Lamond et al. (2025), Liu et al. (2025), McLeod et al. (2024), Saglam et al. (2023), Videnovik et al. (2024), Videnovik et al. (2025), Xu & Li (2025)
3: Teachers' knowledge, confidence and professional development	• Perceived lack of knowledge. • Teachers often report low levels of cybersecurity knowledge. • Uncertainty regarding technical threats. • Uncertainty regarding how to teach it effectively.	Ayyash et.al. (2024), Childers et.al (2022), Hossain et.al. (2024), Lamond et al. (2025), Liu et al. (2025), Mourning et al. (2023), Pencheva et.al. (2020) Prior & Ophoff (2024) Xu & Li (2025)

	• Need for professional development and workshops	
4: Governance, curriculum and organizational frameworks	• Unclear placement of cybersecurity education in policy documents and curricula. • Unclear instructional goals. • Uneven implementation between schools nationally. • Uneven implementation between schools internationally.	Arishi et al. (2024), Blažič & Blažič (2022), Ibrahim et al. (2024), Liu et al. (2025) Lorenz. (2025), Saglam et al. (2023)
5: Pedagogical approaches and the teacher's role	• Student-centered methods. • Game-based and hands-on learning. • Pedagogical responsibility. • Teacher as supervisor, tutor and organizer	Amin et al. (2024) Ayyash et.al. (2024), Blažič & Blažič (2022), McLeod et al. (2024), Pencheva et.al (2020), Prior & Ophoff (2024), Renieri et al. (2025), Videnovik et al. (2024), Videnovik et al. (2025)

3.4 Thematic Analysis

In this section, a more in-depth analysis of the themes identified during the article review is presented. The analysis is organized using headings based on the main themes identified during the thematic coding process.

3.4.1 Limitations in the Delivery of Education

A consistent finding in the literature is that cybersecurity is given limited time and space in classroom instruction. Rather than being treated as a coherent and progressive area of knowledge, it is typically integrated sporadically into existing subjects such as technology, social studies, or computer science.

This reflects broader structural constraints within education systems, where new content areas must compete with already established curricular priorities. Ibrahim et al. (2024) highlight how overloaded curricula restrict the inclusion of cybersecurity, even when its importance is widely recognized. Similarly, Liu et al. (2025) point to gaps in curriculum design and coordination, showing that inconsistencies across schools, teachers, and policymakers further limit structured implementation.

Adding to these challenges, the interdisciplinary nature of cybersecurity often creates conceptual uncertainty. As noted by Ibrahim et al. (2024), unclear terminology and overlapping domains make it difficult to define what should be included in teaching. This is reinforced by Xu and Li (2025), who show that many initiatives lack coherence and remain fragmented, resulting in a more superficial understanding among students. Blažič and Blažič (2022) further argue that

school curricula often struggle to keep pace with rapidly evolving digital risks, creating a gap between what students learn and what they need to know.

In many contexts, cybersecurity education is delivered through short-term or peripheral formats, such as theme days, workshops, or extracurricular activities. While these initiatives can be engaging, they often limit both reach and continuity. Lorenz and Kikkas (2020) also show that such activities tend to attract already motivated students, while others are left without exposure, which affects equal access to knowledge.

The limitations of these approaches are also visible in empirical studies. Prior and Ophoff (2024) show that while students can improve their ability to recognize phishing attempts after just a lesson, these effects often decrease over time without continued reinforcement. A similar pattern is identified by Saglam et al. (2023), who show that isolated awareness activities have limited long-term impact unless they are part of a broader teaching structure.

Related challenges are also visible in teaching practice. Martin et al. (2022) show that teachers often address issues such as cyberbullying and privacy concerns reactively rather than through structured and preventive instruction. Arishi et al. (2024) similarly note that cybersecurity efforts often focus on responding to incidents rather than building sustained awareness over time. As a result, teaching often becomes more situational than systematically planned.

Even when more structured approaches are proposed, challenges remain. Videnovik et al. (2024) emphasize that effective cybersecurity education requires interactive and engaging methods, such as game-based learning and peer instruction, but also point out that schools often lack the time, resources, and expertise to implement these approaches consistently. Similarly, Renieri et al. (2025) highlight that there is still no clear agreement on how cybersecurity should be taught in practice, particularly regarding approaches support continuity and progression.

3.4.2 Access to (and quality of) Teaching Resources

A second clear theme concerns access to teaching resources. The literature highlights a lack of ready-made, age-appropriate, and pedagogically structured materials for cybersecurity education. Although many resources exist, they are often too technical, too abstract, or designed for older students, which makes them difficult to use in compulsory schooling. Amin et al. (2024) further show that many of these resources also lack clear structure for classroom use, forcing teachers to interpret and adapt them on their own.

As a result, teachers express a need for more practical and accessible materials, especially those using simple language and real-life examples.

Ayyash et al. (2024) show that storytelling, problem-solving, and video-based approaches are seen as effective ways to communicate cybersecurity concepts to students. However, Xu and Li (2025) note that many existing resources are outdated or poorly implemented, which limits their usefulness in practice.

The gap is particularly clear in primary and lower secondary education, where materials often do not match students' cognitive level. Lamond et al. (2025) show that even basic topics, such as passwords can be difficult for younger students

when teaching materials do not account for their developmental abilities. More broadly, Liu et al. (2025) identify gaps in curriculum consistency, teacher support, and pedagogical structure, while Saglam et al. (2023) show that cybersecurity content varies widely and lacks coherence across contexts and lacks consistency.

Another issue concerns how resources are designed and used in practice. McLeod et al. (2024) show a clear mismatch between resource creators and teachers. While creators often design complex and interactive tools, teachers tend to use simple, flexible materials such as short videos or basic lesson plans, mainly because they are easier to adapt to everyday classroom situations.

Consequently, the quality of instruction becomes highly dependent on individual teachers' capacity rather than being supported by consistent and well-designed educational materials. Childers et al. (2022) show that teachers' confidence is closely linked to access to resources and training, while Arishi et al. (2024) identify limited resources as a key barrier to implementation.

As a response to these challenges, teaching materials are often developed within the framework of individual research projects. Many articles present their own pedagogical solutions, such as games, digital tools, phishing exercises, or interactive workshops. For example, Videnovik et al. (2024) show that combining peer learning with game-based approaches can improve engagement, while Videnovik et al. (2025) show that such approaches can support longer-term knowledge development. However, few articles report conducting follow-up visits to assess whether their proposed ideas are implemented on a long-term basis within the schools' regular activities, and Liu et al. (2025) highlight challenges related to sustaining such initiatives.

3.4.3 Teachers' Knowledge, Confidence and Professional Development

Several studies show that teachers experience limited knowledge and low confidence when it comes to educating students in areas related to cybersecurity. This is particularly evident in more technical areas and rapidly evolving threats, such as phishing, social engineering, and digital attacks. Teachers describe cybersecurity as a complex subject that requires continuous updating, making it difficult to manage within the constraints of their regular workload.

This is reflected in findings by Pencheva et al. (2020), in which teachers expressed strong interest in teaching cybersecurity but reported a lack of both subject knowledge and adequate support. Similarly, Liu et al. (2025) show that teachers often feel unprepared to address cybersecurity topics, particularly due to gaps in training and coordination across the education system.

This lack of knowledge is closely linked to teachers' self-confidence and willingness to teach the subject. Teachers often report low confidence when dealing with cybersecurity content, particularly when it is perceived as technical or unfamiliar. As a result, even when teachers recognize the importance of cybersecurity education, uncertainty about how to teach the subject can lead to avoidance. Prior and Ophoff (2024) show that teachers face difficulties delivering cybersecurity lessons due to limited topic knowledge and a lack of clear guidance or

structured teaching materials. This suggests that both subject knowledge and pedagogical support are necessary for effective implementation.

The need for professional development therefore emerges clearly in the literature. Several studies show that targeted training initiatives can strengthen both teachers' knowledge and confidence. Childers et al. (2023), for example, found that participation in a structured professional development workshop increased teachers' self-confidence in several aspects of designing and implementing cybersecurity lessons. Similarly, Hossain et al. (2024) report that participation in cybersecurity training improved teachers' awareness of online risks and their understanding of key concepts, while Mourning et al. (2023) show that hands-on workshops supported the development of practical teaching strategies and classroom-ready materials.

At the same time, such initiatives are often time-limited and project-based, which risks their impact diminishing over time if they are not followed up or integrated into teacher education and in-service training. This limitation is also reflected in broader reviews. Xu and Li (2025) note that many cybersecurity education initiatives often suffer from limited implementation and lack of long-term integration, while Liu et al. (2025) identify ongoing gaps in teacher preparation and systemic support

In addition, challenges remain in providing teachers with the support needed to implement cybersecurity education effectively. Ayyash et al. (2024) identify gaps in teacher confidence and institutional preparedness, while teachers in their study emphasized the need for further training, appropriate educational resources, and guidance on effective teaching approaches. Similarly, Lamond et al. (2025) show that primary school teachers express a clear need for additional training, curriculum support, and age-appropriate guidance.

Finally, these challenges are not limited to teachers alone. Ayyash et al. (2024) show that both parents and teachers identify shortcomings in cybersecurity awareness and preparedness, as well as challenges concerning responsibility for supporting children's online safety. This indicates that teacher competence is part of a broader issue in which effective cybersecurity education depends on support and coordination between multiple stakeholders.

3.4.4 Governance, Curriculum and Organizational Frameworks

A common finding is that cybersecurity does not have a clear or consistent place in policies or school curricula. Several systematic reviews show large differences between countries and education systems, both in what is taught and the level of ambition. For example, Sağlam et al. (2023) show that cybersecurity content varies widely between countries and is often inconsistent and fragmented. Similarly, Ibrahim et al. (2024) note that many aspects of cybersecurity are not taught in a structured way in K–12 education, partly due to limitations in current curricula. This leads to unclear teaching goals and makes it difficult for teachers to know what they should include.

The literature also shows that cybersecurity is often included within broader areas like digital literacy or digital competence, without clear definitions or boundaries. Ibrahim et al. (2024) explain that unclear terms and overlapping topics make it hard to define what cybersecurity education should cover. This lack of

clarity leads to fragmented teaching and makes it difficult to create consistent practices. In addition, differences between policies, curriculum frameworks, and teaching resources make implementation more difficult, leaving teachers without clear guidance. Liu et al. (2025), for example, identify gaps in curriculum design, policy support, and coordination between stakeholders, all of which affect how cybersecurity is taught in practice.

The lack of clear guidelines also leads to differences between schools. When guidance is unclear, teaching often depends on local initiatives or individual teachers' interests. Arishi et al. (2024) show that schools often rely on separate awareness activities rather than structured programs, partly due to limited policy support. As a result, students are given unequal opportunities to learn about cybersecurity depending on which school they attend, even within the same national border.

Furthermore, studies show that effective cybersecurity education requires coordination between different stakeholders. Liu et al. (2025) highlight the importance of connections between different levels of the education system. Similarly, Blažič and Blažič (2022) argue that a well-functioning system needs better alignment between actors such as policymakers, schools, and industry. Lorenz (2025) also highlights the need for more structured and coordinated approaches instead of isolated initiatives. However, he notes that such coordination is often limited, making it harder to build a coherent and sustainable educational approach.

3.4.5 Pedagogical Approaches and the Teacher's Role

Finally, the literature indicates that education in cybersecurity is often delivered through student-centered and hands-on approaches. Discussion of real-world scenarios, group work, workshops, and practical exercises are commonly used to make the subject more concrete and engaging for students. Studies consistently highlight interactive and experiential learning methods, such as serious computer games, as particularly effective for developing students' understanding and skills (Blažič & Blažič, 2022; Videnovik et al., 2025). For example, Renieri et al. (2025) describe how participatory lessons combined with game-based activities allow students to actively engage with cybersecurity concepts, while Videnovik et al. (2024) show that combining peer learning with interactive tasks can support collaboration and shared knowledge construction in the classroom. This is also reflected in Pencheva et al. (2020), who emphasize the value of using real-life scenarios and simulations, such as phishing cases or role-based activities, to make learning more meaningful and engaging for students.

Despite these advantages, these approaches require careful design and adaptation to be effective. Research shows that interactive learning is most successful when supported by clear learning objectives, as activities may otherwise be engaging yet lack educational depth (Videnovik et al., 2024). In contrast, Pencheva et al. (2020) highlight an opposite challenge, showing that overly theoretical or lecture-based approaches can reduce student engagement. Together, these findings point to the importance of balancing engaging and structured teaching approaches.

The literature also clearly indicates that the teacher's role remains pivotal, even within these alternative or research-driven forms of instruction. In projects where researchers introduce educational tools or activities in classrooms, the

teacher often continues to function as a supervisor, coordinator, and quality assurer. McLeod et al. (2024) show that teachers actively select and adapt resources to fit their classroom contexts, often preferring simple and flexible materials that can be easily integrated into everyday teaching. Similarly, Prior and Ophoff (2024) highlight that even structured activities depend on teacher guidance to support students' understanding and learning processes.

The teacher is also responsible for adapting the content and methods to the students' age, maturity, and prior knowledge. Studies show that this often involves using simple language, real-life scenarios, and accessible materials to make abstract cybersecurity concepts understandable (Amin et al., 2024; Ayyash et al., 2024). In addition, teachers play a key role in contextualizing cybersecurity concepts and connecting them to students' everyday digital experiences.

