Informaatioteknologian tiedekunnan julkaisuja
No. 96/2022

Lehto, Martti (ed.)

Development Needs in Cybersecurity Education: Final report of the project

JYVÄSKYLÄN YLIOPISTO

Informaatioteknologian tiedekunnan julkaisuja
No. 96/2022

Editor: Martti Lehto
Covers: Teemu Rahikka

ISBN 978-951-39-9469-3 (e-publication)
ISSN 2323-5004

Jyväskylä 2022

Development Needs in Cybersecurity Education

Final report of the project

Martti Lehto (ed.)

JYVÄSKYLÄN YLIOPISTO

jamk | Jyväskylän ammattikorkeakoulu

TURKU AMK

CONTENTS

Introduction

The implementation of cybersecurity research, development, and training and education at different levels strengthens both national expertise and Finland as an information society. Several strategies have been published at the EU and national levels with the aim of improving cybersecurity expertise and facilitating research, education, and innovation in the field.

The current research project promoted and considered the objectives set out in the EU Cybersecurity Strategy 2020, the EU's Digital Agendas for Europe, the Finnish Cybersecurity Strategy (2019) and its Development Programme (2021) and the EU–Finland skills development programmes.

This study, commissioned by the Ministry of Transport and Communications from the University of Jyväskylä, examined the development needs in cybersecurity education and explored comprehensively the quantitative and qualitative development of cybersecurity competencies.

The main research question of the project was defined as "What measures are needed to improve the quantitative and qualitative situation of Finland's cybersecurity expertise?" The study produced a clear depiction of the current state of cybersecurity education at different levels of education and the necessary measures to meet quantitative and qualitative cybersecurity competence needs in the curricula.

The organisations participating in the project were the University of Jyväskylä, Jyväskylä University of Applied Sciences, Turku University of Applied Sciences, and Linkitin Oy. The project comprised seven work packages, and the research work was divided among the participating organisations as follows:

Organisation	Tasks	Participants
University of Jyväskylä	Investigation of cyber education in universities Investigation of cyber education in general upper secondary schools Investigation of cyber education in primary and lower secondary education Investigation of other cyber education and training	Martti Lehto Jussi Simola Annika Nykänen Jussi Aaltonen Marianne Lindroth Matias Holmström
Jyväskylä University of Applied Sciences	Investigation of cyber education at universities of applied sciences	Karo Saharinen Tuomo Sipola Tero Kokkonen
Turku University of Applied Sciences	Investigation of cyber education in vocational education and training	Mika Koivunen Poppy Skarli Jani Ekqvist Jarkko Paavola
Linkitin Oy	Investigation of the quantitative need for cyber expertise	Antti Sillanpää

Summary

The field of cybersecurity suffers from a massive skills shortage. This study set out to investigate ways to respond to this problem. Through surveys and interviews as well as the content analysis of documents, we have reviewed the cybersecurity / information security / digital security education and training provided in basic education, general upper secondary schools, vocational schools, and higher education institutions, as well as in the third sector in Finland. The results clearly show that the current resources will not be sufficient to cover all recruitment needs in cybersecurity. Rather, significant public investments between EUR 8 and 9 million per year are needed.

The study also revealed that terminology in this field is diverse. The concepts of cybersecurity, digital security and information security are often used interchangeably. They do not have nationally or internationally agreed definitions. The Finnish Ministry of Finance's report on digital security in the public sector[1] defines digital security as a broad concept that includes issues related to risk management, business continuity management and preparedness, as well as cybersecurity, information security, and data protection.

Guidelines for competence renewal

Finland is a world leader in using digitalisation in higher education and in continuous learning in higher education. Digitalisation 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.

The Ministry of Education and Culture regulates which degrees can be completed and at which levels in each higher education institution and what education leading to a degree they are obliged to provide. This aims to ensure the provision of education in accordance with the needs of society and working life and to establish a national division of labour between higher education institutions. Deciding on admissions criteria – that is, which skills students are required to have in different fields – falls within the autonomy of higher education institutions.

According to the Finnish Government's education policy report[2], a higher level of competence and, in particular, 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. To achieve this goal, an additional 100,000 new higher education degrees in total must be completed by 2030 compared to what can be achieved with the current intake numbers. The work on the 2030 vision for higher education and research identified a need for more experts, high-quality higher education, and research and innovation in Finland, as well as for forging strong connections with new knowledge produced in other countries. Higher education

[1] Digital Security in the Public Sector. Publications of the Ministry of Finance 2020:45. http://urn.fi/URN:ISBN:978-952-367-337-3

[2] Education Policy Report of the Finnish Government. Publications of the Finnish Government 2021:64. http://urn.fi/URN:ISBN:978-952-383-927-4

institutions have increased their intake; in addition, the government has already decided to increase the intake of higher education institutions by more than 10,000 students between 2020 and 2022.

According to the government report, the additional intake will be mainly directed at fields with a high level of education demand and employment, nevertheless taking into account flexibility in terms of demand fluctuations and labour market changes. It is essential to strengthen conversion training and further training, in which continuous learning plays an important role.

