Cyber Security Training in Finnish Basic and General Upper Secondary Education

Martti Lehto[1] and Pekka Neittaanmäki[2]
[1]Faculty of Information Technology, University of Jyväskylä, Finland
[2]Faculty of Information Technology, University of Jyväskylä, Finland

martti.lehto@jyu.fi
pekka.neittaanmaki@jyu.fi

Abstract: Cyber security in Finland is part of other areas of comprehensive security, as digital solutions multiply in society and technologies advance. Cyber security is one of the primary national security and national defense concerns. Cyber security has quickly evolved from a technical discipline to a strategic concept. Cyber security capacity building can be measured based on the existence and number of research and developments, education and training programs, and certified professionals and public sector agencies.Cybersecurity awareness and the related civic skills play an increasingly important role as our societies become more digitalized. Improving citizens' cyber skills through education is an important goal that would strengthen Finland as a country of higher education and expertise and lay the foundation for the society of the future. Pursuant to the Finland's Cyber Security Strategy (2019) "National cyber security competence will be ensured by identifying requirements and strengthening education and research." Finland's Cyber Security Development Programme (2021) necessitates that in basic education ensures young people have sufficient skills to operate in a digital operating environment and that they understand cyber security threats and know how to protect themselves from them. So, cybersecurity is an important subject for everyone, not just industry or public organizations. It's also vital for our children to understand how to stay safe online, and the need to be aware of any dangers that might come their way. Cybersecurity awareness training is important because it teaches pupils how they can protect themselves from cyber-attacks (MTC, 2021). The study of cybersecurity education in Finland was made in autumn 2021 and spring 2022 for the National Cyber Security Director. According to the study, measures are needed so that cyber security becomes an important aspect when planning education and teaching. There are different models to choose from to make training more effective. This paper presents the results of the research focusing basic and general upper secondary education.

Keywords: Cyber Security Education, Basic Education, General Upper Secondary Education

1. Introduction

Finnish society needs cyber security competence both in public administration and in the business community. At the national level, it must ensure that companies have both top-level experts and other competent personnel. Skills development is also emphasized in the cooperation between the business community and research. (Security Committee, 2019)

Finland is a world leader in using digitalization in higher education and in continuous learning in higher education. Digitalization aims to make educational content as widely available as possible. In view of the growing needs for skills renewal, continuous learning should be given greater priority in the higher education sector. According to the Education Policy Report of the Finnish Government (VN, 2021), a higher level of competence and top expertise are required to develop Finnish society and well-being. One of the objectives is that by 2030, at least half of all young adults in Finland will complete a higher education degree.

Digital transformation has changed societies with an ever-deepening impact on everyday life and demonstrated the need for larger digital education and training in every level. The digital future at school is already integrated into the everyday lives of learners. The pandemic-related exceptional situation during Covid-19 has made it clear to us how important the digitization of state institutions is. At home, smartphones have become indispensable for students. During digitization, schools will transform analog, location-based teaching methods into digital, location-independent training opportunities. The digitization of the schools requires cyber secure systems and cyber security skills from teachers and pupils.

Digital environment has security risks for young people. They are among others social withdrawal, digital gaming addiction, cyberbullying, cognitive overload, material that is harmful for the age, a decrease in mental balance, fake people.

The study, commissioned by the Ministry of Transport and Communications from the University of Jyväskylä leaded consortium, examined the development needs in cybersecurity education and explored comprehensively the quantitative and qualitative development of cybersecurity competencies. This paper is part of this larger study and gives recommendations. (Lehto, 2022)

2. The Finnish Education System

The Finnish education system is a mixture of state controlled or steered and relatively autonomous elements. The government determines the general objectives of education and the division of classroom hours between different subjects. The Ministry of Education and Culture (MEC, 2022) drafts legislation and government decisions pertaining to education. The Finnish National Agency for Education lays out the concrete objectives and core contents of instruction in the different subjects and is responsible for the national core curriculum with its directive norms for good achievement in each. Local authorities (generally municipalities) are responsible for the practical arrangement of schooling and for composing the municipal curriculum based on the national core curriculum. Each school, in turn, writes its own curriculum based on both the national core curriculum and the municipal document. The Finnish education system consists of (FNAE, 2022):

- Early childhood education and care which is provided for children before the compulsory education begins,
- Pre-primary education which is provided for children in the year preceding the beginning of compulsory education,
- Nine-year basic education (comprehensive school), which is compulsory,
- Upper secondary education, which is either general upper secondary education or vocational education and training, and
- Higher education provided by universities and universities of applied sciences.
- Adult education is available at all levels.