The literature thus shows that successful cybersecurity education is not solely dependent on pedagogical methods but, to a large extent, on teachers' conditions and professional competence.

3.4.6 Thematic Analysis Summary

Overall, the resulting themes demonstrate that cybersecurity education across primary and secondary education is shaped by a combination of curricular and structural limitations, insufficient access to appropriate teaching resources, and a pronounced need for professional development among teachers. Cybersecurity is often marginalized within the curriculum, implemented inconsistently, and frequently dependent on individual initiatives rather than systematic, long-term planning. These conditions make it difficult to establish coherent progression and to ensure that all students receive equal opportunities to develop essential knowledge and skills related to safe and responsible online behavior. Addressing these challenges therefore requires support that extends beyond the individual teacher. Taken together, these findings underscore the need for a more structured and coordinated approach to cybersecurity education, in which policy, curriculum, teacher training, and teaching resources are better aligned.

The results further highlight a clear research gap, as much of the existing literature in general primarily focuses on students' knowledge and behaviors, while teachers' perspectives, working conditions, and professional needs receive considerably less attention. At the same time, the included studies reinforce the importance of focusing on teachers. Given the central role they play in planning, delivering, and adapting cybersecurity education, their prerequisites and challenges are crucial to understanding how such instruction can be successfully implemented in practice.

This underlines the need for continued research that places greater emphasis on the teacher's role, with the aim of informing policy development, curriculum design, and targeted support structures for cybersecurity education in schools.

3.5 Thematic Foundation for Interview Study

The five themes identified in the literature analysis guided the design of the interview study and served as a foundation for its overall structure. Rather than being treated as isolated categories, these themes were understood as interconnected dimensions shaping how cybersecurity education is experienced and implemented in practice. The themes therefore informed both the development of the interview guide and the formulation of the interview questions, ensuring that the study addressed central issues consistently highlighted in previous research.

However, it is important to clarify that the goal of the interview study was not primarily to systematically test, verify, or directly compare findings from previous international research. Instead, the results from the literature review mainly served as an initial analytical foundation that helped structure both the data collection and the broader areas of analysis, while still allowing new insights to emerge from the interviews. In this way, the study combined a deductive starting point based on previous research with inductive analysis within and across these broader thematic areas, allowing teachers' own experiences and perspectives to add nuance, challenge, or expand the existing themes.

In line with this, the discussion based on the interview results did not aim to present a direct comparative analysis between the interview findings and previous research. Rather, the intention was to identify possible thematic similarities, recurring patterns, and points of connection between the participants' experiences and the broader research field. This approach allowed the study to remain grounded in existing research while maintaining its exploratory focus on how these issues were understood and managed within real classroom contexts.

4. Research Methodology

This chapter covers the research approach of the study, the methodology used for collecting data, the selection of participants and the reasoning for their selection, the chosen method for conducting data analysis, and the trustworthiness of the study. The chapter also covers the practical implementation of the data collection process and provides examples of the thematic coding conducted on the interview material.

4.1 Qualitative Research Approach

According to Merriam and Tisdell (2016), a qualitative approach focuses on understanding how people interpret situations and how they make sense of their surroundings. Instead of measuring phenomena through numerical data, qualitative research explores the meanings people attach to events, practices, and situations. The aim is therefore to understand how participants describe and interpret a phenomenon within its real-life context. Another important characteristic is that qualitative research is for the most part inductive. This means that the researcher gathers data first and then develops interpretations from that data, rather than starting with a prechosen theory to test. However, the present study was not entirely inductive, but combined inductive and deductive elements. As described in Section 3.5, the themes identified in the literature review provided a deductive starting point for the interview study, while the teachers' responses were analyzed inductively within and across these broader thematic areas.

Data in qualitative research is commonly collected through interviews, observations, or document analysis. During the analysis process, information from the collected data is examined and grouped into patterns or themes. These themes help the researcher move from specific observations toward broader interpretations and understanding. Since the aim of this study is to gain a deeper understanding of how cybersecurity and related topics are taught in Swedish lower secondary schools and how teachers describe their instructional practices, resources, competence, and teaching conditions, a qualitative approach is considered appropriate for answering the established research questions.

4.2 Semi-structured Interviews

The research method used to collect empirical data in this study is semi-structured interviews. Semi-structured interviews are a common data collection method in qualitative research and combine elements of both structured and unstructured interviews. In this type of interview, some questions are prepared in advance in an interview guide, while the format remains flexible enough to allow participants to explain their views in their own words and elaborate on their answers (Oates, 2006). This allows the researcher to focus on relevant topics while still giving participants the freedom to introduce additional ideas or aspects they consider important.

Both semi-structured and unstructured interviews allow participants to "say what they think" and are often used when the main goal is to discover and explore perspectives rather than control specific variables (Oates, 2006). Because of this,

they are commonly used in in-depth studies aimed at understanding participants' views, interpretations, and professional practices.

Another advantage of interviews is that they allow the researcher to ask follow-up questions and clarify responses during the conversation. This flexibility makes it possible to capture nuances, explanations, and practices that might otherwise remain unnoticed in more structured forms of data collection. For example, a teacher might respond negatively in a survey when asked whether cybersecurity is taught in their classes, while an interview may reveal that related topics are still addressed indirectly through lessons on source criticism, fake news, grooming, or phishing.

In this study, semi-structured interviews were therefore chosen to gain a deeper understanding of how teachers described their instructional practices, available resources, competence, and the conditions under which they taught cybersecurity and related areas. In addition, because teaching practices and conditions varied between schools, the method provided insights into differences in how the subject was addressed across different municipalities.

The development of the interview guide drew on two primary sources: *Researching Information Systems and Computing* by Oates (2006), which informed the interview procedure, and *Qualitative Research: A Guide to Design and Implementation* by Merriam and Tisdell (2016), which guided the structure and formulation of the interview questions. These sources provided methodological guidance on how to conduct semi-structured interviews, ensuring that the questions remained open enough to encourage detailed responses while still maintaining a clear focus on the research objectives.

The interview questions were developed and organized around broader subject areas established from the main themes identified in the literature review, which provided the overall structure for the interview guide. For example, several reviewed studies highlighted teachers' limited cybersecurity competence, lack of suitable teaching materials, and insufficient instructional time as recurring challenges (e.g., Blažič & Blažič, 2022; Ayyash et al., 2024). These findings informed interview questions exploring teachers' self-perceived competence, access to pedagogical resources, and the conditions under which cybersecurity-related topics were taught. Similarly, the literature identified considerable variation in how cybersecurity was integrated into teaching, which motivated questions concerning teachers' instructional practices and the subjects through which these topics were addressed. The interview guide was subsequently organized around these themes, allowing the interviews to proceed in a structured yet flexible manner.

The interview guide was also reviewed by the supervisor during its development, and the questions were further refined based on the feedback received. Before the main interviews were conducted, a small pilot study was carried out with three teachers from the researcher's personal network (who did not participate in the main study). Based on the feedback from the pilot participants, minor adjustments were made to the wording and structure of some questions. The revised interview guide was then used throughout the main data collection process. A complete overview of the final interview guide is provided in Appendix A.

4.3 Selection / Sampling Group

A purposive sampling strategy was used to ensure that participants had relevant experience related to the study's focus. As mentioned under "Delimitations and Scope", this study targeted teachers working in lower secondary schools (grades 7–9) within the Skaraborg region. As of spring 2026, there were 27 public municipal schools providing lower secondary education in the region. Of these, 20 were so-called "dedicated" lower secondary schools, meaning institutions that exclusively provided education for grades 7–9. These 20 schools constituted the sampling frame for the study. This was done to ensure a more focused and comparable context among participants. Schools were contacted via email with an invitation to participate in the study. In the invitation, schools were asked to nominate teachers whom they knew or believed actively worked within the relevant subject area of the study, rather than selecting participants at random. This approach was used to increase the likelihood that participants possessed relevant knowledge and experience.

As mentioned in Chapter 2, before contacting the schools, the Swedish Federation of Young Scientists was consulted to determine whether any lower secondary schools in the Skaraborg region had requested their educational materials. They reported that all public lower secondary schools in the region had done so at some point between 2019 and 2025. However, they were unable to provide more detailed information regarding when the materials had been ordered or who at each school had made the request. While this suggested a general interest in cybersecurity-related content among these schools, it did not reveal how, or to what extent, the materials had actually been used in teaching.

The interviews were intended to be conducted primarily through digital meeting platforms such as Teams, Zoom, and Google Meet. The rationale for this approach was that digital interviews provide greater flexibility for participants and facilitate scheduling without requiring travel. At the same time, the environment in which an interview takes place can influence participants' responses. If participants feel stressed or uncomfortable during an interview, there is a risk that their responses may become brief or less carefully considered (Oates, 2006). It was therefore considered important to prioritize an interview environment in which participants felt safe and comfortable. For this reason, on-site interviews were also offered as an alternative when scheduling, availability, and practical circumstances permitted. Using the University of Skövde as a reference point, the maximum travel distance to a relevant lower secondary school was estimated to be approximately 70 kilometers by car, which was considered acceptable within the scope of the study.

Regardless of location or format, the interviews were audio-recorded (with the teacher's consent) and subsequently transcribed. After reviewing and correcting the transcription, a finished copy, including a summary, was sent back to the participants to ensure that the written record accurately reflected the content of the interview.

4.4 Data Analysis: Thematic Coding

The data collected through the interviews were analyzed using thematic coding, building on the thematic analytical approach used in the systematic literature review presented in Chapter 3. As discussed previously, qualitative data analysis often involves identifying themes and patterns within the collected material, with codes and categories being developed through the analytical process. Since the study included teachers with diverse backgrounds and experiences, thematic analysis was considered an appropriate method, as it enables the identification of similarities and differences across participants' responses. The resulting themes provide a clear and systematic framework for presenting the findings, facilitating the interpretation and comparison of patterns across participants' accounts while supporting well-grounded conclusions. For these reasons, thematic analysis was considered particularly suitable for analyzing the interview data in this study, as it supports both depth and comparability in the interpretation of qualitative material (Oates, 2006).

Although the interview guide was informed by the themes identified in the systematic literature review, the analysis combined deductive and inductive elements. The five literature-derived themes provided the overarching deductive structure for the interview analysis. Within and across these broader thematic areas, the interview material was coded inductively to identify more specific patterns, perspectives, and subthemes from the teachers' own accounts. The literature-derived themes were therefore not treated as fixed codes that the interview data simply had to confirm. Instead, the analysis remained open to findings that could support, challenge, expand, or add nuance to previous research.

Once the coding process was complete, the resulting subthemes and patterns were considered alongside the findings of the literature review to identify areas of similarity and difference, as well as findings specific to the Swedish context.

4.5 Validity, Reliability and Bias (Trustworthiness)

Merriam and Tisdell (2016) emphasize that in qualitative research, validity and reliability are best understood through the concept of trustworthiness, which includes credibility, dependability, confirmability, and transferability. These concepts focus on how accurately the findings reflect the participants' perspectives and how consistently and transparently the study has been carried out.

Credibility refers to the extent to which the findings are believable and accurately reflect participants' experiences. In semi-structured interviews, credibility is closely linked to how questions are understood and interpreted. Since qualitative research focuses on people's meanings and experiences, there is a risk that participants understand important concepts differently. For example, the term cybersecurity may mean different things depending on a person's knowledge and experience.

To improve credibility, important concepts were explained during the interviews, and simple definitions and examples were provided beforehand. A list of common cybersecurity terms, such as phishing and grooming, was included in the invitation email. It was also explained that terms like cybersecurity and digital security are broad concepts that include many different topics.

Credibility can also be affected by how participants choose to respond. For instance, participants may adapt their answers to align with what they perceive as socially desirable or expected. To address this, neutral and non-leading questions were used, and a comfortable interview setting was maintained to encourage open and honest responses. Also, while the participants received information about the interview topics beforehand, they did not receive the exact interview questions. This was done to avoid prepared answers.

Another potential challenge relates to participant fatigue during longer interviews, also known as "the maturation effect", which may lead to shorter or less detailed answers over time. To mitigate this, interviews were designed to last approximately 45 minutes. In the few cases where interviews lasted longer, the semi-structured format helped maintain participant engagement by allowing natural and conversational interactions.

Dependability concerns the consistency of the research process and whether the study could be repeated with similar results. In this study, dependability was strengthened by using a consistent interview guide and following established qualitative research procedures. The interview process was also carefully documented to ensure transparency in how data were collected and analyzed.

Confirmability refers to the extent to which the findings are shaped by the participants rather than researcher bias. In qualitative research, complete objectivity is not possible, but it is important to acknowledge and manage potential bias, as there is a risk that the researcher may consciously or unconsciously emphasize certain responses during analysis. To reduce this risk, the study followed established analytical procedures, and participants were given the opportunity to review interview summaries to confirm that their perspectives were accurately represented. This process, often referred to as member checking, helps ensure that interpretations remain grounded in the data.

Limited data saturation can also affect confirmability, as a small number of participants may restrict the range of perspectives captured. In this study, efforts were made to try and recruit approximately 10 participants. While this number was considered sufficient for identifying common patterns and themes, it may still limit the depth and variation of the findings. However, since this study was conducted within a limited timeframe, this number of participants was considered reasonable and manageable for the scope of the research.