The Service Centre for Continuous Learning and Employment (JOTPA) promotes the development of skills for people of working age and the availability of a skilled workforce. It analyses the competence and labour market needs of working life, finances education and training for people of working age, develops information, advisory and guidance services, supports regional and other cooperation, and participates in the development of a digital service package for continuous learning. With more than EUR 40 million at its disposal, JOTPA will launch a networked proactive development project together with education providers and higher education institutions to support their strategic and operational planning. In addition, the service centre initiates central government grant applications and procurement procedures based on identified training and competence needs.

The civic skills related to cybersecurity play an increasingly important role as our societies become more digitised. With that in mind, Aalto University and the Ministry of Transport and Communications are carrying out a project in 2022–2024 to create an educational package to promote cybersecurity skills in the EU Member States. The main goal of the project is to launch an open website that teaches cybersecurity skills to citizens. The content of the website will be available in all official languages of the European Union.

Digital security teaching in basic education

The importance of and need for digital security education are recognised in basic education. 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. Developing and increasing digital security instruction in basic education may be carried out through three models, which are not mutually exclusive.

A. Digital security as an area of transversal competence

This model would develop the concept of transversal competences. Currently, transversal competence includes seven areas that form the common objectives of all subjects in primary and lower secondary education. By adding digital security as a separate area (**Digital security, T8**), it would become a visible and concrete area in basic education.

B. Digital security as part of the ICT competence area

A smaller structural change to make digital security more visible in all aspects of basic education would be to include digital security in the current ICT competence area (5).

C. Digital security as part of 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.

Digital security education in general upper secondary schools

Developing and increasing digital security education in general upper secondary education may be carried out through three models. The three models identified in the study are partly overlapping and not mutually exclusive.

A. Digital security as an area of transversal competence

This solution could be implemented on the basis of the current curriculum by developing 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 a separate area would make it visible in general upper secondary school education.

B. 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 current competence areas (5).

C. Digital security as part of ICT education

This development goal could be achieved by improving the availability of ICT education in general upper secondary schools. Digital security would be embedded in ICT education as one component.

Strengthening digital safety education requires additional resources for general upper secondary education. Adding a new area to the concept of transversal competence would require changes to the curriculum. Teachers should also be guaranteed access to continuous training if they so wish, so that the area could be included in the instruction of different subjects by all teachers equally.

In addition, one line of development is to explore the possibility of creating **specialised upper secondary schools in ICT** in Finland, or alternatively the possibility of adding a specialisation into ICT to existing general upper secondary schools. These ICT studies would include digital security education.

Cybersecurity instruction in vocational education and training

Currently, cybersecurity instruction is mainly provided in the training of IT support specialists, ICT technicians, and network installers. The national requirements for qualifications in cybersecurity are considered a good starting point for teaching. However, the requirements were considered so demanding that there is little possibility of demonstrating competence in workplaces. Rather, demonstrations must be carried out in an educational institution.

Cybersecurity competence areas are only included in initial, further, and specialist vocational qualifications in ICT as an optional competence area. **To increase national cybersecurity competence, we recommend making cybersecurity training a mandatory part of vocational training and education in ICT.** In addition, it should be systematically integrated into all other vocational education and training as well.

Teachers' interest in developing their own skills is necessary and requires support. Higher education institutions must be given resources for organising opportunities for continuous learning for vocational teachers, and measures should be taken to promote teachers' familiarity with the working life.

Cooperation between different educational institutions, teacher to teacher, must be developed and a platform and a forum created for it. Such cooperation would bring many benefits. If the qualifications are based on the same criteria, it is possible to use the same training materials. The development of educational environments can also be carried out in cooperation. Up-to-date information on technological developments may be easily shared. Jointly created models will also lower the threshold for starting education and training in new institutions.

Cooperation with the working life must be developed by promoting awareness of initial, further, and specialist vocational qualifications and the included traineeships with the business sector.

Cybersecurity education in universities of applied sciences

The shortage of skilled cybersecurity experts is globally recognised. Regarding this skills shortage, it is important to consider the different competences needed in different jobs. The range of knowledge, skills, and competences in cybersecurity is wide, and cyber professionals need to specialise in a specific area. This must be taken into account in education, that is, educators will need to be mindful of the jobs in which graduating students are expected to be employed. Of course, it must be kept in mind that education provides certain basic competences, which may be developed later into deeper expertise through work assignments, specialisation, and possible specialist training.

The cybersecurity education provided by universities of applied sciences (UAS bachelor's and UAS master's degrees as well as specialist education, continuing education, and conversion training) is comprehensive in content and is able to adapt to the needs of the industry due to its modular structure. The current intake in cybersecurity studies at universities of applied sciences is approximately 555 (Model A and Model B degree programmes). The intake in Model A education is 165 and in Model B, 390. **Investments are needed in educational resources to meet the demands of continuously expanding digitisation.**

When considering the resources for training, it should also be remembered that universities of applied sciences generally provide technical cybersecurity training, which aims for technical competence. Such engineering **instruction requires extensive and complex learning environments**, which are expensive to acquire and maintain. To guarantee sufficient technical expertise, the acquisition, development, and maintenance costs of the necessary learning and training environments must be considered in resource allocation.

It is necessary to increase the number of teachers if cybersecurity education is to be increased. The challenge is in the attractiveness of teaching in the recruitment of sufficiently skilled experts. In this rapidly developing sector, instructional content must support working life and therefore also partly stem from its needs.