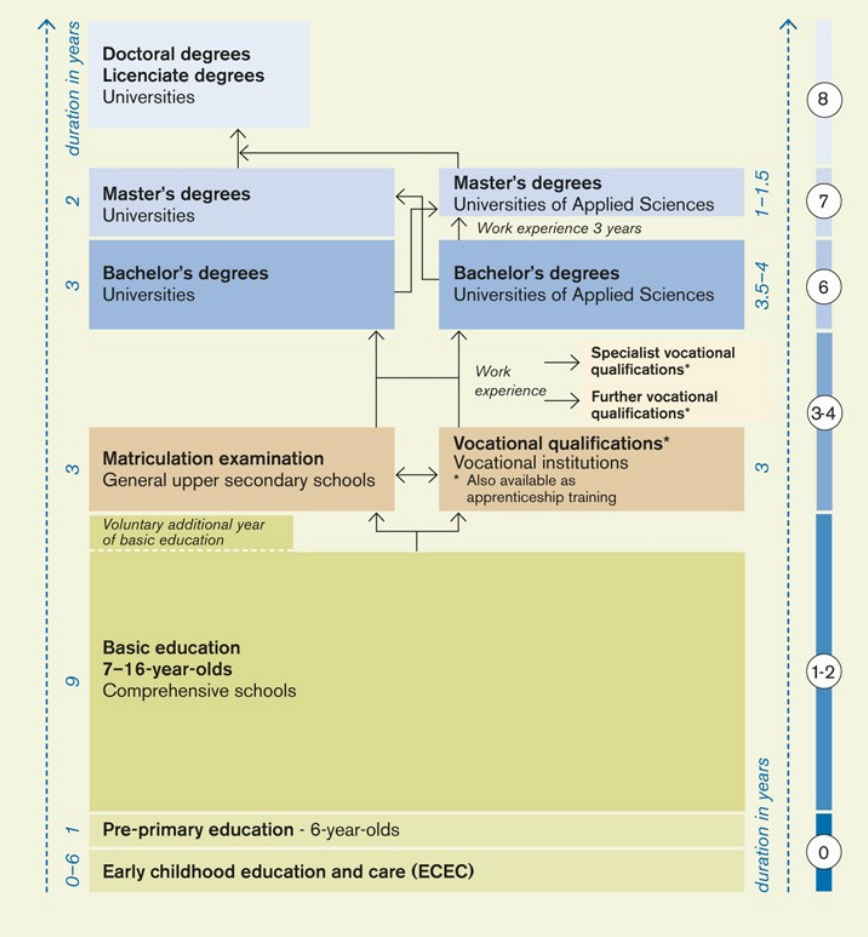

Figure 1: illustrates the Finnish education system.

3. Basic education

3.1 Fundamentals of basic education

Basic education starts in the year when a child turns seven and lasts nine years. basic education starts with comprehensive school and ends at the age of 18. Comprehensive school education (basic education) consists of school years 1 to 9 and is meant for all children aged between 7 and 17 (whole age group). All children who reside permanently in Finland must attend compulsory education. Basic education is provided within a single structure, that is, there is no division into primary and lower secondary education. Instruction is usually given by the same class teacher in most subjects in the first six year-classes and by subject specialists in the last three years. In the curriculum, transversal competence refers to a combination of knowledge, skills, values, attitudes, and will. Competence also means the ability to apply knowledge and skills in a given situation. (FNAE, 2014.) The transversal competence areas are:

1. Thinking and learning to learn
2. Cultural competence, interaction, and self-expression
3. Taking care of oneself and managing daily life
4. Multiliteracy
5. ICT competence
6. Working life competence and entrepreneurship
7. Participation, involvement, and building a sustainable future

Cybersecurity and information security are not a separate subject in the curriculum. Instead, the curriculum includes information and communication technologies (ICT) as a transversal subject. This means that transversal learning outcomes are integrated into the intended learning outcomes of different subjects in different grades. The curriculum states that "ICT is methodically exploited in all grades of basic education, in different subjects and multidisciplinary learning modules, and in other schoolwork." The organiser of the teaching is responsible for planning the content of the teaching in accordance with the curriculum. (FNAE, 2014

One of the transversal competence objectives is ICT competence, which is an important civic skill both in itself and as part of multiliteracy. The pupils are supported in familiarising themselves with various ICT applications and uses and in observing their significance in their daily life. The aim is that they also learn to perceive its risks in a global world. ICT competence is developed in four main areas (FNAE, 2014):

1. The pupils are guided in understanding the principle of using ICT, its operating principles and key concepts and supported to develop their practical ICT competence in producing their own work.
2. The pupils are guided in using ICT responsibly, safely, and ergonomically.
3. The pupils are guided in using ICT in information management and in exploratory and creative work.
4. The pupils gather experience of and practice using ICT in interaction and networking.