Transferability refers to the extent to which the findings can be applied to other contexts. In qualitative research, generalization is not the primary goal; instead, the aim is to provide sufficiently rich descriptions so that readers can determine whether the findings are applicable to other settings. To support transferability, the study context and participant characteristics were clearly described, including participants' main teaching areas and professional backgrounds.

A related concern is ensuring that participants belong to the intended target group and have relevant experience. If participants lack appropriate background knowledge, the relevance of the findings may be reduced. To address this, recruitment was carefully managed. Invitations were sent to school principals with instructions to only forward them to teachers they knew or believed had relevant knowledge or experience of the topic in their teaching. Additionally, only preconfirmed participants were included. This approach helped ensure that the data collected was relevant to the study's purpose and context.

4.6 Data Collection

A total of 20 lower secondary schools within the Skaraborg region were contacted and asked to participate in the study. Initial contact was made via email to the principal(s) at each school, followed in several cases by additional emails and telephone calls. Responses were received from all 20 schools, although not all forwarded the request to teachers. This process resulted in eight teachers from seven different schools participating in the interview study. Two of the participating teachers worked at the same school but represented different subjects and teaching approaches.

All interviews were conducted via Microsoft Teams, allowing participants to take part from a location they considered comfortable and convenient. In accordance with the guidelines of the Swedish Ethical Review Authority, each teacher received an individual email prior to the interviews outlining the purpose of the study, the nature of the data collection, how the information would be used, that the interview would be audio-recorded and transcribed, and their rights as participants. This information was also reiterated at the beginning of each interview. An English-translated version of the information email is provided in Appendix B.

All participants orally provided informed consent to participate in the interviews and agreed to have the sessions recorded and transcribed using Microsoft Teams' integrated recording and transcription features (All participating teachers were already familiar with Microsoft Teams and the Office 365 suite through their work at their respective schools). Following each interview, the transcripts were carefully reviewed and manually corrected to ensure accuracy. The revised transcripts were then sent to the respective participants for verification and approval.

Table 6 provides an overview of the teachers who participated in the interview study. To preserve participant anonymity, only the teachers' primary teaching subjects are presented, as these are considered relevant for understanding and contextualizing the interview results. The participants consisted of three women and five men and represented schools in both rural and urban areas.

Table 6
Interview Participants

Teacher ID	Teaching subjects	Interview date	Duration (minutes)
T#1	Social Studies, History, and Geography	2026-03-24	46
T#2	Art and Spanish	2026-03-25	60
T#3	Science, Mathematics, and Technology	2026-04-08	53
T#4	English and German	2026-04-09	47
T#5	Social Studies, also acting as Computer/IT Lead	2026-04-16	38
T#6	Art and Librarian	2026-04-20	48
T#7	Science, Mathematics, and Technology	2026-04-20	38
T#8	Science, Mathematics, Technology, and Physics	2026-04-21	49

4.7 Interview Coding Process

As with the literature review, the interview material was analyzed using thematic analysis to identify recurring patterns in how cybersecurity-related education is implemented in schools. The analysis began with repeated readings of the interview transcripts to become familiar with the material and identify meaningful excerpts connected to the study's research focus. These excerpts were then assigned initial codes based on the teachers' descriptions.

The coding process combined deductive and inductive elements. The five literature-derived themes provided the broader areas for the analysis, reflecting the structure already established through the interview guide. Initial codes were then developed inductively from the teachers' descriptions within and across these broader areas and were progressively grouped based on similarities and recurring patterns in the interview material. This allowed more specific patterns, perspectives, and subthemes to emerge from the teachers' accounts and made it possible to examine how the broader areas identified in previous research were expressed, developed, and contextualized in the teachers' own accounts.

Table 7 presents an example illustrating how interview excerpts, initial codes, and thematic development contributed to the final theme. As the table serves as an illustrative example of the analytical process, not all relevant excerpts are included. The same applies to the analysis presented in the results chapter, where only selected quotations are reported. As the interviews were conducted in Swedish, all participant quotations were translated into English for presentation in this thesis.

Table 7
Example of the Thematic Analysis Process

Delivery of education			
Material →	Initial codes →	Theme development →	Final subtheme
"...not very clearly written into all subjects..." (T#3) "...we do not have a clear plan..." (T#7) "...gets integrated into other parts..." (T#5)	Weak curriculum integration; decentralized implementation; lack of planning	Fragmented but integrated cybersecurity education	Integrated but Decentralized Cybersecurity Education
"...comes up in biology and sex education..." (T#8) "...connected to source criticism..." (T#5) "...discuss AI-generated images..." (T#2)	Subject-integrated teaching; cross-curricular implementation; embedded instruction	Cybersecurity integrated through existing subjects	Integrated but Decentralized Cybersecurity Education

5. Results

This chapter presents the findings of the interview study. As mentioned previously, the interview questions were designed based on the five themes identified through the literature review. These themes serve as the main sections of the chapter, with additional subthemes emerging from the thematic analysis of the interview material itself. The purpose of this structure was to build on areas already identified in previous research while allowing more specific patterns, perspectives, and subthemes to emerge from the interview material. This also made it possible to consider points of connection with previous international research while maintaining the exploratory focus of the interview study. This proved to be an effective approach, as teachers' responses often extended beyond the broader thematic areas and revealed additional nuances, variations, and contradictions

Table 8 provides an overview of the main headings, including both the previously established themes and the new subthemes identified during the interviews. The overview is intended to help the reader navigate the results, while the subtheme titles also help provide a concise indication of the main findings presented in each section.

Table 8
Thematic Coding Results

Original overarching themes		**New inductively developed subthemes**
Delivery of Education	⇨	Integrated but Decentralized Cybersecurity Education
		Student-Active and Situational Teaching Practices
		Focus on Social and Ethical Dimensions of Cybersecurity
Teaching resources and teaching methods	⇨	Fragmented and Teacher-Driven Resource Practice
		Digital and Audiovisual Resources as Central Teaching Tools
		Discussion-Based and Student-Active Teaching Forms
Teachers' knowledge, confidence and professional development	⇨	Varied but Uneven Teacher Confidence and Competence
		Limited and General Professional Development Opportunities
		Collegial Support and Informal Knowledge Sharing
Governance, curriculum and organizational frameworks	⇨	Broad but Ambiguous Curriculum and Policy Connections
		Decentralized Organization and Uneven School Structures
		Organizational Priorities and Shared Responsibility
Teacher's overarching role and Ideal Pedagogical Approaches	⇨	The Teacher as a Guiding and Trustworthy Adult
		Ideal Teaching as Concrete, Interactive, and Connected to Students' Reality
		Short, Recurring, and Continuous Teaching Rather Than Isolated Events

The findings from the interviews are presented thematically in the following sections. Each section addresses one of the five overarching themes previously identified through the systematic literature review, while the inductively developed subthemes are presented within each section. Longer interview excerpts are presented as indented block quotations without quotation marks to visually distinguish participants' accounts from the surrounding analysis. Shorter quotations are incorporated with quotation marks directly into the text.

5.1 Delivery of Education

Integrated but Decentralized Cybersecurity Education

The thematic analysis indicated that cybersecurity-related education to a limited extent was present across all schools participating in the study, although it was rarely organized as a separate or clearly structured subject area. Several teachers initially described the teaching as loosely organized or dependent on individual initiative. However, a closer reading of the interviews revealed that cybersecurity-related topics were discussed across different subjects and teaching situations. Rather than being absent, the teaching appeared to be integrated sporadically into broader educational practices connected to source criticism, online behavior, grooming, misinformation, AI-generated content, and digital responsibility.

Teachers also reported considerable differences in how such teaching was delivered. Some referred to recurring discussions and activities, whereas others described the area as more occasional or dependent on current events. T#7 stated that “we don’t really have a clear plan for this,” while T#3 characterized the content as “not very clearly written into all subjects.” These descriptions indicate that cybersecurity-related education often lacks a clearly articulated progression and a shared structure across subjects and schools.

Even so, the interviews contained several examples of how cybersecurity-related topics and issues were integrated into everyday classroom teaching. Social studies, art, science, and mentor sessions all emerged in the interviews as recurring contexts for these discussions. cybersecurity-related discussions also arose naturally in connection with current events, as T#1 illustrated:

> I often show news to my students, and then topics connected to digital security come up. For example, if card payments or digital systems in Sweden stop working due to cyberattacks. Then we start discussing: what do you do in that situation? How should you think? Can you protect yourself from it?

Similarly, all teachers interviewed frequently cited areas of source criticism as one of the main entry points for cybersecurity-related education. Rather than focusing only on academic credibility, teaching source criticism nowadays has expanded to cover areas such as disinformation, manipulated media, propaganda, and online influence. T#3 articulated this approach in a simple but recurring way: “I usually tell them to double-check everything. Just because something looks real online doesn’t mean that it actually is.” T#2 also outlined how questions about manipulated and AI-generated material as regularly included in teaching activities:

> We usually let students look at pictures and try to figure out whether they are AI-generated or not. Then we discuss why it can be difficult to tell and what consequences that can have." In these interview accounts, cybersecurity-related education becomes closely connected to broader discussions about digital information, trust, and media awareness.

Student-Active and Situational Teaching Practices

The interviews also portrayed teaching as frequently grounded in practical examples and situations familiar to students from their own digital environments. Several teachers reported using online content, news events, or situations connected to students' social media use to make cybersecurity-related issues more concrete and relevant. For example, T#3 explained that his students sometimes work directly with manipulated content themselves: "The students get to create edited videos themselves, just to understand how easy it actually is to manipulate things online."

These accounts highlight how teachers seek to make cybersecurity-related issues tangible by engaging students in discussions and practical activities related to digital risks and manipulation, rather than simply having them receive information passively.

The interviews also showed that many cybersecurity-related discussions often emerge in response to ongoing events or situations involving students. Several teachers characterized the teaching as situational and reactive. T#5 explained: "It becomes situation based. When something comes up, then we talk about it." T#4 similarly outlined how discussions often begin after something has happened online or among students: "Usually, it's when something has happened that we start discussing it." T#2 also noted that incidents connected to bullying, online exposure, or current news events often lead to immediate classroom discussions:

> If something happens in the news, then we usually say: okay, we need to bring this up with the students. Or if something has happened connected to online bullying or exposure, then it becomes urgent.

These accounts portray cybersecurity-related education as something that often develops responsively in response to students' digital experiences and current events rather than through predetermined lesson structures.

Another emphasized aspect was that teaching often becomes situated within specific organizational contexts, such as theme days, mentor sessions, and external initiatives. Several teachers described how, for example, visits from the police often address issues such as cyberbullying, grooming, and fraud. At the same time, these initiatives were often described as sporadic or disconnected from continuous classroom teaching. T#5 referred to them as "isolated interventions," while T#1 questioned their broader "impact." This frames such initiatives as supplementary rather than fully integrated parts of everyday educational practice.

Focus on Social and Ethical Dimensions of Cybersecurity

Another recurring pattern in the material was that cybersecurity-related education primarily is focused on the social, behavioral, and ethical dimensions of digital life. Topics such as cyberbullying, grooming, phishing, misinformation, scams, online manipulation, and sharing personal information appeared repeatedly across the interviews. These issues are often connected to broader discussions about responsibility, relationships, trust, and online behavior rather than purely technical cybersecurity skills.

In contrast, technical aspects of cybersecurity appeared less prominent across the interviews, although they were not entirely absent. T#7, along with some other teachers, address topics such as passwords, firewalls, and basic security awareness. T#7 also stood out by allowing students to troubleshoot their computers for malware as part of the science class coursework:

> We also cover basic cybersecurity practices such as firewalls and antivirus software. One simple activity involves students scanning their own computers to identify potential threats. If any threats are detected, we further discuss when the malware was installed or when the devices became infected.

Several teachers also described grooming and online exploitation as topics commonly addressed during sex and relationship education in science classes. These discussions are framed around social media use, online contact with strangers, and risks connected to sharing information or images online. T#4, for example, outlined how students are encouraged to reflect on who they interact with online, and the risks connected to false identities on social media and gaming platforms:

> You might meet someone through a game or social media where there is a profile picture [...] and then believe that it is a fifteen-year-old 'Alex', when in reality it's an imposter. So we emphasize that students must be extremely cautious.

Similarly, T#5 explained how discussions about online behavior and responsibility often emerge when incidents involving social media occur among students:

> We often discuss fictional examples: Someone writes something on TikTok and another student shares it further. Then we discuss what they have actually done, who is responsible, and what is okay or not okay to say and do online.

T#8 also discussed how conversations surrounding social media increasingly center on topics related to echo chambers, filter bubbles, and algorithmic influence. The teacher explained how students are encouraged to reflect on how personalized content flows may shape their perceptions and understanding of information online:

> I usually talk about how everyone has their own 'bubble'. My phone might be full of astronomy videos, while their feeds contain completely different things, such as Eurovision or other interests. It can be difficult to get out of such a bubble or even realize that you are in one. A recent good example of

> this was when some of my students started looking into flat-earthers and similar things. Gradually, they began receiving more and more of that type of content, to the point that they actually started to believe in it. Eventually, they even started getting videos questioning the moon landing. So, I felt I had to step in and encourage them to actively seek information from other sources as well, to step outside their own bubble sometimes.