Cybersecurity education must also be targeted at different areas of working life. In this way, the necessary skills would be available to society in general. Continuing education that updates existing degrees also requires teaching resources.

Cybersecurity education in universities

The intake of degree programmes in cybersecurity and security is estimated at around 250 in 2022. Approximately 60%–70% of those who start in these programmes will graduate within the normal timeframe. Overall, approximately 80% of the intake will complete the degree programme. Of course, even those who have entered working life without completing their degree have quite good cybersecurity skills. Overall, the number of experts produced by universities is relatively small when considering the identified skills shortage.

The number of applicants for key degree programmes in the field, such as the Master’s Degree in Cyber Security at the University of Jyväskylä, studies in Security and Cloud Computing (Security) at Aalto University, and in Cyber Security at the University of Turku, show that cybersecurity as a field of education attracts significant interest.

At the time of this investigation, Finnish universities offered little continuing education and specialist education in cybersecurity, with the exception of Aalto University, which offered more continuing education related to the field. Instead, it is possible to study several cybersecurity courses in the academic year 2021–2022 through the FITech Network University. However, it only offers individual courses, not full study modules on cybersecurity.

There is a lack of cooperation between universities in cybersecurity education, even though significant benefits were identified if it were developed. Additional resources would improve teaching, and this would be reflected, for example, in the increase of **exercises developing practical skills in cybersecurity**. One challenge for resources is the recruitment of experts in the field.

The number of cybersecurity experts in society can be increased by influencing several factors. **One way is to increase the number and initial intake of degree programmes in the field**. This **requires an increase in human resources**. In addition, the number of cybersecurity experts can be increased **by developing university-level continuing education** and the course selection of the FITech Network University, for example, in the form of a full study module on cybersecurity. Furthermore, improving

educational cooperation between universities would enable students to acquire more versatile specialisations in different areas of cybersecurity.

The ongoing **Digivisio 2030 project** would enable the implementation of a pilot study programme in cybersecurity. In the Digivisio project, all Finnish higher education institutions together build a future for learning. The aim is a new era of learning, at the core of which is the continuous development of digital pedagogy, and in which each of us can more easily learn and accumulate our knowledge in a changing world.

Other cybersecurity training and education

Non-degree studies in cybersecurity are available in Finland, but currently those most in need of education will not find it, nor will they seek it. For example, there is very little training aimed at older people.

Children and young people receive some training in cybersecurity as part of their educational paths, both in primary and lower secondary education and later studies. However, those who completed their studies at a time when cybersecurity was not part of basic education or further studies may currently be completely excluded from cybersecurity training if they do not receive it at their workplace.

There are quite a few providers of training to companies and other organisations in Finland. Employees in large companies and public organisations generally receive training in connection with their work, but employees in SMEs, the self-employed, and entrepreneurs may not. Another problem may be that SME management or entrepreneurs do not recognise the need for training, or the price of training creates problems. The supply of education is scattered, and not everyone has an understanding of what kind of education they would need.

Adult education centres train different age groups, but even education providers themselves do not necessarily have an idea of what kind of training should be organised.

For large companies and public organisations, the situation is positive. Large companies have the capacity to purchase cybersecurity training for their employees, and training companies are happy to provide training solutions tailored to their needs. In the public sector, HAUS offers a wide range of cybersecurity-related training, which ensures basic competence for organisations' personnel.

Key development areas

Critical target groups particularly include older people, children, parents of young children, and immigrants who do not have access to education in their own language. Training should be organised for these risk groups in cooperation with organisations already working with them, for example, in the case of children, with the Central Union for Child Welfare. The importance of cybersecurity issues should also be communicated especially to senior citizens and those working with them.

The staff of SMEs, the self-employed, and entrepreneurs are easily left without adequate cybersecurity training. Their understanding of the importance of cybersecurity should be increased, and they should be supported in acquiring cyber training. One example of such support measures would be vouchers for the purchase of training services. These groups would benefit from having all cybersecurity training on offer under a single website.

Adult education centres are a major provider of training for senior citizens, but not all adult education centres or teachers have sufficient knowledge of cybersecurity training. Further training in cybersecurity is needed for adult education teachers and education coordinators. Participants will also need subsidies.

Effective cooperation networks have been established in other EU countries, connecting companies, government bodies coordinating cybersecurity training, and the third sector. Finland would need **a body responsible for training citizens and coordinating the related cooperation** along with sufficient financial and human resources. The cooperation network could be used to design a website that gathers cyber training and to develop further the concept of cybersecurity for citizens. The network should involve the largest training providers from all sectors as well as those working with at-risk groups, SMEs, and entrepreneurs.

Quantitative needs and their development

The skills shortage is a reality, although it is difficult to predict its level accurately. Based on existing data, it is estimated that Finland will need between 5,000 and 8,000 cybersecurity professionals in the coming years. In addition, between 1,000 and 5,000 new professionals will work with cybersecurity alongside other work. All these people need to be trained accordingly. The greatest number of new experts is needed in secure production. More specifically, this group of 6,000 to 13,000 new cyber professionals can be divided according to their main field of training as follows:

1. Secure production 1,100–2,400 persons
2. Operation and maintenance 900–1,900 persons
3. Oversight and governance 1,000–2,200 persons
4. Protection and defence 1,000–2,300 persons
5. Analysis 800–1,700 persons
6. Collection of data and operation 600–1,300 persons
7. Investigation 600–1,300 persons

Increasing the intake of cybersecurity education requires resources for both education and research. The challenge is to recruit researchers and teachers to higher education institutions within a short timeframe.