The list below shows by grade the third main area, which focuses on the safe and responsible use of ICT.

- In grades 1 and 2, the aim is to discuss together with the pupils and search for safe ways to use ICT and the related etiquette.

- In grades 3 to 6, the pupils are guided in responsible and safe use of ICT, good manners, and knowledge of basic copyright principles. In their schoolwork, they practice using various communication systems and educational social media services.

- When moving to grades 7 to 9, information security and the related risks are addressed in a more concrete way: the pupils are guided to use ICT in a way that is safe and ethically sustainable. They learn how to protect themselves from possible information security risks and how to avoid losing data. They are guided towards responsible activities by reflecting on, for example, the meaning of the concepts of information protection and copyrights and the potential repercussions of irresponsible and illegal activities. (FNAE, 2014.)

3.2 Analysis of the research

Eleven towns across Finland were selected for the survey, which was sent to a total of 448 school principals. The schools were primary or lower secondary schools that follow the Finnish national curriculum for basic education. A total of 108 responses were received.

Inclusion of cybersecurity education in teachers' subjects

Teachers were asked to assess on a scale of 1 to 5 (completely disagree to fully agree) whether they include cybersecurity education as allowed by the subject requirements. The average score was 3.45. Teachers whose answers ranged between 4 and 5 represent equally both primary and lower secondary schools. However, teachers whose answers ranged between 1 and 2 mostly represent teachers in grades 7 to 9. It can be noted that in primary school, cybersecurity / information security is addressed more extensively in different subjects than in secondary school. The result is shown in Figure 2.

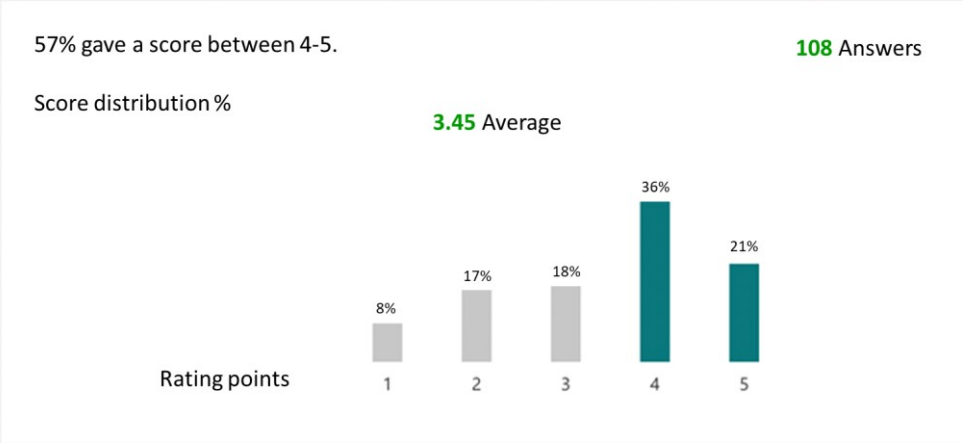

Figure 2: Inclusion of cybersecurity education in teachers' own subject.

Inclusion of cybersecurity education in other subjects

The teachers were asked whether cybersecurity education should in some way be included in all subjects or whether it should be taught separately, for example, only as part of IT education. The teachers were not unanimous on this point: 27% of the respondents felt that it would be more sensible to only teach cybersecurity as part of IT education, while 73% of the respondents felt that cybersecurity belongs to all areas of basic education.

Pupils' and teachers' awareness of secure use of services

The survey asked teachers to assess pupils' and staff's knowledge of the secure use of equipment and study-related services. The assessment was carried out on a scale of 1 to 5 (fully disagree to fully agree). The average response was 3.26. Most responses ranged between 3 and 4, suggesting that teachers perceive both their own and their pupils' knowledge of the secure use of equipment and study-related services as quite strong.