These accounts suggest that teachers do not necessarily separate cybersecurity from broader forms of social and ethical education related to digital environments. Instead, cybersecurity-related topics are often discussed in relation to social media use, online relationships, misinformation, algorithmic influence, and students' evaluation of information, communication, and self-protection within digital environments.

Taken together, the interviews describe cybersecurity-related education primarily delivered through integrated subject teaching, student-active discussions, and situational classroom activities. Rather than being presented as a separate or highly technical subject area, cybersecurity-related topics often appear embedded within broader discussions about social media, online behavior, digital ethics, misinformation, and responsibility in digital environments.

5.2 Teaching Resources and Teaching Methods

Fragmented and Teacher-Driven Resource Practice

The thematic analysis illustrates how teaching resources connected to cybersecurity are described as decentralized and heavily dependent on individual teachers. Across the interviews, few teachers referred to shared or standardized teaching materials. Instead, resources were described as selected, adapted, or created locally, depending on the subject context, teacher interest, and available time.

The lack of common teaching materials emerged as a recurring concern in teachers' accounts of current practice. T#3 explained that there is no "finished material that everyone works from", while T#4 stated that teachers often need to "find things and create" material themselves. Similarly, T#5 described how resources are frequently "pieced together" from different sources rather than taken from a structured framework.

The interviews also portray teachers as acting not only as educators but also as selectors, adapters, and creators of teaching materials. T#8 stated that he often creates "my own material too, mostly videos", while T#6 described creating realistic AI-generated images that students then analyze to determine whether they are authentic or manipulated. Several other teachers similarly reported collecting examples from online platforms, current news events, or social media. Taken together, these accounts suggest that teaching resources are often selected, adapted, and developed locally by individual teachers rather than drawn from shared structures. However, teachers also characterized this decentralized approach as providing flexibility, allowing them to adapt materials to current digital trends, subject-specific contexts, and students' everyday experiences.

As mentioned previously, all participating schools had, at some point between 2019 and 2025, ordered educational materials from the Swedish Federation of

Young Scientists. However, while some teachers were familiar with the organization itself, none of the interviewed teachers appeared aware of the specific resources or that such material had been ordered by their schools. These accounts indicate that externally provided resources do not necessarily become integrated into or widely circulated within everyday school practice.

Digital and Audiovisual Resources as Central Teaching Tools

Digital and audiovisual resources were featured prominently in teachers' accounts of cybersecurity-related teaching. Several teachers mentioned resources such as SVT Play, UR Play (both part of Swedish Televisions web services), and YouTube as recurring sources of material. T#3, T#5, and T#6 reported using SVT or UR content because they provide concrete and accessible examples related to digital issues and online behavior. Similarly, the Swedish Internet Foundation was mentioned by T#5 as a useful source of material on source criticism, misinformation, and digital awareness.

Visual and audiovisual resources appeared especially prominent in the interviews. Teachers repeatedly reported using videos, images, short clips, and online examples rather than relying primarily on traditional textbook material. T#7 explained that films can function as support when one is "not personally competent in every single part," highlighting how external resources may also be used to support the teaching of complex or unfamiliar topics.

Several teachers also described using material connected to students' everyday online environments. T#2 explained that examples are often taken from "the digital reality that anyone can encounter," including social media content, online videos, and AI-generated material. T#2 also outlined a classroom activity where students first watch an AI-generated video and then discuss whether it is authentic or manipulated: "First, they get to watch a video that is AI-generated, but not in an obvious way. Then they sit in groups and discuss whether it is fake or not."

Similarly, several teachers described using manipulated images, online examples, and digitally altered content in classroom discussions. Taken together, the teachers' accounts suggest that digital and audiovisual resources are often selected because they are current, recognizable, and closely connected to students' everyday online experiences. These resources also appear to function as important tools for making cybersecurity-related issues more concrete and understandable.

Discussion-Based and Student-Active Teaching Forms

Across the interviews, cybersecurity-related teaching was commonly described as discussion-based and student-active. Rather than emphasizing lectures, formal testing, or individual written assignments, teachers frequently emphasized activities centered on dialogue, reflection, and collaborative analysis.

Group discussions were frequently highlighted in teachers' accounts of cybersecurity-related teaching. T#1 explained that students are encouraged to "reflect together with each other," while T#6 described presenting examples and then allowing students to discuss them together. T#7 and T#8 similarly described discussion as a central part of their teaching practice. T#8 explains:

> I have a fairly good example. I show a video about a girl being groomed into sending pictures online (which I suppose could also be classified as a form of phishing and social engineering). After the students watch the video, they discuss the different stages of the process, such as when the grooming could have been recognized, what warning signs were present, and what methods the groomer used. The purpose is not to blame the victim in any way, but to help students reflect on how similar situations can be identified and potentially avoided.

These accounts suggest that cybersecurity-related education is often organized around shared reflection and discussion rather than fixed answers or memorization. This emphasis on dialogue is further reflected in teachers' descriptions of interactive and participatory activities. For example, T#7 explained the use of "four-corner exercises," in which students physically position themselves in different parts of the classroom based on their opinions or responses. T#8 similarly described working with text comparisons where students get to analyze different sources, assess credibility, and reflect on underlying agendas.

Another aspect that emerged from the interviews was the relatively limited role of formal assessment in relation to these activities. T#6 explained that written tests are rarely used and that the focus instead tends to be placed on discussion and reflection. Other teachers similarly described the area as exploratory and conversation-oriented, rather than strongly connected to grading or standardized assessment practices.

Taken together, the findings indicate that cybersecurity-related teaching is centered on dialogue, participation, and collaborative reflection. While teachers' activities vary, students are commonly portrayed as engaging with digital issues through discussion, interpretation, and evaluation rather than through formal testing practices.

5.3 Teachers' Knowledge, Confidence and Professional Development

Diverse but Uneven Teacher Confidence and Competence

The thematic analysis illustrates how teachers describe their knowledge and confidence regarding cybersecurity-related education in different ways. While several teachers described themselves as fairly confident in discussing certain aspects of digital safety, the interviews also presented differing accounts of competence, prior experience, and comfort with the topic. Rather than describing a shared or standardized competence base, the interviews suggest that teachers often relate their knowledge in the area to personal interest and individual experience.

Several teachers described their competence as relatively good, although often with some hesitation or limitations. For example, T#1 characterized his own competence as "relatively good," but also emphasized that it "varies greatly at the school" between teachers. Similarly, T#5 described feeling "fairly confident," while T#8 stated that they are "probably at a higher level than many other teachers" regarding digital issues. T#3 instead characterized himself more simply as

“average.” Taken together, these accounts suggest a shared sense of having at least a basic understanding of cybersecurity-related issues, although confidence and experience vary among individuals.

Across the interviews, teachers often distinguished between social and technical aspects of cybersecurity. Topics such as online behavior, source criticism, grooming, misinformation, passwords, and digital responsibility were frequently discussed as familiar and comparatively easier to address in teaching. T#1 stated: “I feel fairly comfortable talking about the general parts: how you should behave online, passwords, what to think about when using the internet.” Similarly, T#4 noted that they felt most comfortable with “the social parts” of digital safety, like identifying fake profiles and discussing cyberbullying. Several teachers also connected these topics to their everyday teaching practice and regular conversations with students.

In contrast, technical aspects of cybersecurity were often discussed as more difficult or unfamiliar. T#4 openly described themselves as “quite bad at the technical stuff,” while T#1 noted that he would struggle to teach “more advanced programming.” Similarly, although T#7 educated students about malware identification and related aspects, described difficulties explaining more technical concepts, such as encryption, in a pedagogical way.

Another aspect that emerged from the interviews was how teachers portrayed cybersecurity-related issues as difficult to keep up with due to the rapid pace of technological change. T#3 noted that “a lot is happening in the digital world [...] very quickly,” while T#8 characterized AI development as making it “very difficult to teach” because things constantly change. T#6 similarly explained that even recently learned knowledge can quickly become outdated.

At the same time, several teachers linked their confidence to prior work experience or personal interests outside regular teaching. Several teachers identified technology as a personal interest and related it to their engagement with cybersecurity-related issues. T#2 also noted that previous work has included security training about phishing and digital risks, which contributes to feeling “quite confident” in her understanding of the area. However, she emphasized that good educational material is still preferable for teaching longer sessions on the topic:

> Standing and talking about cybersecurity-related topics for hours with the resources available... I am more doubtful about that. But if there are good resources and ready-made educational materials available to support the teaching, then I’m absolutely open to bringing it up and discussing it with the students!

Taken together, the interviews illustrate how teachers describe their confidence and competence regarding cybersecurity-related education in different ways. While teachers often describe themselves as comfortable discussing social, ethical, and behavioral aspects of digital safety, technical areas are more commonly described as difficult. The accounts also show how teachers relate their confidence to previous experiences, personal interests, access to educational materials, and their own engagement with digital technologies.

Limited and General Professional Development Opportunities

Another theme that emerged from the interviews concerned teachers' opportunities for professional development and competence training within cybersecurity-related areas. Across the interviews, current professional development was often described as limited, general, and rarely focused specifically on cybersecurity or digital safety. Rather than describing structured, subject-specific training linked to cybersecurity-related teaching, teachers frequently referred to shorter and broader educational activities.

T#1 explained that professional development today mainly consists of "more general lectures" that are not always directly relevant for all teachers. Similarly, T#8 noted that most study days focus more on general pedagogy than on IT or cybersecurity-related questions. T#7 also expressed frustration about the lack of structured education within the field: "There really isn't any training in this area."

Several teachers also characterized the available training as brief and surface-level. T#1 explained that staff regularly receive short digital "micro-trainings" through email, often connected to phishing, password management, or digital safety. These activities are described as taking "a couple of minutes" and usually consist of short texts, videos, and a few follow-up questions. T#4 described similar activities as: "Micro trainings [...] three to five minutes long." T#6 and T#8 also reported similar activities. Although these initiatives were generally described positively, the accounts also portrayed them as primarily focused on staff routines and organizational safety. T#1 explained that much of the training concerns how employees should behave online as staff members, for example regarding GDPR, passwords, or suspicious links, rather than if and how teachers should teach these issues to students.

The teachers also described opportunities to deepen their knowledge within the area as limited. T#2 stated: "I actually don't think there is very much being offered right now." The same teacher added that resources certainly exist online, but that teachers largely need to "look for it themselves." Similarly, T#3 explained that development opportunities are available but mostly require individual initiative rather than being actively organized or pushed by school leadership. T#5 also characterized cybersecurity as: "Not really a prioritized area."

The interviews suggest that responsibility for competence development is often described as resting with the individual rather than the organization. Personal interest is frequently discussed as an important factor in whether teachers continue to develop their knowledge within the field. T#2 emphasized: "If you are personally interested in the topic, then it becomes natural that you look for it."

One area that teachers frequently returned to, however, concerned AI-related education. The interviews suggest that AI is among the digital topics that schools have recently begun addressing more actively. While T#2 mentioned that teachers at their school have received "a walkthrough of AI a little bit," several others described how AI-related discussions increasingly appear during study days or collegial meetings. However, these activities are generally focused on AI as a teaching tool or broader educational phenomenon rather than on cybersecurity specifically. Even so, several teachers described how the rapid growth of AI in recent years has expanded discussions around source criticism to include issues

more closely connected to cybersecurity, such as manipulated media, misinformation, and digital trust.

What emerges from the interviews is a description of professional development related to cybersecurity education as limited, broad, and insufficiently structured. While schools provide initiatives such as micro-trainings, AI introductions, and general digital awareness activities, teachers frequently discuss competence development as dependent on individual motivation and self-directed learning rather than on systematic organizational support directed toward teachers themselves.

Collegial Support and Informal Knowledge Sharing

Partly reflecting the previous theme, another theme that emerged from the interviews concerned collegial support and informal knowledge sharing within schools. Several teachers described how knowledge related to cybersecurity and digital issues is shared through everyday conversations and collaboration among colleagues rather than through formal organizational structures.

T#6 emphasized that colleagues are an important resource when new technologies or AI-related questions arise, and that teachers often discuss examples and share experiences with one another. Other teachers portrayed similar forms of collaboration. T#5 outlined how teachers within his work team try to build a shared "lesson bank" together, while several others mentioned exchanging examples of misinformation, manipulated images, or AI-generated material with colleagues before using them in class. These accounts illustrate how collegial exchange serves as an informal source of support and knowledge development in relation to cybersecurity-related issues.

The interviews also suggest that local engagement among teachers is frequently tied to whether and how cybersecurity-related issues are incorporated into teaching at all. T#1 characterized these questions as often driven by "individual teachers" or "enthusiasts" who personally find the topic important. T#2 similarly explained that some teachers are naturally more interested in digital technology, while others are "more technology-averse" and therefore engage less with these topics in their teaching.

Teachers often characterized collaboration as practical and experience-based rather than formally organized. They referred to discussing current digital trends together, helping each other solve technical problems, and exchanging ideas connected to AI, misinformation, and online behavior. These accounts suggest that competence development is often embedded in everyday school practice and in informal collaborations among colleagues.

Taken as a whole, the interviews portray collegial learning and informal support structures as important sources of knowledge sharing and professional support in relation to cybersecurity-related education. Rather than referring primarily to formal development structures, teachers often describe exchanging ideas, discussing new technologies, and building confidence through everyday collaboration with colleagues.