The cost of the increased intake in universities of applied sciences (UAS) depends on the degree level and field of study. At the UAS bachelor’s level, the additional cost is about EUR 6,000/year/student, and at the UAS master’s level, about EUR 9,000/year/student.

In universities, the cost impact arises when the intake increases by dozens of students. At the bachelor’s level, the need is about EUR 6,000/year/student and at the master’s level, EUR 9,000/year/student.

Increasing the admission of students to degree studies at universities and universities of applied sciences (universities +250, +555) requires an additional annual investment of approximately EUR 6 million.

In addition, additional resources are needed in vocational education and training, conversion and further training, and support for the third sector and other providers of cyber education and training for about EUR 2–3 million per year. It is essential to ensure the long-term sustainability of funding to enable training institutions to make long-term educational investments.

1 Foundations and starting points

1.1 Research on cybersecurity education

Research into cyber education, and in particular its requirements, is extensive across the globe. It is worth noting that international research has indicated a shortage of cyber experts. This naturally creates both qualitative and quantitative requirements for cyber education. Already in 2017, the European Cyber Security Organisation (ECSO) investigated this problem in Europe and summarised the results as follows: there is a skills shortage, cybersecurity training requires special adaptive training environments, training must be timely and consider both genders (it is well known that technical fields have more male than female students) (ECSO, 2017). ECSO has also produced a report on the skills required of cybersecurity professionals (ECSO, 2021). Academic research on the subject has also been carried out in Europe, and the results are very similar to those of the ECSO report (Blažič, 2021).

In addition to ECSO, the US National Institute of Standards and Technology (NIST) has published reports on cybersecurity skills. The NIST documents National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Newhouse et al., 2017) and Cybersecurity Workforce Framework (NICE Framework) (Petersen et al., 2020) provide a reference for the Knowledge, Skills, and Abilities (KSA) required for cybersecurity tasks. Other reference curricula on the topic include the following:

- Computing Curricula 2020 (CC, 2020); Provides a basis for academic study programmes in computing
- Cybersecurity Curricula 2017 (CSEC, 2017); Provides a standardised basis for cybersecurity study programmes

Guidelines for cybersecurity competence and training are provided by the following organisations, among others:

- Association for Computing Machinery (ACM)
- IEEE Computer Society (IEEE-CS)
- Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC)
- International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)

It should be noted that these documents are already some years old, and the field and its competence requirements are developing at an increasing pace.

The European Union Agency for Cybersecurity (ENISA) has published a report on addressing the skills shortage through higher education (ENISA, 2021). The report provides an overview of cybersecurity training provision in Europe by analysing the data collected and generated by the newly created Cybersecurity Higher Education Database (CyberHEAD). The report also illustrates the approaches adopted by EU Member States to increase and maintain the cybersecurity workforce. The above-mentioned approaches have been categorised and analysed on the basis of the objectives defined by ENISA's National Capabilities Assessment Framework (NCAF). These objectives are cybersecurity awareness, training, challenges, and exercises. The report (ENISA, 2021) also makes five recommendations for remedying the EU's cybersecurity skills shortage:

1. Add intake/enrolment and thus graduations to cybersecurity training programmes.
2. Support an integrated approach between government, industry, and universities.
3. Increase cooperation between Member States.
4. Analyse cybersecurity market needs and trends.
5. Support the use and promotion of CyberHEAD.

The International Information Systems Security Certification Consortium (ISC)[2] has published a study on the cybersecurity workforce. According to the study, 4.19 million people worldwide work in this field. Despite the large number of professionals working in cybersecurity globally, the shortage of cybersecurity professionals is approximately 2.72 million people. This also indicates the size of the national skills deficit and the training requirements. (See ISC2, 2021.)

1.2 Perspectives on cyber competence development

The resolution of the Finnish Ministry of Transport and Communications on the Cyber Security Development Programme on 10 June 2021 defines the key measures to improve cybersecurity throughout society. According to the resolution, high-level, national cybersecurity calls for necessary expertise, extensive participation across all levels of society, close cooperation between the public administration and business life, a strong domestic cybersecurity industry that will provide potential for ensuring the services in digital society, and cybersecurity capabilities in public institutions that will form the basis for the secure operation of the entire society.

A wide range of comments were given on the resolution, the most important of which are summarised here. The comments expressed concerns that Finland will not be able to adequately ensure the security of the services and information provided by our companies and public administrations unless a significant number of new professionals enter the field in the next few years. As cybersecurity and related security aspects become even more complex operating environments, this also requires a new kind of national training and education; it must develop to reflect the change taking place in the digital environment. The most important objective is to give priority to high-level expertise.

Developing high-level expertise is an important part of meeting future cybersecurity needs. Therefore, competence must be developed, and training opportunities expanded from the current level. In addition to professionals with high expertise, we also need practical training for citizens. In educating children and young people, attention should be paid to the development of citizens' basic skills in terms of information security, media literacy, and privacy. These basic skills will also improve national resilience.