Implementation of secure use of information and communication technologies in teaching

Teachers were asked to assess whether the objectives for the safe use of information and communication technology defined in the curriculum for different grades are met in their teaching. The majority of teachers felt that the objectives were met in their teaching. Eleven teachers estimated that the grade-specific objectives are not achieved in their teaching. Of these teachers, all teach grades 7 to 9 (see Figure 3).

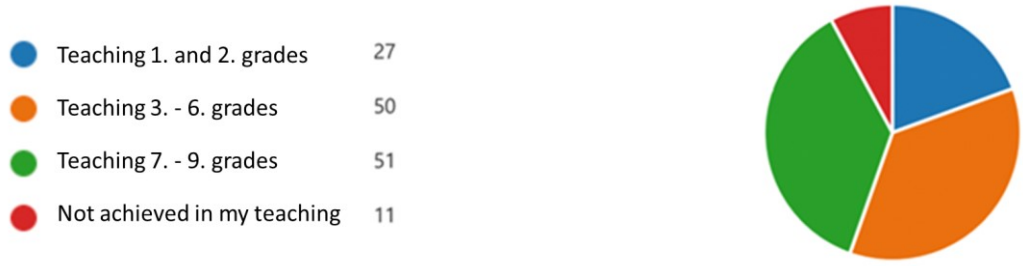

Figure 3: Objectives of secure use ICT in the curriculum by grade.

Clarity of the current curriculum guidelines for teaching cybersecurity/information security

Teachers were asked to assess on a scale of 1 to 5 (fully disagree to fully agree) how clear the instructions in the current curriculum are in support of cybersecurity and information security education. The average was 2.96 (see Figure 4). Most respondents answered 3, which indicates that the teachers receive some support from the curriculum, but do not consider the curriculum guidelines sufficiently clear when it comes to teaching cybersecurity / information security.

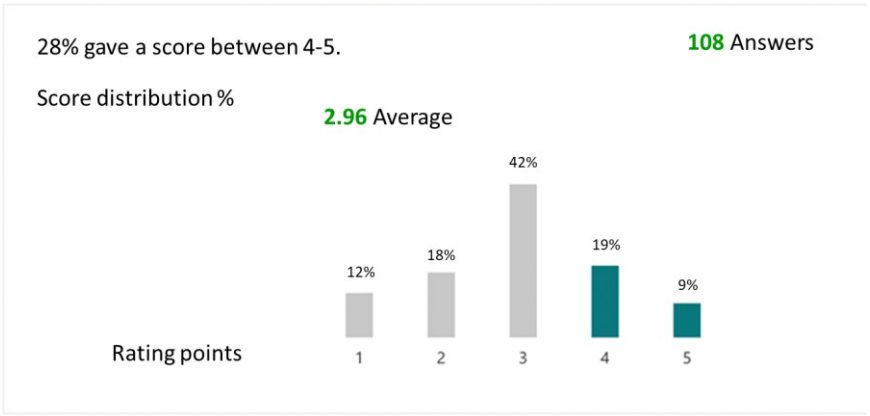

Figure 4: Curriculum guidelines for cybersecurity teaching.

Teachers' perception of their cybersecurity teaching competence

Teachers took a rather positive view of their own knowledge and ability to incorporate cybersecurity as part of their teaching. The assessment was carried out on a scale of 1 to 5 (fully disagree to fully agree). The average score was 3.66. Teachers who responded on a scale of 4 to 5 (n = 68) are fairly evenly divided between teachers of grades 3 to 6 and of grades 7 to 9. Of those responding between 1 and 3 (n = 40), a clear majority (n = 27) teach grades 7 to 9. This is in line with the answers to previous questions, where lower secondary school teachers see cybersecurity/information security as a separate subject rather than a topic to be included in all subjects. Figure 5 presents the teachers' view of their ability to teach cybersecurity.

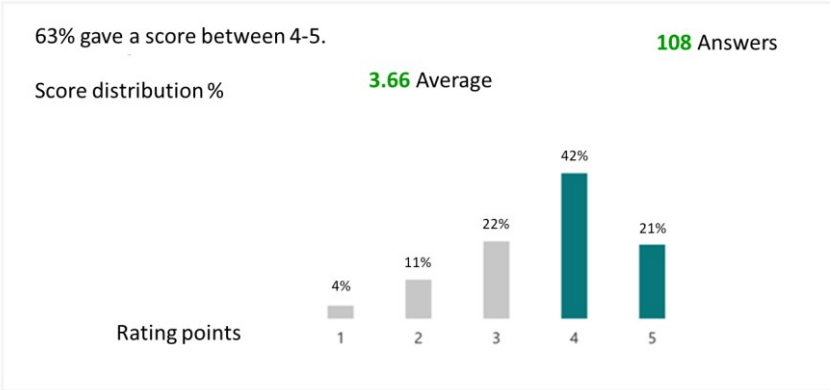

Figure 5: Teachers' self-assessment of their competence.