5.4 Governance, Curriculum and Organizational Frameworks

Broad but Ambiguous Curriculum and Policy Connections

The interviews suggest that cybersecurity education is often understood in relation to the school's broader mission and curriculum goals. However, this connection is frequently described as indirect and open to interpretation. Across the interviews, teachers noted that cybersecurity rarely appears as a clearly separated area within curriculum documents. Instead, the topic is often discussed in terms of broader concepts such as digital competence, source criticism, ethics, and democratic citizenship.

T#2 stated that the curriculum "quite clearly" states that schools should teach digital competence but also noted that cybersecurity itself is "embedded in other formulations" rather than explicitly spelled out. Similarly, T#4 described the wording in the curriculum as "quite vague," while T#1 characterized the connection between cybersecurity and the curriculum as "weak."

At the same time, several teachers (including the ones just mentioned) still connected these issues to broader aspects of the school's educational mission. T#5 linked the area to helping students become responsible societal citizens who can understand information, influence, and manipulation online. T#7 instead explained that the curriculum mainly approaches these issues through "ethics and morality." In contrast, T#8 connected the topic more strongly to source criticism, digital responsibility, and technical understanding, a view echoed in several other interviews.

The interviews also suggest that these different interpretations may partly be connected to teachers' subject backgrounds, as certain cybersecurity-related topics were described as fitting more naturally within some subjects than others. Across the interviews, the curriculum was often described as leaving considerable room for interpretation regarding both content and responsibility, something several teachers portrayed as problematic.

Several teachers therefore expressed a desire for clearer direction and stronger organizational steering, guidance, and support. T#2 emphasized that initiative needs to come "from higher up in the organization" if schools are to prioritize the area more consistently. T#1 similarly argued that schools would benefit from more explicit structures and clearer expectations for digital safety and cybersecurity-related education.

Together, these descriptions suggest that schools are given a broad mandate to work with digital competence and related cybersecurity issues, while the curriculum simultaneously leaves considerable room for interpretation regarding content, responsibility, and organizational direction.

Decentralized Organization and Uneven School Structures

Another recurring finding in the interview material concerns how cybersecurity-related education is organized within schools. Across the interviews, teachers often described the work as decentralized and unevenly structured, with organization frequently connected to local initiatives, individual teachers, or smaller work teams rather than broader school-wide systems.

Several teachers reported that there is no common structure connecting the work across subjects or year levels. T#3 stated that the area is "not organized," and "mostly only brought up when the ball bounces", while T#5 noted that there is no clear "common thread" throughout their school as a whole. T#7 similarly outlined how cybersecurity-related topics are often addressed only "when the opportunity appears." These accounts portray the area as frequently incorporated into existing teaching practices in informal and situational ways rather than through coordinated long-term planning.

However, the interviews also contained examples of smaller local structures through which teachers actively try to coordinate and organize the work themselves. T#5, T#6, and T#8 all described attempts to create greater coordination within their respective work teams. T#6 provided one of the clearest examples of this, describing how teachers in her workgroup try to implement different cybersecurity-related topics across several subjects:

> Among others, we have a Home and Consumer teacher who works with digital footprints, targeted advertising, cookies, and certain types of online scams. We also have a technology teacher who discusses AI, source criticism, and disinformation with his students. In addition to those two, we also have a teacher who covers topics such as cyberbullying and grooming as part of her social studies class. We also try to coordinate among ourselves how we work with these questions and how they should be addressed, especially so we don't repeat things another teacher has already covered.

These accounts portray smaller informal collaborations as one way of creating continuity and progression in the absence of larger organizational structures.

Overall, the findings indicate that cybersecurity-related education is largely decentralized and locally shaped. While the work appears informal and uneven, the findings also highlight smaller collaborative efforts through which teachers seek to coordinate content and create progression between subjects.

Organizational Priorities and Shared Responsibility

Another theme that emerged from the interviews concerns how cybersecurity-related education is prioritized within schools and how responsibility for the area is understood in relation to schools, homes, and other societal actors. Teachers frequently described the topic as important, while also highlighting how it competes with other educational priorities and practical constraints within everyday school life. T#4 also emphasized that while school leadership is generally positive toward teacher initiatives, the lack of time makes it difficult to continuously introduce new content into already established subjects: "You cannot just keep adding more. If we are going to add something new, then something else also needs to be removed. There simply isn't unlimited time."

Similarly, T#8 described cybersecurity-related issues as usually not highly prioritized "as long as nothing happens," and noted how attention to the area instead often increases following incidents or current societal discussions. T#8 continued:

> For example, we had a case involving grooming at the school, and it immediately became a big thing. The police were involved quickly, and everything

> was handled quite fast. So when something actually happens, both the police and school leadership prioritize it very highly. But the preventive work beforehand is not really prioritized in the same way and still depends a lot on individual teachers' own interest, competence, and time available.

Several teachers therefore expressed a need for more structured and long-term educational timeslot that focuses on digital competence and cybersecurity-related topics. A recurring idea in teachers' accounts concerned the possible reintroduction of a dedicated "computer literacy" subject, but in a modernized form adapted to today's digital society. Several teachers argued that such a subject should not only focus on technical computer skills, but also include broader topics such as misinformation, phishing, digital footprints, online behavior, and AI-generated content. T#7 characterized the idea as: "An upgraded version, which also includes more of the social aspects."

T#2 expressed a similar view and reflected on the earlier decision to remove the course in favor of spreading digital competence across different subjects: "At the same time as we introduced digital tools and one-to-one computers, we removed the dedicated time where students would actually learn about it."

The interviews therefore point to a perceived gap between the growing importance of digital technology in society and the amount of structured educational time currently dedicated to these questions within school.

Another aspect that emerges from the interviews concerns how responsibility for digital safety is sometimes understood as shared between multiple actors. T#8 especially emphasized that homes and parents carry an important responsibility regarding young people's digital behavior and social media use outside school: "I honestly think a large part of the responsibility lies with the home."

T#8 further noted that many digital situations begin long before students are technically old enough to use certain social media platforms, making it difficult for schools alone to manage the consequences. Similar reflections appeared elsewhere in the interviews, with several teachers mentioning that while it is important for students to learn about cybersecurity-related issues in school, external actors such as banks, national authorities, online platforms, and other organizations increasingly provide information and education about scams, fraud, and digital risks outside the school environment as well.

Taken as a whole, the interviews portray cybersecurity-related education as situated within broad curricular and organizational frameworks that leave considerable room for local interpretation and implementation. Teachers describe a combination of decentralized organization and competing educational priorities when discussing how cybersecurity-related issues are addressed within schools. Responsibility for digital safety is also often described as shared between schools, homes, and broader societal actors, a view that may further contribute to uncertainty about how much responsibility schools are expected to bear in this area.

5.5 Teachers' Overarching Role and Ideal Pedagogical Approaches

The Teacher as a Guiding and Trustworthy Adult

A recurring theme throughout the material concerned how teachers describe their own role in cybersecurity-related education. Across the interviews, teachers rarely described themselves as technical experts whose primary task is to deliver factual knowledge. Instead, the role was more often framed around guidance, discussion, trust, and helping students navigate everyday digital environments. T#6 especially emphasized the importance of teachers actively addressing these issues with students:

> If a teacher does not dare to raise questions about things like how students use ChatGPT or what they do online, then it becomes problematic. [...] If teachers avoid the subject, or do not dare to ask questions, then students are left without guidance.

The same teacher further argued that teachers may actually have a stronger influence than external lectures or temporary initiatives because students meet teachers continuously over time and build trust toward them: "The teacher has a very important role, even more than an external lecturer can have. The teacher is someone students meet continuously and build trust toward." Similarly, T#7 characterized the responsibility as naturally ending up with teachers: "We as teachers actually have a very important role. Because who else is going to teach them?"

T#2 also connected the role directly to the school's broader social and democratic mission:

> We have this social responsibility as teachers, to prepare students to become responsible citizens. That includes not going into debt online or giving away your personal information. Teaching basic manners today is just as much about the digital world as it is about behavior in real life. You cannot just ignore it and move on by saying that it is only the parents' responsibility. We as teachers will have to work from one direction, and the parents from another, for the students to grow up and eventually become good members of society.

Several teachers also characterized the role as highly connected to discussion and reflection rather than simply correcting students or delivering information. T#6 emphasized: "It is not only about communicating facts, but about asking questions and making students reflect: How did you think here? Why did you choose to trust this source?"

Similarly, T#8 stated that the teacher's role is fundamentally about helping students understand how to approach information online: "What is good data? What is bad data? What kind of data do you want to share yourself, and what kind of data should you avoid taking in?"

T#3 further argued that discussions become more meaningful when they are connected to situations students recognize from current events or everyday life: "You need to connect it to something relatively fresh in people's minds."

Multiple teachers also described their role as closely connected to creating a sense of safety and reducing anxiety when digital incidents or broader societal events affect students. Discussions about digital risks and online behavior are described as important for "spreading calm" and helping students process situations that might otherwise create uncertainty. T#3, for example, outlined a hypothetical scenario in which multiple students film a conflict at school and share the recordings online, unintentionally escalating the situation through social media circulation. In such cases, the teacher emphasized the importance of limiting further dissemination, discussing the potential consequences of sharing content online, and maintaining communication with parents:

> It becomes important to communicate clearly with guardians and show that this kind of behavior is not acceptable. It is about preventing further spread, reducing anxiety, and showing what consequences it can have.

Together, these descriptions suggest that teachers largely view their role as extending beyond technical instruction alone. Instead, the role becomes closely connected to guidance, trust, emotional support, and helping students navigate social and digital environments responsibly.

Ideal Teaching as Concrete, Interactive, and Connected to Students' Reality

Another recurring theme concerned how teachers described ideal cybersecurity-related instruction if they were able to design it themselves. Across the interviews, several teachers emphasized practical participation, concrete examples, and interactive classroom activities rather than traditional lecture-based teaching.

T#5 suggested that ideal teaching should begin with clear explanations of concepts before moving toward concrete and recognizable examples: "I like to work with concrete examples, preferably as current as possible, and preferably examples from their perspective, what they themselves encounter." Similarly, T#4 emphasized that students need to become actively involved in the lesson rather than simply listening passively: "They need to be engaged; they cannot just sit and listen."

Several teachers also characterized ideal lessons as strongly connected to practical experimentation and participation. T#3 repeatedly emphasized wanting students to "test things themselves" to understand better how quickly information spreads online: "I would gladly let students test things themselves a lot."

The teacher gave examples of wanting students to experiment with how images spread online, how algorithms reinforce negative content, and how digital material can remain online long after publication. T#8 similarly expressed an interest in students actively creating manipulated or misleading material themselves to understand digital influence better: "If a thirteen-year-old can create something that looks believable, then basically anyone can do it."

The same teacher also outlined exercises where students analyze AI-generated mistakes and identify false information presented by AI systems: "Their task was to figure out what was wrong; to identify what mistakes the AI had made."

T#2 outlined similar approaches where students first analyze whether AI-generated material is authentic before discussing why the content may have been created and what influence it could have on viewers. The teacher also explained that students later create manipulated material themselves as part of the same activity. These exercises illustrate how practical activities can be used to strengthen students' digital awareness and connect teaching to situations they may realistically encounter online.

Several teachers additionally emphasized that ideal teaching should remain closely connected to current societal developments, social media, AI, and situations students already encounter online in everyday life. Together, these descriptions suggest that teachers largely envision ideal cybersecurity-related education as practical, discussion-based, and connected to recognizable real-world situations rather than abstract technical instruction.

Short, Recurring, and Continuous Teaching rather than Isolated Lessons

A final recurring theme concerned how teachers described ideal cybersecurity-related education as something that should occur continuously over time rather than through isolated lectures or single thematic days. T#6 explained that the current situation, where students may only encounter these topics once per school year, is insufficient: "I would like to be able to do more of these smaller sessions during the school year, where each occasion focuses on a specific area."

The same teacher further explained that shorter recurring sessions would work better than longer lectures: "I do not believe in lessons that are too long within this area. Students become tired, and it is difficult to take everything in at once."

Similarly, T#2 outlined an ideal format inspired by the shorter "micro-trainings" used for municipal staff. The teacher suggested that students could instead work with shorter recurring activities connected to digital safety: "Maybe two or three minutes at a time, just to remind students about different aspects."

The teacher further suggested combining short films, quizzes, and discussions in smaller recurring moments throughout the school year: "Maybe show a short film followed by a quiz and then a short discussion around the specific topic."

T#1 expressed similar thoughts regarding continuity and long-term work: "I think it would be good to have a more recurring and structured way of working in order to educate and help students."

Together with several other teachers, T#1 also discussed the possible reintroduction of a modernized computer literacy subject as a way to create more structured and continuous cybersecurity-related teaching in the area.

Several teachers therefore describe ideal teaching less as isolated projects and more as smaller recurring discussions and activities integrated continuously throughout students' education. Together, these descriptions suggest that teachers view repetition, continuity, and gradual progression as important parts of meaningful cybersecurity-related education.