In addition to the education system, organisations, and their contribution to the improvement of citizens' cybersecurity skills play an important role in competence development. It is therefore important to support cooperation with organisations that develop and assist the grassroots competences and activities of citizens and future experts. The problem is that there is a lack of an appropriate forum for planning and carrying out such cooperation, which is why such a forum should be established.

Cybersecurity education should be widely integrated into the degree programmes in technology. In addition, basic cybersecurity expertise should be included in all university degrees. This would also support the goal of increasing everyday cybersecurity expertise. Even a change at the level of legislation could be considered so that regulations on university degrees would include the basic skills required by the modern information society as a learning objective.

Systematic capacity building will create a solid basis for cybersecurity among different age groups and sections of the population. In addition, these skills enable the building of necessary technological cyber capabilities for the needs of both public authorities and companies. It is necessary to ensure that the competence needs of research, cybersecurity manufacturing industry, and cybersecurity user organisations are taken into account in all areas. Continuous dialogue with the working life on skills needs is a way of communicating about educational contents.

Degree studies do not provide sufficient competence in the field, and it is therefore necessary to rely on on-the-job training and further training to safeguard the skills of the workforce. Clearly, the workforce needs to learn more quickly and not all professional needs can be included in degree programmes. The duration of the degree programmes is long, and they change slowly. In any case, flexible forms of continuous learning will become more common in all sectors to support the skills needed in working life.

Improving citizens’ cyber skills through education is an important goal, which would strengthen Finland as a country of higher education and high competence and lay the foundations for future society. In addition to providing degree studies that support industry and society, Finland should invest in flexible continuing education and in courses and training that support lifelong learning.

The means described in the Cyber Security Development Programme to develop civic skills (including awareness of threats, media literacy) are good, as is their inclusion in the curriculum of primary and lower secondary education. Specific measures are also needed to reach those parts of the population that are not necessarily the primary target of cyber threats or attacks, but that will inevitably be affected by major crises.

Strengthening the knowledge base and improving the operating conditions of the cybersecurity industry are of paramount importance, not only from the point of view of industrial policy, but also from the point of view of national security. This means that significant additional investments must be made in Finland to increase cybersecurity education, to invest in it, and to launch research and development projects and bring their results to the market. The skills shortage already hampers the development of the sector and companies’ chances of success. The skills shortage in the cybersecurity sector will increase even more with major technological changes and digitization. Access to education must be increased both in working life and at different levels of education.

Another pathway in addition to degree programmes could also be apprenticeships and traineeship programmes that allow for specialisation in cybersecurity and learning through practical work. In addition to foreign specialists, younger foreign employees who are interested in the cybersecurity sector and who have been in the sector for a shorter time could also be attracted to Finland with various incentives. Establishing close links with national and international centres of excellence is important and requires planning and investments.

The prevention of cyber threats requires extensive cooperation. The main objective is to identify, prevent, and eliminate risk factors and situations that enable risks related to digital media. The involvement of citizens in preventive work is important and must be implemented in extensive cooperation with educational institutions, service providers, software developers, social media, researchers, lawyers, the police, social services, and other professionals working with children.

Every citizen, but especially children, has the right to information, safety skills, and guidance appropriate to their age and development. Children, young people, and adults should be educated about the dangers of the Internet. To develop cybersecurity, it is therefore important to produce educational material for all ages, which can be used to better illustrate the dangers of the Internet and the various forms and phenomena of cybercrime.

There is a need to ensure a sufficient number of professors and doctoral researchers in cybersecurity. Currently, research in this field is carried out in several universities, but the resources are insufficient. Attention should be paid to nation-wide education in the long term. In addition, the use of national expertise, as well as national and international cooperation, must continue to be actively pursued between public authorities and private actors (creating a functional cybersecurity ecosystem and utilising the cyber industry in public administration).

Cybersecurity expertise will be part of school education in the future. Communication about citizens' cybersecurity skills must be carried out through multiple channels and targeted at groups suffering from various functional limitations.

The assessment of citizens' cybersecurity skills should be included in national cybersecurity metrics. National cybersecurity capabilities are key and lay the foundations for cybersecurity in society as a whole. As part of the national cybersecurity capability, the prerequisites of municipalities as key actors in society must be ensured to achieve the desired capability. The development of industry-independent cybersecurity training, from basic education to university level, provides a strong basis for competence building. Supporting new business opportunities alongside training strengthens the development of the sector.

Changes in education and training are very important. They are needed for those working in the cybersecurity professions. Even more important may be ensuring, by means of training beginning in early childhood education, that all citizens understand the basics of cybersecurity and that those entering working life as well as the current workforce are able to understand the requirements of cybersecurity for their own work. For example, those working in service or product development need to know how cybersecurity should be taken into account in their field.

The development of national cybersecurity expertise requires the emergence of a sufficient centre of excellence. The creation of such a centre of excellence requires extensive national and international cooperation, as suggested in this report. Achieving international competitiveness requires high-quality students, researchers, and experts in the field to be brought to Finland. In order to develop cybersecurity, Finland must be seen as an attractive destination for international experts.

Domestic education must be developed and barriers to work-based migration dismantled, but in the short term we must focus on the barriers to the migration of international experts because it is a faster measure than the comprehensive development of the entire education system.