3.3 Development of digital safety education in basic education

3.3.1 General development needs

The training needs of digital security and its importance are widely recognised. There is thus a willingness to develop training. Recent projects, such as the *Cyber Security Development Programme*, *New Literacy Development Programme,* and the Finnish National Board of Education's guidelines for schools on information security, demonstrate a desire to make digital security an important area in the planning of education and teaching at the level of basic education.

Currently, however, materials and tools serve more as guidelines and support than as obligations, so that responsibility for the use of these materials, or lack thereof, rests with the organiser of the teaching. In addition, the objectives for the use of ICT set out in the curriculum within different subjects remain broad, so that implementation methods can vary greatly, for example, between different towns, not to mention within different schools within a town. Information and communication technologies are offered as an elective subject in many towns, but the teaching includes very little digital security. The objectives are often very similar, regardless of the grade.

It should be noted that one of the objectives of the *Cybersecurity Development Plan* is that digital security should be included in the curriculum as a separate subject. This objective would be particularly important if reached. In addition to ensuring that primary and lower secondary school pupils have digital security skills, there is also a need to ensure an adequate supply and level of education for teachers. This will cover the needs of the entire comprehensive school regarding digital security.

In order to fulfil the goal of Finland's cybersecurity strategy and to enable everyone to operate safely in the digital world, more studies must be carried out on the digital security learning needs of children in this age group.

3.3.2 Development models based on research

There are two ways of approaching the development of digital security education in primary education: the study examined teachers' views on whether digital security should be integrated into every subject or whether it should be separated into, for example, information technology education. For a number of subjects, the curriculum for basic education identifies skills that are also needed for secure behaviour in the digital world, such as source criticism and media literacy, but there is no clear stance on digital security/cybersecurity/information security directly.

The results of the survey demonstrate that the inclusion of digital security teaching in primary and lower secondary schools within the subject limits varies between teachers: some do not include digital security in their teaching at all. In addition, teachers' views on the guidelines for the development of digital security education are divided. The study highlighted three models of how digital security education can be developed and increased in basic education. The models are not mutually exclusive.

Model 1: Digital security as a concept of transversal competence

This line of development could be achieved on the basis of the current curriculum by modifying the concept of transversal competences as regards ICT skills. Currently, transversal competence consists of six areas, and it forms the common objectives of all subjects in basic education. By adding digital security as a separate area, it would become visible and concrete in all areas of basic education.

This addition is well justified by the fact that digital security and its importance have grown in all sectors of society in recent years at a very fast pace. In addition, it is present everywhere in the school world. This is also evident in the open answers to the survey: most responses could not be determined to relate to a single subject. Rather, cybersecurity is visible in all subjects.

Some way of incorporating digital safety education into each subject would require additional resources for primary schools. In particular, adding an entire area to the concept of transversal competence would require extensive changes to the curriculum and, as a result, to the content of the subjects. To this end, teachers in both primary and lower secondary schools should be guaranteed access to continuing education in order to enable the inclusion of this component in their teaching.

Model 2: Digital security as part of the ICT competence area

A smaller structural change to make digital security more visible in all aspects of primary education would be to include digital security in the current ICT competence area.

Model 3: Digital security as part of extended ICT education

This objective could be achieved by strengthening the compulsory nature of ICT in primary and lower secondary schools in Finland. Currently, the availability of this elective subject depends on the school's own emphasis or willingness to offer ICT studies as elective courses. ICT education would include a digital security component.

Most of the teachers who responded to the survey stated that they do include cybersecurity in their teaching. If digital security were part of ICT education, it should be noted that this line of development also requires additional resources in terms of the content of teacher training, but also in terms of the number of staff.

4. General upper secondary education

4.1 Fundamentals of the general upper secondary education

Students who have successfully completed compulsory education are eligible for general or vocational upper secondary education and training. Student selection to upper secondary schools is mainly based on students' grades in their basic education certificate. More than 90 per cent of the relevant age group starts general or vocational upper secondary studies immediately after basic education. Completion of upper secondary education gives students eligibility to continue to higher education.