5.6 Thematic Analysis Summary

Overall, the resulting themes demonstrate considerable variation in teachers' experiences, confidence, resources, and approaches to cybersecurity-related education, while several common patterns also emerge across the material. Cybersecurity-related topics are generally integrated into existing subjects and teaching situations rather than treated as a distinct area, with teaching frequently centered on social, ethical, and information-related issues and connected to students' everyday digital experiences. Across the interviews, teachers commonly described the work as decentralized and dependent on individual initiative, while formal structures, shared resources, and professional development are perceived as limited. Despite these differences in current practices and conditions, the findings indicate a shared emphasis on practical, discussion-based, and continuous teaching, as well as on the teacher's role in guiding students toward safer and more responsible participation in digital environments.

6. Discussion

This chapter presents a discussion of the findings based on the interviews conducted. It begins with reflections on the study's main findings and methodological consideration, including the strengths and limitations of the chosen research approach. The chapter then explores similarities between the findings and themes identified in previous international research, focusing on recurring patterns and points of connection rather than direct comparisons. Furthermore, the ethical and societal aspects connected to the study are discussed. Finally, the chapter concludes with reflections on the overall research process and possible directions for future research.

6.1 Reflections on the Results and Methodological Considerations

The findings of this study suggest that cybersecurity-related topics are present in Swedish lower secondary schools to varying degrees, but rarely as a clearly defined or systematic subject area. Instead, these issues are often addressed through broader discussions concerning source criticism, social media, artificial intelligence, grooming, privacy, and online fraud. This observation is particularly interesting given that several teachers did not initially describe such activities as cybersecurity education, despite later discussing teaching practices that clearly related to cybersecurity-related themes. This may indicate that cybersecurity is often understood more narrowly than the broader range of issues that are addressed in practice. However, the broad definition of cybersecurity used in this study should also be considered when interpreting this finding. The presence of cybersecurity-related topics across the participating schools does not imply comprehensive or coordinated cybersecurity education, as the topics addressed varied between teachers and schools.

At the same time, the findings do not only highlight challenges and limitations. Despite limited resources, unclear guidelines, and varying levels of confidence in certain aspects of the subject, many teachers demonstrated clear engagement with these issues and a strong willingness to help students navigate digital environments in a safe and responsible manner. Several participants also provided reflective and nuanced descriptions of both digital risks and the pedagogical approaches they use to address them. Despite the absence of formal structures in many schools, several teachers also described informal collaboration with colleagues and local initiatives aimed at integrating cybersecurity-related topics into teaching. This suggests that teachers often seek practical ways to address these issues even when organizational support and formal guidance are limited.

One overall reflection arising from the study is that cybersecurity education appears to be less about teaching isolated technical concepts and more about supporting students' ability to navigate an increasingly complex digital society. Throughout the interviews, teachers often described cybersecurity-related education as closely connected to digital competence, critical thinking, and responsible participation in digital environments. Several participants also reflected on a perceived gap between students' everyday use of digital technologies and their

understanding of associated risks and consequences. Furthermore, the interviews revealed concerns regarding the rapid development of new technologies, particularly artificial intelligence, which challenge both existing teaching materials and teachers' ability to remain up to date. This may indicate that cybersecurity-related education is becoming increasingly intertwined with broader questions concerning digital literacy, information verification, and the ability to evaluate AI-generated content critically.

Before discussing the findings in relation to previous research, it is important to reflect on the study's methodological strengths and limitations that may have influenced the results and their interpretation. One of the key strengths of the chosen methodological approach was the use of semi-structured interviews. The nuanced nature of the findings illustrates how this format allowed participants to elaborate on their experiences and reasoning in ways that would likely not have emerged as clearly in a quantitative study. The interviews revealed, for example, that teachers' initial descriptions of cybersecurity education could be further developed through follow-up discussions, revealing practices and perspectives that may not have emerged through more structured forms of data collection. At the same time, the structure of the interview study itself needs to be considered when interpreting these findings.

A further methodological consideration concerns the role of the literature review in shaping the interview study. Since the interview guide was structured around the five themes identified in previous research, these themes inevitably influenced which broader areas were explored during the interviews. Some degree of thematic overlap between the literature review and the interview findings could therefore be expected. At the same time, the semi-structured format and inductive coding within and across these broader areas allowed participants to introduce additional perspectives, nuances, and patterns that were not predetermined by the literature-derived themes.

The flexibility of the semi-structured interviews introduces an additional methodological consideration. The use of follow-up questions allowed participants to expand upon issues they considered important, but it may also have influenced which topics received greater attention during the interviews. Furthermore, the interaction between researcher and participant inevitably forms part of the data collection process and may have affected how participants chose to describe their experiences. While this flexibility contributed to richer and more nuanced data, it may also have led to some variation across interviews.

There are also other limitations associated with the chosen method. Since the study relies on teachers' self-reported descriptions, it is not possible to determine the extent to which teaching is actually carried out as described. In addition, participants varied in terms of their professional roles, experience, and insight into school-wide practices. While some teachers discussed broader organizational perspectives, others primarily reflected on their own classroom teaching. As a result, descriptions of the same school or teaching practices may differ depending on the individual participant.

Another limitation concerns the size and composition of the sample. The study focuses exclusively on municipal lower secondary schools within the Skaraborg region and is based on eight interviews conducted across seven schools, out of a total of 20 dedicated municipal lower secondary schools in the region. This limits the extent to which the findings can be transferred to other contexts and makes

it more difficult to capture the full range of experiences and perspectives that may exist, even within the region itself. However, the purpose of the study was not to establish a broad statistical generalization, but rather to develop a deeper understanding of how teachers perceive and manage cybersecurity-related teaching in practice. Although the number of participants was limited, several recurring themes emerged across the interviews, which suggests that some of the identified experiences and challenges may extend across different school contexts. It should also be noted that while schools from both urban and rural areas were represented, no clear differences in the interview findings were identified between these contexts, as similar themes and experiences emerged across both urban and rural schools. However, the limited sample does not allow firm conclusions to be drawn in this regard. A more detailed discussion regarding the recruitment process and related challenges is presented in subsection 6.4, Reflections on the Research Process.

There is also a possibility that teachers who chose to participate already had a particular interest in digitalization or cybersecurity-related issues. This potential selection bias may have been reinforced by the recruitment process, since schools were asked to nominate teachers who were believed to have relevant experience within the study area. While this approach increased the likelihood of obtaining informed and detailed responses, it may also have resulted in participants with greater awareness of these issues than teachers more generally. This may have influenced the findings, resulting in a somewhat more positive view of the area than might have emerged from a completely random sample. At the same time, several clear challenges and uncertainties still emerged throughout the interviews despite this potential bias, which could suggest that the identified issues extend beyond the group of teachers who chose to participate.

6.2 Findings in Relation to Previous Research

Several aspects of the findings show clear similarities to previous research identified in the literature review. Rather than providing direct comparisons, this section considers recurring themes, differences, and points of connection between the interview findings and the broader research field.

A recurring finding was that cybersecurity-related education was often described as sporadic and reliant on individual teachers rather than on systematic planning. Similar patterns are reported by Ibrahim et al. (2024), Liu et al. (2025), and Saglam et al. (2023), who likewise describe cybersecurity-related topics as being addressed within existing subjects rather than taught as a distinct area of knowledge.

Similar descriptions of limited time and unclear guidelines are also evident in previous research. Several teachers in this study expressed uncertainty regarding what is actually expected to be taught within the area and how far their responsibilities extend in practice. The interviews also revealed a desire for clearer direction from higher levels of the education system, from both school leadership and national authorities, with several teachers calling for more concrete frameworks for prioritizing and integrating cybersecurity-related topics into teaching. This relates to the findings of Arishi et al. (2024) and Lorenz (2025), which identify unclear policy documents and a lack of national coordination as central barriers to implementing cybersecurity education. The findings therefore suggest

that clearer curricular guidance and organizational support may contribute to a more systematic and equitable integration of cybersecurity-related education across schools.

Another clear similarity concerns teachers' competence and confidence. Several participants described feeling relatively comfortable teaching social and everyday aspects of digital security, such as source criticism, social engineering, online privacy, and digital behavior, but less confident when discussing more technical topics, such as encryption and tracking technologies. This relates to the findings of Childers et al. (2022), Pencheva et al. (2020), and Hossain et al. (2024), who similarly report uncertainty about subject knowledge and teaching methods, particularly regarding more technical aspects of cybersecurity.

Related to this, competence development within the area was often described as limited and largely dependent on individual initiative rather than on structured organizational support. Similar challenges are discussed by Hossain et al. (2024), Mourning et al. (2023), and Liu et al. (2025), who emphasize the importance of sustained professional development to build teachers' confidence and competence in cybersecurity-related education. The rapid development of technologies such as artificial intelligence further reinforces this challenge, as several participants described difficulties in keeping teaching materials and subject knowledge up to date.

Beyond these similarities, the findings also add nuance to the existing research. While previous studies often focus on knowledge transfer and technical competencies, the teachers interviewed in this study rarely described themselves as technical experts. Instead, they frequently emphasized their role as trusted adults responsible for facilitating discussion, encouraging reflection, and helping students understand the consequences of their actions in digital environments. Throughout the interviews, cybersecurity was more often framed in terms of behavior, judgment, responsibility, and everyday digital practices than in terms of technical protection measures. This perspective aligns closely with ENISA's concept of Cybersecurity Culture, where cybersecurity extends beyond technical protection to include knowledge, attitudes, values, and everyday behavior (ENISA, 2017). The findings suggest that teachers can contribute to such a culture without positioning themselves as technical experts, instead supporting students' reflection, judgment, and responsible behavior in digital environments.

Another recurring observation was that teachers often described students as highly active and experienced users of digital technologies, yet simultaneously lacking awareness of digital risks, online influence, and manipulation. This observation resembles findings from the ICILS study and is consistent with the argument that extensive technology use does not necessarily translate into strong digital competence or cybersecurity awareness.

The findings also indicate a preference for practical and discussion-based teaching approaches grounded in real-world examples and students' own digital experiences over traditional lecture-based instruction. Similar pedagogical ideals are reflected in previous research on game-based, peer, and scenario-based learning (Videnovik et al., 2024; 2025; Renieri et al., 2025).

An important difference from some previous studies is that several teachers in this study expressed a degree of skepticism toward large-scale external initiatives or one-off awareness campaigns. Instead, they emphasized the value of brief but

recurring discussions and the continuous integration of cybersecurity-related topics into everyday teaching. This view is consistent with the findings of Saglam et al. (2023) and Prior and Ophoff (2024), who suggest that isolated educational interventions often have limited long-term effectiveness unless supported by ongoing reinforcement. The findings of the present study may therefore indicate that the continuous integration of cybersecurity-related topics into regular classroom practice is perceived as both more feasible and pedagogically sustainable than larger stand-alone initiatives.

The contribution of the present study therefore lies not only in identifying similarities with previous international research, but also in showing how these broader challenges are expressed within a Swedish municipal lower secondary school context. While limited to the participating teachers and schools in Skaraborg, the findings provide empirical insight into an educational context that remains comparatively underexplored.

6.3 Ethical and Societal Aspects

The findings of this study suggest that cybersecurity can no longer be understood solely as a technical specialty, but rather as an increasingly important societal issue connected to everyday life and participation in digital environments. Children and young people today grow up in a society where communication, information, entertainment, and social interaction largely take place online. As a result, issues related to privacy, manipulation, fraud, online influence, and AI-generated content have become part of their daily experiences.

Schools therefore play an important role in preparing students for participation in society. Just as schools have traditionally been responsible for developing literacy, democratic understanding, and critical source evaluation skills, the findings suggest that a basic understanding of digital security is becoming an increasingly important part of this mission. This becomes particularly evident when several teachers in the study described their students as experienced users of digital platforms while at the same time lacking sufficient understanding of digital risks, consequences, and how manipulation can occur in online environments.

At the same time, the findings indicate that opportunities to engage with cybersecurity-related topics may vary depending on local priorities, available resources, and individual teacher initiatives. From a societal perspective, this raises questions of educational equity, as students may receive different opportunities to develop cybersecurity awareness and digital safety skills depending on the school they attend.

Ethical considerations remained important throughout the research process. Participation was voluntary, informed consent was obtained, and participants were reminded that they could withdraw at any time without providing a reason. No participant chose to withdraw, and there were no indications that the interview questions caused discomfort or reluctance to share information. Since the interviews focused on professional experiences and teaching practices rather than personal matters, the ethical risks associated with participation were considered limited.

An additional ethical consideration concerned the purpose and presentation of the study. The intention was not to evaluate or criticize individual schools or teachers, but rather to explore how cybersecurity-related topics are addressed in classroom practice and to identify opportunities and challenges associated with teaching these subjects. Presenting the findings at a broader thematic level helped reduce the risk of identifying individual participants or schools while encouraging a constructive discussion of the issues raised.

These broader societal and educational implications also align with the perspective of the research field of Privacy, Information and Cyber Security (PICS), where cybersecurity is understood as something shaped not only by technology but also by human behavior, social interaction, and societal structures. This perspective was reflected throughout the interviews, where teachers rarely described cybersecurity as purely technical instruction. Instead, they emphasized discussion, reflection, trust, critical thinking, and responsible participation in digital environments.

Overall, the findings suggest that cybersecurity education is not only about protecting students from digital risks, but also about supporting the development of responsible and critically aware digital citizens. While the study does not provide definitive answers regarding how cybersecurity should be taught, it may contribute to future discussions among teachers, school leaders, policymakers, and researchers. As society becomes increasingly digitalized, cybersecurity competence is likely to become an increasingly important component of general education.