Cutting-edge expertise is needed in all areas of cybersecurity. However, there is no need to pursue the highest-level excellence in all areas. In order to succeed, top-level experts need the support of a workforce with solid skills, which also generates more top-level experts. Excellence can arise in other ways than through undergraduate and postgraduate studies. A professional having completed continuing education or conversion training may be a necessary specialist or a top-level expert because they combine cybersecurity competence with skills from another field. Such combining of activities and ICT competence is a central factor for success in cybersecurity. Three types of skills are needed:

1. Civic skills
   - What does everyone need to know about cybersecurity to live and function in the information society?
2. Basic field-specific skills
   - What cybersecurity skills are needed in different fields and professions?
3. Specialist skills
   - What are the general and field-specific competence requirements for cyber professionals?

There are not enough highly qualified cybersecurity experts available to meet the needs of Finnish society and the business sector. What is central is to train the most talented domestic and international students and support their integration into society and working life. Particularly strong support is needed for students who have graduated abroad to integrate in Finland.

ICT excellence will become a critical success factor for the future, and robust investments in education, research, and product development are needed to ensure excellence. At all levels of education, there is a need to teach more widely not only the safe use of information technology, but also its application and development. Diverse investments in ICT education beginning from basic education are essential for the future of Finland’s digital society as a whole.

However, several years of education do not solve the immediate skills shortage. The updating of previous skills to meet the current needs of working life must be ensured by flexible training solutions. Those already in working life must have the opportunity to move to areas where skills are needed through various forms of conversion training.

Cybersecurity education should be included in general training in technological fields, for example, as a minor subject, and industry needs will also need to be considered in educational planning. In addition to separate degree programmes, minor study modules, and other more extensive studies, the basics of cybersecurity must be included in all training and education in the field of technology. It is important that cybersecurity competence will not be overly concentrated in separate degree programmes. It is equally important that actors such as business management also have sufficient cybersecurity expertise, and training should be provided both in continuing education and in connection with training and education in other fields.

In terms of developing citizens' cybersecurity skills, it is important that cybersecurity is already included in the curriculum of early childhood education and basic education, and in a way that combines cybersecurity skills with other skills related to the digital environment.

Strong cybersecurity requires citizens to be able to identify and protect themselves from cyber threats, understand the meaning of their own actions, and report their findings to authorities when necessary. Organisations have a key role to play in identifying citizens' capacity to use digital services and equipment and in identifying the risks and procedures involved when problems arise. At the national level, up-to-date cybersecurity training is not consistent and does not reach everyone. We therefore have a large group of people relying on self-education and information search and being out of reach of available training and education.

When national defence is everyone's responsibility, so is cyber defence. The general improvement of cyber skills and the development of the cybersecurity education system also influence cyber defence: skills and abilities are increased on the daily front line through the improved expertise of citizens as well as through professionals or conscripts hired as top-level experts in cyber defence. Thus, the development of cyber competence in both civil life and national defence strongly supports each other.

New national cybersecurity products and services should be developed in Finland, and through them, expertise. This is measured directly by the number of patents and by turnover in the sector. If we operate exclusively with foreign information and security systems, we have transferred competence out of Finland and are unable to accumulate domestic competence. In addition, the lack of significant new developments means that new experts do not find their way to Finland.

The development programme has successfully highlighted the need to develop top-level expertise and suggested actionable measures. The mere inclusion of cybersecurity teaching in training and education in the field of technology will not be sufficient if the processing of personal data is not planned more extensively. In addition to secure cyber practices, the processing of citizens' personal data and the related rights should be more clearly included in education in order to make data protection and security a genuine civic skill.

References

Blažič, B. J. (2021). The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. Technology in Society 67, 101769. doi: https://doi.org/10.1016/j.techsoc.2021.101769.

CC (2020). Computing Curricula 2020 – CC2020: Paradigms for Future Computing Curricula (Draft, Version 36). https://cc2020.nsparc.msstate.edu/.

CSEC (2017). Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. ACM, IEEE, AIS, IFIP. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

ECSO (2017). Gaps in European Cyber Education and Professional Training. European Cyber Security Organisation (ECSO) https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf.

ECSO (2021). European Cybersecurity Education and Professional Training: Minimum Reference Curriculum. European Cyber Security Organisation (ECSO). https://www.ecs-org.eu/documents/publications/61967913d3f81.pdf.

ENISA (2021). Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

ISC2 (2021). A Resilient Cybersecurity Profession Charts the Path Forward. 2021 Cybersecurity Workforce Study, International Information Systems Security Certification Consortium (ISC)^2. https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

Newhouse, W., Keith, S., Scribner, B. & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/nist.sp.800-181. Withdrawn and superseded by Petersen et al. (2020).

Petersen, R., Santos, D., Wetzel, K. A., Smith, M. C. & Witte, G. (2020). Workforce Framework for Cybersecurity (NICE Framework). National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.SP.800-181r1.

2 Cybersecurity education in primary and lower secondary schools

2.1 Previous research in information security competence in primary and lower secondary education

The need for information security expertise in schools is well known. ICT skills are included in curricula, and the Finnish National Board of Education has stated that the increasing use of information technology will bring about new risks that need to be taken into account (Opetushallitus, 2021). The aim is to develop research and methods so that they are interesting and learnable for children.