General upper secondary education provides, as its name suggests, general education. It does not qualify students for any particular occupation. At the end of general upper secondary school, students take a national school-leaving examination known as the Finnish matriculation examination. Those who pass the examination are eligible to apply for further studies at universities, universities of applied sciences and vocational institutions. General upper secondary education usually takes three years to complete. (FNAE, 2019)

The syllabus of general upper secondary education is designed to last three years, but students may complete it in 2 to 4 years. Instruction is organized in modular form not tied to year classes and students can decide on their individual study schedules rather freely. Each course is assessed on completion and when a student has completed the required number of courses, which include compulsory and elective studies, he or she receives a general upper secondary school certificate. (FNAE, 2019)

The Finnish National Agency for Education (2019) decides on the objectives and learning outcomes of the different subjects and study modules for general upper secondary education. Based on the national core curriculum, each education provider then prepares the local curriculum. Due to the modular structure of upper secondary education, students may combine studies from both upper general education and vocational education and training.

The curriculum was introduced locally as of 1 August 2021. While the new Act on General Upper Secondary Education entered into force on 1 August 2019, all aspects described in greater detail in local curricula, or those related to teaching, support for learning, guidance and cooperation, became obliging to education providers as of August 2021 (FNAE, 2019, 9).

The national core curriculum for general upper secondary education states that "Education and other activities in general upper secondary schools must be organized in accordance with the general national objectives defined in the Government Decree on General Upper Secondary Education (810/2018)." The aim is that the students may grow into educated members of society, acquire knowledge and skills required by the changing operating environment, and improve their capabilities for continuous learning. Particular emphasis is placed on the importance of transversal general knowledge and ability and understanding broad issues, and on encouraging the students towards ethically responsible and active agency as part of the local, national, European, and global community. (FNAE, 2019, 58.)

The students become accustomed to assessing the reliability of texts and information. In addition, the instruction guides the students in advancing their knowledge of information and communication technology and using it appropriately, responsibly, and safely, both when working alone and with others. (FNAE, 2019, 58.)

The areas of transversal competences comprise the common objectives of the general upper secondary school subjects (FNAE, 2019, 60). The transversal competences are complemented and expressed in concrete terms in the local curriculum for each subject and in the description of each study unit. Transversal competences are

taken into account in the school culture. Their implementation is complemented by descriptions of arrangements for familiarization with higher education studies and the world of work as well as international competence included in the curriculum. The contents of the thematic studies can be selected from the areas of transversal competences. (FNAE, 2019, 61–62.) Areas of transversal competences are:

1. Global and cultural competence
2. Well-being competence
3. Interaction competence
4. Multidisciplinary and creative competence
5. Societal competence
6. Ethical and environmental competence

4.2 Analysis of the research

The survey was targeted at 103 general upper secondary schools and sent to their principals. A total of 54 responses were received from 16 towns. The aim was to recruit respondents among teachers who include cybersecurity/information security/digital security in their teaching. Therefore, more than one teacher may have responded from each participating school.

Inclusion of cybersecurity in education in a timely manner as permitted by the subject

Teachers were asked to assess on a scale of 1 to 5 (completely disagree to fully agree) whether they include cybersecurity education as allowed by the subject requirements. The average score was 2.77. (See Fig 6)

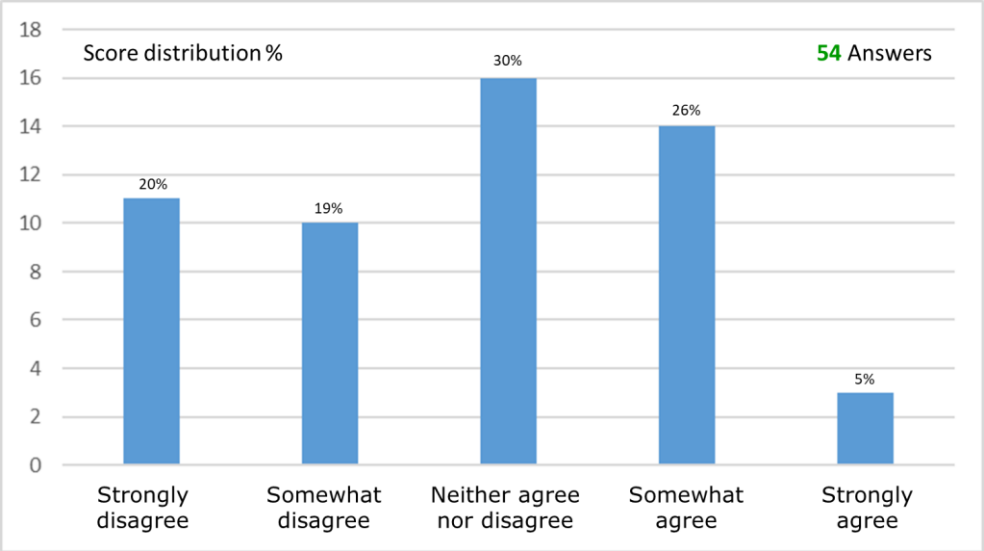

Figure 6: Inclusion of cybersecurity education in subject teaching.