6.4 Reflections on the Research Process

The research process proved more demanding than initially expected, particularly regarding participant recruitment. Recruiting teachers required extensive follow-up communication with schools and resulted in fewer participants than originally anticipated.

Several external factors also influenced data collection. During the recruitment period, Swedish schools faced increased workloads due to last-minute changes in the administration of the national tests, in which planned digital examinations were replaced with paper-based ones. As a result, teachers were required to spend considerably more time on grading and administrative tasks, which several participants identified as a reason for their limited availability and reduced opportunities to participate in the study. This illustrates the practical challenges of conducting research in school environments, where teachers' workloads are often already high and where external factors can quickly affect opportunities for participation.

Once the interviews had been conducted, additional time-consuming stages followed, such as transcription, processing, and analysis of the material. Compiling the interviews, examining patterns across them, and considering the findings in relation to previous research required both precision and time. Time constraints have therefore been a clear challenge throughout the project, while the ambition has been to produce results that are both relevant and useful.

Overall, the research process highlighted both the practical challenges of conducting research in school environments and the importance of allowing sufficient time for recruitment, data collection, and qualitative analysis.

6.5 Future Work

Future research could benefit from conducting a similar study with a larger number of participants, as the present study is limited to eight interviews across seven schools. If a larger study is planned, recruiting participants earlier in the school year may increase the likelihood of obtaining a broader sample. A broader geographic scope could also help determine whether the patterns identified in this study are consistent across different regions of Sweden.

Since the study focuses exclusively on teachers' perspectives, future research could also include students, school leaders, and guardians. Including these groups could provide a more comprehensive understanding of how cybersecurity-related education is viewed, prioritized, and implemented in schools. Comparative studies may also identify similarities and differences between stakeholder groups.

Future research could also complement teachers' self-reported accounts with classroom observations. However, the fragmented and situational teaching identified in this study may be difficult to capture through conventional observations. Teacher diaries, classroom documentation, or longer-term observations could therefore provide a more systematic picture of how cybersecurity-related topics are addressed in practice.

Another possible direction would be to conduct a similar study in independent schools (friskolor). Comparing the findings with those from municipal schools could reveal differences in teaching practices, resources, and organizational support.

Longitudinal studies could further examine how cybersecurity education evolves over time, particularly in relation to the rapid development of artificial intelligence (AI) and changing digital habits among young people. Future political decisions and curriculum revisions may also influence how cybersecurity-related topics are addressed in Swedish schools. In addition, the continued implementation of the NIS2 directive could contribute to a broader societal and institutional focus on cybersecurity, potentially creating indirect effects on how cybersecurity-related issues are addressed within educational contexts. Future research could therefore investigate whether cybersecurity education becomes more structured and integrated into curricula and school governance, or whether it remains largely dependent on individual teachers' interests and initiatives.

Finally, intervention studies evaluating specific teaching materials or pedagogical approaches in Swedish schools could provide valuable insights into which methods are most effective for strengthening students' cybersecurity awareness and digital resilience.

7. Conclusion

The purpose of this study was to examine how cybersecurity-related education is practiced in Swedish municipal lower secondary schools and how teachers describe their instructional practices, resources, competence, and conditions for teaching the subject.

Regarding the first research question, the findings suggest that cybersecurity-related topics are present in all participating schools but rarely as a clearly defined or standalone subject area. Instead, topics such as source criticism, social media, privacy, misinformation, artificial intelligence, grooming, online fraud, and digital responsibility are integrated across different subjects. Teaching is often discussion-based, student-active, and connected to students' everyday digital experiences, although practices vary between schools and teachers.

Regarding the second research question, teachers described their instructional practices as largely shaped by individual initiative, locally selected resources, and professional judgment. While they generally felt comfortable addressing social and everyday aspects of digital safety, uncertainty was more common regarding technical topics. Limited time, unclear guidance, and restricted opportunities for professional development were also recurring challenges.

A notable observation was that several teachers initially described cybersecurity education as limited, yet later discussed classroom activities that clearly addressed cybersecurity-related issues. This suggests that cybersecurity may sometimes be understood more narrowly in educational practice than in research, making existing cybersecurity-related teaching less visible than it actually is. The central challenge therefore appears not to be the absence of cybersecurity-related education, but its fragmentation.

Given the limited qualitative sample, the interview findings should primarily be interpreted within the context of the participating teachers and schools. At the same time, recurring observations emerged across interviews, and similar patterns were identified in the international research included in the systematic literature review, suggesting that the issues identified may not be unique to the participating schools. Taken together, the results provide answers to both research questions within the scope of the study.

The findings point to several practical areas for improvement. Policymakers, municipalities, and school leaders could provide clearer guidance on responsibility, progression, and support for teachers. For teachers and schools, dedicated lessons or a more clearly defined subject area could provide greater structure and continuity, but an entirely new subject is not necessarily required. Existing practices involving discussion, current examples, source criticism, digital behavior, and students' everyday online experiences already provide useful starting points, particularly when addressed continuously rather than through isolated activities.

Cybersecurity education is not only about protecting students from digital risks, but also about preparing them to participate safely, responsibly, and critically in an increasingly digital society. The challenge moving forward may therefore not be how to introduce cybersecurity education, but how to make the education already taking place more systematic, continuous, and accessible to all students.

References

Amin, S., Petraki, E., El-Fiqi, H., & Abbass, H. (2024). Securing young minds: Analysing primary teachers' perspectives and practices in cyber safety. In *ACIS 2024 Proceedings* (Paper 93). AIS Electronic Library (AISeL). https://aisel.aisnet.org/acis2024/93

Arishi, A. A., Kamarudin, N. H., Bakar, K. A. A., Shukur, Z. B., & Hasan, M. K. (2024). Cybersecurity awareness in schools: A systematic review of practices, challenges, and target audiences. *International Journal of Advanced Computer Science and Applications, 15*(12), Article 49. https://doi.org/10.14569/IJACSA.2024.0151249

Ayyash, M., Alsboui, T., Alshaikh, O., Inuwa-Dutse, I., Khan, S., & Parkinson, S. (2024). Cybersecurity education and awareness among parents and teachers: A survey of Bahrain. *IEEE Access, 12*, 87713–87730. https://doi.org/10.1109/ACCESS.2024.3416045

Brifelt, L., & Karlsson, A. (2023). *Nulägesanalys om gymnasieelevers kunskap och förhållningssätt kring IT-säkerhet och hur lärare undervisar inom ämnet* [Analysis of the current situation regarding high school students' knowledge and attitudes towards IT security, as well as how teachers are teaching the subject] [Bachelor's thesis, University of Skövde]. DiVA. https://his.diva-portal.org/smash/record.jsf?pid=diva2%3A1778406

Cawthorne, B. (2025, February 11). *Almost half of 8 to 17-year-olds have been scammed online*. UK Safer Internet Centre. https://saferinternet.org.uk/blog/almost-half-of-8-to-17-year-olds-have-been-scammed-online

Childers, G., Linsky, C. L., Payne, B., Byers, J., & Baker, D. (2023). K-12 educators' self-confidence in designing and implementing cybersecurity lessons. *Computers and Education Open, 4*, 100119. https://doi.org/10.1016/j.caeo.2022.100119

Cisco. (n.d.-a). *What is cybersecurity?* Retrieved February 15, 2026, from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Cisco. (n.d.-b). *What is IT security? Information technology security*. Retrieved February 15, 2026, from https://www.cisco.com/c/en/us/products/security/what-is-it-security.html

Cybersecurity Academy. (2025). *Lärarhandledningar i IT-säkerhet genom hela grundskolan*. Retrieved December 29, 2025, from https://cybersecurityacademy.se/skola/lararhandledningar/

Erukulla, T. (2026, March 31). *What cybersecurity can learn from the adolescent brain*. Identity Defined Security Alliance. https://www.idsalliance.org/blog/what-cybersecurity-can-learn-from-the-adolescent-brain/

European Court of Auditors. (2022). *Cybersecurity of EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats* (Special Report 05/2022). https://doi.org/10.2865/294640

European Union Agency for Network and Information Security. (2017). *Cyber security culture in organisations*. https://doi.org/10.2824/10543

Feldner, D. (2025, March 3). *Scopus data crosses the 100 million item threshold!* Scopus Blog. https://blog.scopus.com/100-million-reasons-to-trust-scopus

Funck, E. K., & Karlsson, T. S. (2021). *Handbok för systematiska litteratur- och dokumentstudier inom samhällsvetenskapen* (Förvaltningshögskolans rapporter, nr 158). Förvaltningshögskolan, Göteborgs universitet. https://gupea.ub.gu.se/handle/2077/67445

Graff, G., & Birkenstein, C. (2018). *They say / I say: The moves that matter in academic writing with readings* (4th ed.). W. W. Norton & Company.

Higson-Smith, C. (2000). *Writing your research proposal: A workbook for first-time and inexperienced researchers in the social sciences and humanities* (J. Parle, L. Lange, & A. Tothill, Contributors). National Research Foundation.

Hossain, G., Shin, M., & Afrose, M. (2024). Empowering K-12 STEM educators: Enhancing cybersecurity awareness through professional development. In *2024 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 1–5). IEEE. https://doi.org/10.1109/ICCE59016.2024.10444288

Ibrahim, A., McKee, M., Sikos, L. F., & Johnson, N. F. (2024). A systematic review of K-12 cybersecurity education around the world. *IEEE Access, 12*, 59726–59738. https://doi.org/10.1109/ACCESS.2024.3393425

Internetstiftelsen. (n.d.). *About the Swedish Internet Foundation*. https://internetstiftelsen.se/en/

Internetstiftelsen. (2024). *Barnen och internet 2024 – skärmtid*. https://svenskarnaochinternet.se/rapporter/barnen-och-internet-2024/skarmtid

Internetstiftelsen. (2025a). *Internetstiftelsens remissvar på betänkandet Kunskap för alla – nya läroplaner med fokus på undervisning och lärande (SOU 2025:19)*. https://internetstiftelsen.se/app/uploads/2025/06/internetstiftelsens-remissvar-sou-2025-19-.pdf

Internetstiftelsen. (2025b). *The Swedes and the Internet 2025*. https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2025/english/

Jerman Blažič, B., & Jerman Blažič, A. (2022). Cybersecurity skills among European high-school students: A new approach in the design of sustainable educational development in cybersecurity. *Sustainability, 14*(8), 4763. https://doi.org/10.3390/su14084763

Lamond, M., Prior, S., Renaud, K., & Wood, L. A. (2025). Teachers' perspectives and practice of cybersecurity education in primary schools. *Discover Education, 4*, Article 312. https://doi.org/10.1007/s44217-025-00471-0

Liu, N., Long, S., & Martin, F. (2025). Systematic review of elementary cybersecurity education: Curriculum, pedagogy, and barriers. *Journal of Cybersecurity Education, Research and Practice, 2025*(1), Article 21. https://doi.org/10.62915/2472-2707.1265

Lorenz, B. (2025). Improving cybersecurity education in schools: An assessment of the "Digitally Safer School" proposal. In B. K. Smith & M. Borge (Eds.), *Learning and collaboration technologies: HCII 2025* (Lecture Notes in Computer Science, Vol. 15806, pp. 315–327). Springer. https://doi.org/10.1007/978-3-031-93564-0_19

Lorenz, B., & Kikkas, K. (2020). "Trust me, you will need it": Cybersecurity as extracurricular subject at Estonian schools. In A. Moallem (Ed.), *HCI for cybersecurity, privacy and trust: HCII 2020* (Lecture Notes in Computer Science, Vol. 12210, pp. 175–188). Springer. https://doi.org/10.1007/978-3-030-50309-3_12

Martin, F., Bacak, J., Polly, D., Wang, W., & Ahlgrim-Delzell, L. (2022). Teacher and school concerns and actions on elementary school children digital safety. *TechTrends, 67*(3), 561–571. https://doi.org/10.1007/s11528-022-00803-z

McLeod, J., Zhang-Kennedy, L., & Stobert, E. (2024). Comparing teacher and creator perspectives on the design of cybersecurity and privacy educational resources. In *Proceedings of the Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (pp. 587–603). USENIX Association. https://dl.acm.org/doi/10.5555/3696899.3696930

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation* (4th ed.). John Wiley & Sons.

Mourning, C., Chenji, H., Hallman-Thrasher, A., Kaya, S., Abukamail, N., Juedes, D., & Karanth, A. (2023). Reflections of cybersecurity workshop for K-12 teachers. In *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE 2023)* (pp. 987–993). Association for Computing Machinery. https://doi.org/10.1145/3545945.3569761

Myndigheten för civilt försvar. (2025). *Kampanjen Tänk säkert 2025*. https://www.mcf.se/sv/amnesomraden/informationssakerhet-och-cybersakerhet/arbeta-systematiskt-med-informationssakerhet-och-cybersakerhet/informationssakerhetsmanaden/tank-sakert/kampanjen-tank-sakert/

Oates, B. J. (2006). *Researching information systems and computing*. SAGE Publications.