The competence of teaching staff in teaching digital safety has been studied by Koivula and Mustola (2017) in the early childhood education environment. According to their research, the skills in teaching digital safety at this level are poor. Children often know how to use digital devices better than adults, and there is no actual pedagogical education in the topic at all. The research by Tekerek and Tekerek (2019) also supports the idea that children are more skilled than adults in using devices.

Kosonen's (2019) study on the ICT competence of fifth and sixth graders in Lahti showed that children have deficiencies in information security management. According to the study, children share contact information and user account information with each other. On the other hand, children's self-assessments show that they consider passwords to be secure and do not share them with others. According to the study, there is also room for improvement in the distribution of material, and children do not understand what kind of images are suitable for sharing on the Internet.

A Turkish study of primary school pupils' knowledge of information security showed that their understanding of the basics was low (Tekerek & Tekerek, 2017). According to the study, this can be seen in weak passwords, lack of secure communication, unprotected documents, and lack of critical thinking when getting to know people online. The study indicates an increased need for training and education in digital security.

A study conducted in Russia by Bocharov, Mozharov, and Simonova (2019) examined how children in pre-primary education understand information security. The study states that teachers should organise simulated situations of cybersecurity threats and discuss them afterwards with the pupils. In the study, the response to different threats was clearly improved after training. The study by Bocharov et al. (2019) also states that when children reach school age, their parents' influence decreases as the children's independence increases. The phenomenon can be clearly observed in Finland when children begin to go to school independently instead of their parents taking them to day care or pre-school.

According to Bocharov et al. (2019), systematic information security training and education are needed for children already in primary school, and children should learn critical thinking in information search, identification of information security threats, and decision-making in risk situations. Teaching should also aim to increase students' motivation to take information security into account when working in different digital environments.

Madetoja (2021) has investigated what methods of verification are used by pupils in Finnish primary and lower secondary schools and has considered the position of children as users of digital environments. The results of the study correspond to the findings of Tekerek and Tekerek (2017). Children lack an understanding of how to protect their privacy in the digital world, and they choose passwords in a way that relates to their own life and are therefore easily deduced.

To summarise, many studies show that children's understanding of digital safety remains lacking. The challenge is known, and solutions are being developed. One solution would be to increase systematic cybersecurity/information security education.

2.2 Situation in primary and lower secondary schools

To support the implementation of the early childhood education plan and the curricula for pre-primary and basic education, the Ministry of Education and Culture launched the *New Literacy* development programme in 2020. The aim of the programme is to develop the teaching of ICT skills, media literacy, and programming skills. During the first year, the development programme prepared descriptions for the demonstration of ICT skills, media literacy skills, and programming skills, separately for each grade in basic education. Correspondingly, descriptions of pedagogical best practices for these skills have been prepared for early childhood education and pre-primary education. The descriptions were published on 16 February 2021 on the website of the development programme (uudetlukutaidot.fi, only in Finnish and Swedish). The descriptions are based on national core curricula and include information security competence. The objectives of the programme for the years 2021–2022 are to support the use of these descriptions in early childhood education and teaching and to produce materials and digital content that facilitates teaching and learning these contents. The **New Literacy** development programme is part of the **Right to Learn** programme.

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.

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. The way students will use their knowledge and skills is influenced by the values and attitudes they have adopted and their willingness to take action. The increased need for transversal competence arises from changes in the surrounding world. Competences that cross the boundaries of and link different fields of knowledge and skills are a precondition for personal growth, studying, work, and civic activity now and in the future. (See Opetushallitus, 2014.)

Values, the conception of learning, and the school culture lay the foundation for the development of competence. Each subject builds the pupil's competence through the contents and methods typical of its field of knowledge. Competence development is influenced not only by the contents on which the pupils work but also, and especially, by how they work and how the interaction between the learner and the environment functions. Feedback given to the pupils as well as guidance and support for learning influence attitudes, motivation, and willingness to act.

Learning modules are frequently interconnected. Their joint objective is, in line with the mission of basic education and taking the pupils' age into account, to support growth as a human being and to impart competences required for membership in a democratic society and a sustainable way of living. It is particularly vital to encourage the pupils to recognise their uniqueness and their personal strengths and development potential, and to appreciate themselves.

The areas of transversal competence are presented as follows:

Thinking and learning to learn (T1)

Thinking and learning skills underlie the development of other competences and lifelong learning. The way in which the pupils see themselves as learners and interact with their environment influences their thinking and learning. The way in which they learn to make observations and to search for, evaluate, edit, produce, and share information and ideas is also essential. The pupils are guided to realise that information may be constructed in many ways, for example, by conscious reasoning or intuitively, based on personal experience. An exploratory and creative working approach, doing things together, and possibilities for focusing and concentration promote the development of thinking and learning to learn. The pupils are supported in laying a good foundation of knowledge and skills and developing an enduring motivation for further studies and lifelong learning.

Cultural competence, interaction, and self-expression (T2)

Pupils in basic education are guided in recognising and appreciating cultural meanings in their environment and building a personal cultural identity and a positive relationship with the environment. The pupils learn to know and appreciate their living environment and its cultural heritage as well as their personal social, cultural, religious, philosophical, and linguistic roots. They are encouraged to consider the significance of their own background and their place in the chain of generations. The pupils are guided to consider cultural diversity as a fundamentally positive resource. They are also supported to recognise how cultures, religions, and philosophies exert influence in society and daily life and how the media shapes culture, and also to consider what is unacceptable as a violation of human rights.