Cybersecurity education should be included in every subject

The teachers were asked whether cybersecurity education should in some way be included in all subjects or whether it should be taught separately, for example, only as part of IT education. This divided teachers' opinions, also among ICT teachers. Taken together, the majority of all respondents (33) thought that cybersecurity belongs to all areas of the general upper secondary school. 21 respondents think it should be part of ICT teaching.

Clarity of the current curriculum guidelines for teaching cyber/information security

Teachers were asked to assess on a scale of 1 to 5 how clear the instructions in the current curriculum are in support of cybersecurity and information security education. The average was 1.96 (see Figure 7). The low average indicates that the responding teachers do not think the curriculum guidelines are clear when it comes to teaching cybersecurity and information security.

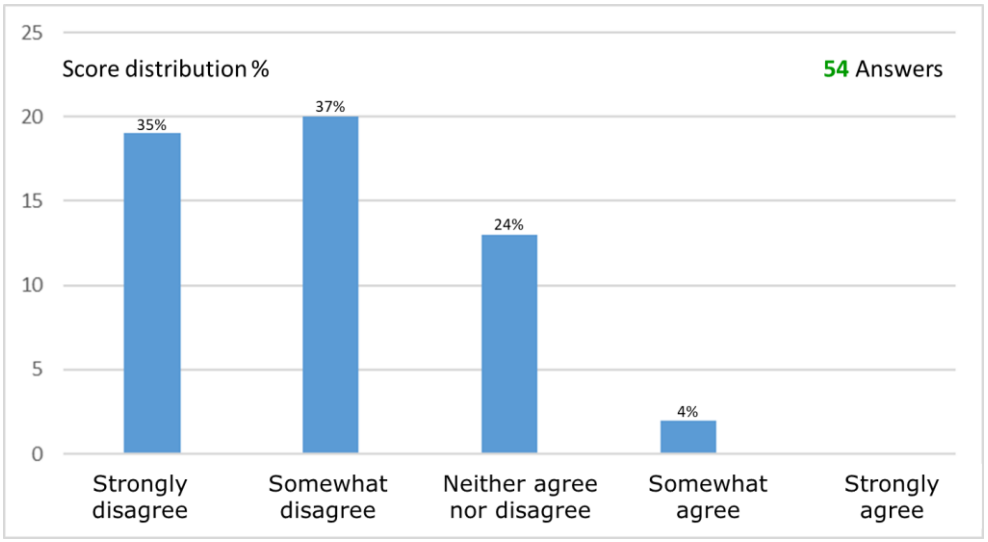

Figure 7: The clarity of the curriculum guidelines regarding cybersecurity teaching.

Teachers' capabilities in incorporating cybersecurity into teaching

On average, teachers were fairly neutral about their own ability to incorporate cybersecurity into their teaching. The assessment was carried out on a scale of 1 to 5. The average was 3.06.

4.3 Development of cybersecurity education in general upper secondary education

The development of cybersecurity education in general upper secondary education can be approached in several ways. This report explored teachers' views on whether cybersecurity education should in some way be included in each subject or whether it should be separated as part of a single subject such as information technology education. The study identified three models that are not mutually exclusive.

Model 1: Digital security for all areas of the general upper secondary school

This line of development could be achieved on the basis of the current curriculum by modifying the concept of transversal competences. Currently, transversal competence consists of six areas, and it forms the common objectives of all subjects. Adding digital security as an area of its own would make cybersecurity visible in all areas of the general upper secondary school. This addition is well justified by the fact that digital security and its importance have grown in all sectors of society. In addition, it is a multidisciplinary field of study, and this is also reflected in the survey responses.

Model 2: Digital security as part of the current areas of transversal competence

A smaller structural change to make digital security more visible in all aspects of general upper secondary education would be to include digital security in any of the existing competence areas.