Panhans, D., Hoteit, L., Yousuf, S., Breward, T., AlFaadhel, A. M., & AlShaalan, B. H. (2022). *Why children are unsafe in cyberspace*. Global Cybersecurity Forum & Boston Consulting Group. https://api.gcforum.org/api/files/public/upload/427a19dc-a35a-485b-938a-08e64ac9ae95_Why-Children-Are-Unsafe-in-Cyberspace.pdf

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy, 18*(2), 40–46. https://doi.org/10.1109/MSEC.2020.2969409

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in computing* (5th ed.). Pearson.

Prior, S., & Ophoff, J. (2024). Lessons learnt from using educational phishing materials with UK primary school children. In N. Clarke & S. Furnell (Eds.), *Information security education – Challenges in the digital age: WISE 2024* (IFIP Advances in Information and Communication Technology, Vol. 707, pp. 36–49). Springer. https://doi.org/10.1007/978-3-031-62918-1_3

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction, 30*, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

Renieri, M., Renieri, A., & Galletta, L. (2025). WalkthroughCyber: Teaching cyber-awareness in Montessori middle schools. In F. Skopik, V. Naessens, & B. De Sutter (Eds.), *Availability, reliability and security: ARES 2025* (Lecture Notes in Computer Science, Vol. 15999, pp. 5–22). Springer. https://doi.org/10.1007/978-3-032-00644-8_1

Saglam, R. B., Miller, V., & Franqueira, V. N. L. (2023). A systematic literature review on cyber security education for children. *IEEE Transactions on Education, 66*(3), 274–286. https://doi.org/10.1109/TE.2022.3231019

Skolverket. (2023). *ICILS 2023: En internationell studie om digital kompetens hos elever i årskurs 8*. IEA & Skolverket. https://www.skolverket.se/publikationer?id=13168

Skolverket. (2024). *Curriculum for compulsory school, preschool class and school-age educare: Lgr22*. https://www.skolverket.se/publikationer?id=13128

Skolverket. (2025). *Fyra aspekter av digital kompetens*. https://www.skolverket.se/kompetensutveckling/stod-i-arbetet/fyra-aspekter-av-digital-kompetens

Sveriges Radio. (2024, November 13). *Många ungdomar har dåliga datorkunskaper*. https://www.sverigesradio.se/artikel/manga-ungdomar-har-daliga-datorkunskaper

Säkerhetskollen. (n.d.). *Säkerhetskollen – privat*. SSF Stöldskyddsföreningen. https://sakerhetskollen.se/privat

Säkerhetskollen. (2024). *Barns säkerhet på nätet*. SSF Stöldskyddsföreningen. https://sakerhetskollen.se/bli-trygg-pa-internet/tips-for-foraldrar/barns-sakerhet-pa-natet

Säkerhetskollen. (2025). *Nätklok – Are You Secure?* SSF Stöldskyddsföreningen. https://natklok.sakerhetskollen.se/

Unga Forskare. (n.d.). *About the Swedish Federation of Young Scientists*. https://ungaforskare.se/

Unga Forskare. (2019, October 28). *”Är du säker? #290 CyberSecurity” – Unga Forskare går ihop med IBM och andra jättar i IT-branschen för att stärka elever i internetsäkerhet*. https://ungaforskare.se/2019/10/28/pressmeddelande/

Videnovik, M., Filiposka, S., & Trajkovik, V. (2024). A novel methodological approach for learning cybersecurity topics in primary schools. *Multimedia Tools and Applications, 84*, 22949–22969. https://doi.org/10.1007/s11042-024-20077-2

Videnovik, M., Trajkovik, V., Vold, T., Kiønig, L. V., Bogdanova, A. M., & Filiposka, S. (2025). Using peer-learning and game-based instruction for achieving long-lasting knowledge of cybersecurity in primary schools. *IEEE Access, 13*, 11679–11688. https://doi.org/10.1109/ACCESS.2024.3479921

Wallström, A. (2024, November 13). IEA-chefen: Myt att IT-generationen lär sig själv. *Svenska Dagbladet*. TT. https://www.svd.se/a/B06PG9/iea-chefen-myt-att-it-generationen-lar-sig-sjalv

Xu, Y., & Li, H. (2025). Cybersecurity matters for primary school students: A scoping review of the trends, challenges, and opportunities. *IEEE Transactions on Learning Technologies, 18*, 513–529. https://doi.org/10.1109/TLT.2025.3564610

Appendices

Appendix A – Semi-Structured Interview Guide and Research Questions (translated from Swedish to English)

Introduction – Background and Digital Context

1. Could you begin by briefly describing your role as a teacher?

- How long have you worked as a teacher?
- Which subjects do you teach?
- Have you worked at other schools previously?

2. How would you describe the digital environment in teaching at your school?

- Which digital tools and platforms are used in teaching?
- What do you perceive students use most in their schoolwork?

Theme 1 – Implementation of Teaching

3. How are issues related to digital security and cyber hygiene usually addressed in your teaching?

- Is this something that is regularly planned into the teaching, or does it arise more spontaneously?
- Are there, for example, theme days, projects, or campaigns related to online ethics or digital security?
- Are there individuals at the school who particularly drive these issues, such as dedicated staff members or responsible teachers?

4. In which subjects or contexts are issues related to Digital Security usually addressed?

- Does it differ between subjects?

5. Which areas related to digital security do you usually discuss with students in teaching?

Social and societal aspects

- Source criticism on the internet, AI, and disinformation/influence campaigns
  Being able to determine what is true or false online.
- Students' digital footprints
  Everything you do online leaves traces that can be stored for a long time.
- Sharing information on social media and apps
  Thinking carefully before sharing images, opinions, or personal information.

- Echo chambers and filter bubbles
  How algorithms can reinforce one's own opinions and limit perspectives.
- Cookies, targeted advertising, and fake advertisements
  Understanding how online tracking and manipulated advertisements influence users.
- Cyberbullying
  When someone is exposed to harassment or offensive behavior online.
- Grooming
  When an adult deceives or manipulates children online with harmful intentions.
- Privacy and integrity
  Your right to keep personal information private.

Fraud and manipulation

- Fraud
  When someone attempts to deceive you through social media, email, or games in order to obtain money or information.
- Phishing
  Fake emails or messages designed to make you reveal passwords or banking information.
- Deepfakes and AI manipulation
- Clickbait and misleading information
  Attempts to make you click on unsafe or misleading links.

Technical aspects (if addressed in teaching)

- Encryption
  Making information unreadable to unauthorized individuals.
- Strong passwords
  How to create *long and difficult passwords that are hard to guess.*
- Two-factor authentication (2FA)
  Additional security, such as a code sent to your phone combined with a password.
- Safe use of public networks
  Being cautious when using open WiFi networks, as others may be able to see your traffic.
- Risks associated with QR codes
  They might lead you somewhere else.
- Risks associated with cloud services
  Who has access to your information?

6. Can you describe a specific occasion when you worked with issues related to online security?

- What was the lesson or situation about?
- How did the students react?

Theme 2 – Access to and Quality of Teaching Resources

7. What materials or resources do you use when working with issues related to digital security in teaching?

- Are you familiar with the organization *Unga Forskare* (The Swedish Federation of Young Scientists) and their educational initiatives, including cybersecurityacademy.se?

- Your school has ordered some of their educational materials and lesson packages. Have you come across these materials in your teaching, or do you know if any colleagues at your school have used or worked with them?

8. What types of activities or teaching methods do you use when discussing these issues with students?
Examples:

- Video clips or films
- Quizzes or digital tests
- Group discussions
- Scenarios or role-playing
- Games or simulations

Theme 3 – Teachers' Knowledge, Confidence, and Professional Development

9. How would you describe your own ability, competence, and conditions when it comes to discussing and teaching students about digital security?

- Which factors do you perceive affect your ability to work with these issues?
- Is there anything that facilitates or complicates teaching within this area?

10. Can you describe areas where you feel particularly confident teaching and discussing, as well as the opposite?

- What makes certain areas easier or more difficult to teach?

11. What opportunities are available for teachers to develop their knowledge and competence within this area?

- What support, training, or professional development opportunities are available?

Theme 4 – Governance, Curriculum, and Organizational Frameworks

12. How do you perceive issues related to digital security as connected to the school's mission or governing documents?

13. How is the work with these issues organized at your school?

- Is it something planned collectively, or is it mainly handled by individual teachers?

14. Do you feel that you have support and sufficient conditions from school leadership to work with these issues?

- For example, in terms of time, resources, or prioritization within the organization.

Theme 5 – Pedagogical Approaches and the Role of the Teacher

15. How do you view the teacher's general pedagogical role in developing students' understanding of Digital Security and Cyber Hygiene?

- How do you view the teacher's role as a guide, mentor, or organizer when students work with these issues?

16. If you imagine an ideal form of teaching about Digital Security, what would it look like in practice?

- What would the students do?
- How would the teacher work?

Concluding Reflection Questions

17. What usually causes issues related to digital security to actually be addressed in teaching?

- Is it planning, current events, or situations that arise among students?

18. Is there anything related to teaching about these issues that we have not discussed but that you believe is important to highlight?

Appendix B – Information for Research Participants (translated from Swedish to English)

Study on Teaching Digital Security and Cyber Hygiene in Lower Secondary School

We would like to ask whether you would like to participate in a research project. This document provides information about the project and what participation involves.

What is the project about and why are we asking you to participate?

The purpose of the project is to investigate the extent to which topics related to Digital Security and Cyber Hygiene are taught in municipal lower secondary schools in the Skaraborg region. These areas may be referred to by many different terms — for example Cybersecurity, IT security, or Information Security — but fundamentally they concern how we use digital services and the internet safely and responsibly in everyday life.

The study has a particular focus on how teachers themselves describe their experiences, approaches, and conditions for teaching within this area. A request was therefore sent to your school principal regarding teachers who address these issues in their teaching. You were subsequently recommended as one of these teachers, as the principal assessed that your teaching may involve the relevant subject area and could therefore contribute valuable experiences and perspectives.

The research principal for the project is the University of Skövde. The research principal refers to the organization responsible for the project.

How will the project be conducted?

Participation in the study involves taking part in a semi-structured interview focusing on your experiences and perspectives related to the subject area in question.

The interview will be conducted either in person or through a digital meeting platform, such as MS Teams, Zoom, or Google Meet, depending on what best suits the circumstances.

The interview is expected to take approximately 30–45 minutes and will mainly consist of open-ended questions, allowing you to elaborate on your responses. No preparation is required on your part, apart from having a functioning microphone and webcam if the interview is conducted digitally.

The interview will be recorded and transcribed to ensure an accurate representation of the content. After the transcription has been completed and corrected, the finished transcript (including a summary of the most important points) will be sent back to you for review to ensure that no misunderstandings or misinterpretations occurred during the interview.

Possible consequences and risks of participating in the project

If the interview is conducted digitally, recording and transcription may be carried out using the built-in functions of the selected meeting platform, where such functions are available.

In this context, there is a minor risk that recorded material may temporarily be processed or stored in cloud services connected to the platform. This handling entails a limited privacy risk; however, no sensitive personal data will be requested within the scope of the study.

There is also the option of using a local recording tool to avoid uploading information to the meeting platform's cloud services.

Apart from this, participation is not considered to involve any physical or psychological risks, other than the time allocated for the interview.

What will happen to your information?

The project will collect and register information about you, for example through the recordings and transcriptions that are made. Contact information such as your name and email address will also be processed during the course of the project when the summary of the most important points from the transcription is returned to you for feedback.

The collected material will be handled with great care and used only for the specific research purpose. Access to raw data, such as recordings and transcriptions, will be restricted to those responsible for the project and handled in a way that prevents unauthorized access.

The University of Skövde is responsible for your personal data. According to the EU General Data Protection Regulation (GDPR), you have the right to access, free of charge, the information about you that is processed within the project and, if necessary, to have any inaccuracies corrected. You may also request that information about you be deleted and that the processing of your personal data be restricted. However, the right to deletion and restriction of processing does not apply when the data are necessary for the current research.

If you wish to access the information, please contact Linus Brifelt, b20linbr@student.his.se.

In the final thesis, all information that can be linked to you as an individual will be anonymized. This means that names, contact details, and other identifying information, including information about the school where you work, will be removed or replaced with de-identified information. The purpose of this is to ensure that individual participants cannot be identified in the final material.

After the project has been completed and the final thesis finalized, certain information that may be linked to individual participants may be retained for a limited period of time. This is done to allow for possible additions, quality assurance,

or further analyses, for example in connection with potential scientific publication.

However, all such information, including recordings, transcribed material, and contact details, will be deleted no later than two years after the completion of the project, in order to ensure participants' privacy.

How will you receive information about the results of the project?

As previously mentioned, you will have the opportunity to review and provide comments on the interview in which you participated when you receive the interview summary for review.

When the study has been completed, you will also be given the opportunity to access the final thesis in its entirety. A link to the publication will be sent to you once the work has been published in DiVA – Digital Scientific Archive.

Participation is voluntary

Your participation is voluntary, and you may choose to withdraw from the study at any time. If you choose not to participate or wish to withdraw your participation, you do not need to provide a reason, and this will not affect you in any way.

If you wish to withdraw your participation, please contact the person responsible for the project (see below).

Persons responsible for the project
The person responsible for the project is Linus Brifelt, b20linbr@student.his.se, Academic supervisor: Oskar MacGregor, oskar.macgregor@his.se.