Model 3: Digital security as part of ICT education

This line of development could be achieved by increasing the amount of ICT education in general upper secondary schools. Digital security would be included as one component of ICT education. The majority of responding ICT teachers stated that they already include digital security as part of their teaching. This line of development requires additional resources.

In addition, one line of development is to explore the possibility of creating general upper secondary schools specialised in the field of ICT in Finland, or alternatively the possibility of adding a specialisation into ICT to existing general upper secondary schools.

Incorporating digital safety education into all subjects would require additional resources for general upper secondary education. Especially adding an entire new area to the concept of transversal competence would require significant changes to the curriculum. Teachers should also be guaranteed access to continuous training if they so wish, so that the implementation of the component in the subject is equally possible for everyone.

5. Conclusion and discussion

The training needs of digital security and its importance are widely recognized. There is thus a willingness to develop training. Recent projects, such as the Cyber Security Development Programme, New Literacy Development Programme, and the Finnish National Board of Education's guidelines for schools on information security, demonstrate a desire to make digital security an important area in the planning of education and teaching at the level of basic education (FNAE, 2021). Currently, however, materials and tools serve more as guidelines and support than as obligations, so that responsibility for the use of these materials, or lack thereof, rests with the organizer of the teaching. In addition to ensuring that primary and lower secondary school pupils have digital security skills, there is also a need to ensure an adequate supply and level of education for teachers. This will cover the needs of the entire comprehensive school regarding digital security.

The national curriculum for general upper secondary education defines transversal competences and its different areas. These areas comprise the common objectives of the general upper secondary school subjects. Transversal competences create the preconditions for acquiring the knowledge and skills which enable students to cope with change in an increasingly digital and complex world. General upper secondary school education has several overall objectives defined in the curriculum. One of the objectives is to guide the individual in advancing their knowledge of information and communication technology and using it appropriately, responsibly, and safely, when working both alone and with others.

The results show that responding teachers do not feel that the curriculum contains clear instructions on how to teach cybersecurity. On average, teachers were fairly neutral about their own ability to incorporate cybersecurity into their teaching. Teachers' views were divided on whether cybersecurity education should in some way be included in all areas of the general upper secondary school, or whether cybersecurity education should be differentiated into a single subject such as information technology education. The majority of responding ICT teachers include cybersecurity education in their teaching.

Increasing and developing cybersecurity education can be approached from several different perspectives. This report identified different approaches which are not mutually exclusive. In the first approach, cybersecurity education will be integrated into all subjects by modifying the concept and content of transversal competences. The second option increases and develops cybersecurity education by improving access to ICT education and takes cybersecurity into account as part of its education.

IT skills, communication skills, media literacy and the use of social media constitute the foundation for the skills needed to use digital services. The proposed goals included the incorporation of ICT use as an integral part of the education in schools as well as in basic and supplementary teacher training. In addition, the investment in applied ICT know-how should be scaled up – with cyber security being one of its elements – and given a more prominent place in curriculum design throughout all education.

The challenge regarding the way things are now is the lack of cyber security education objectives for the entire education system. The sought-after improvement of competencies requires defining the basic skills and competencies for the entire national education system. It is necessary to have an understanding of what each citizen needs to know about cyber security, the demands of working life, what kind of professional skills are needed.

References

FNAE. (2014). Perusopetuksen opetussuunnitelman perusteet. https://www.oph.fi/fi/koulutus-ja-tutkinnot/tietoturva-ja-suoja-koulussa.

FNAE. (2019). National Core Curriculum for General Upper Secondary Education 2019, Finnish National Agency for Education. https://www.oph.fi/sites/default/files/documents/lukion_opetussuunnitelman_perusteet_2019.pdf.

FNAE. (2021). Tietoturva ja -suoja koulussa, Finnish National Agency for Education, https://www.oph.fi/fi/koulutus-ja-tutkinnot/tietoturva-ja-suoja-koulussa.

FNAE. (2022). Finnish education system, Finnish National Agency for Education. https://www.oph.fi/en/education-system.

Lehto M. (Edit.) (2022). Development Needs in Cybersecurity Education, University of Jyväskylä Research report 93/2022.

MEC. (2022). General education. https://okm.fi/en/general-education.

MTC. 2021. Finland's Cyber Security Development Programme 2021, Ministry of Transport and Communications, 2021:7.

Security Committee. (2019). Finland's cyber security strategy 2019, Government Resolution 3.10.2019.

VN. (2021). Education Policy Report of the Finnish Government, Publications of the Finnish Government 2021:64.