Taking care of oneself and managing daily life (T3)

The pupils are encouraged to take care of themselves and others, to practice skills that are important for managing their daily lives, and to work for the well-being of their environment. During their years in basic education, the pupils learn to know and understand the significance of factors that promote or undermine well-being and health and the significance of safety, and to find information related to these areas. They also learn time management, which is an important part of daily life management and self-regulation. In instruction, the versatility of technology is examined, and the pupils are guided to understand its operating principles and cost formation. In basic education, the pupils are guided in using technology responsibly and invited to consider ethical questions related to it.

Multiliteracy (T4)

Multiliteracy is the competence to interpret, produce, and make a value judgement on a variety of different texts, which will help pupils to understand diverse modes of cultural communication and to build their personal identity. Pupils need multiliteracy to interpret the world around them and to perceive its cultural diversity. Multiliteracy means abilities to obtain, combine, modify, produce, present, and evaluate information in different modes, in different environments and situations, and by using various tools. Multiliteracy supports the development of critical thinking and learning skills. The pupils must have opportunities to practice their skills both in traditional learning environments and in digital environments that exploit technology in different ways.

ICT competence (T5)

Competence in information and communication technology (ICT) is an important civic skill both in itself and as part of multiliteracy. It is an object and a tool of learning. Basic education ensures that all pupils have possibilities for developing their ICT competences. ICT is methodically exploited in all grades of basic education, in different subjects and multidisciplinary learning modules, and in other schoolwork.

Working life competence and entrepreneurship (T6)

Working life, occupations, and the nature of work are changing because of drivers as technological advancement and globalisation of the economy. Anticipating the requirements of work is more difficult than before. Basic education must impart general capabilities that promote interest in and a positive attitude towards work and working life. It is important for the pupils to obtain experiences that help them understand the importance of work and enterprising, the potential of entrepreneurship, and their personal responsibility as members of their community and society. In schoolwork, the pupils learn teamwork, project work, and networking.

Participation, involvement, and building a sustainable future (T7)

Participating in civic activity is a basic precondition for an effective democracy. Basic education creates the foundation for the pupils' interest in the school community and society. The pupils take part in planning, implementing, assessing, and evaluating their own learning, joint schoolwork, and the learning environment. They gather knowledge and experiences of the systems and methods for participation and involvement in civic society and communal work outside the school. They are guided to understand the significance of their choices, way of living, and actions not only to themselves but also to their local environment, society, and nature.

2.3 Content of transversal competence in information and communication technology (T5)

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:

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.

In the following, the 2nd main area, which focuses on the safe and responsible use of ICT, is presented by grade:

- 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. (See Opetushallitus, 2014.)

2.4 Analysis of the survey of schools

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. The cover letter asked for the survey link to be sent to teachers at the addressed school who teach information technology or whose work involves information security. A total of 108 responses were received (see Figure 1).

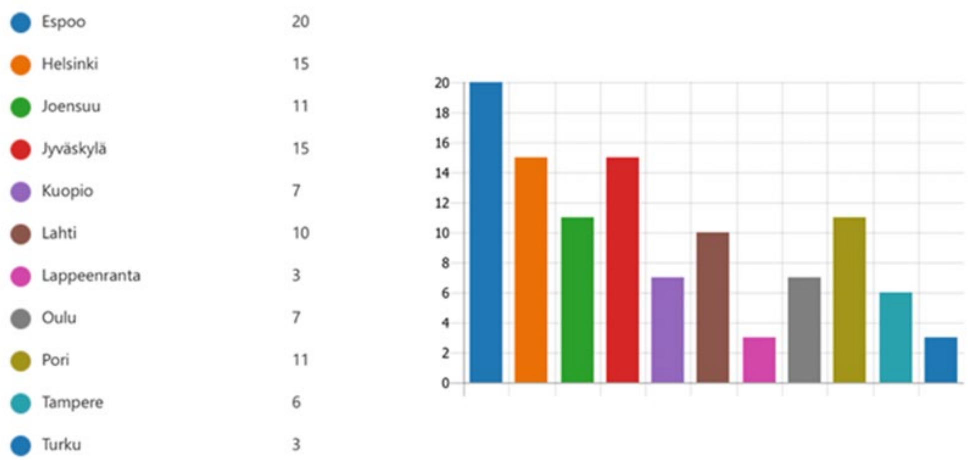


FIGURE 1. Number of survey respondents by town

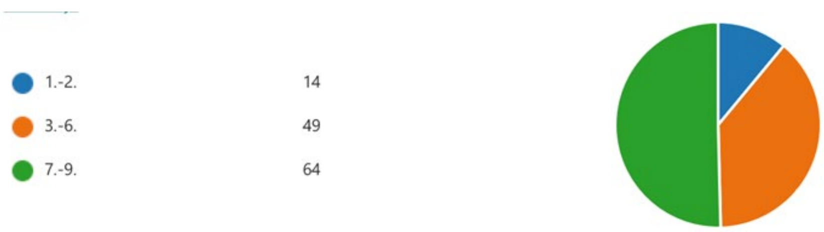


FIGURE 2. Distribution by grades taught

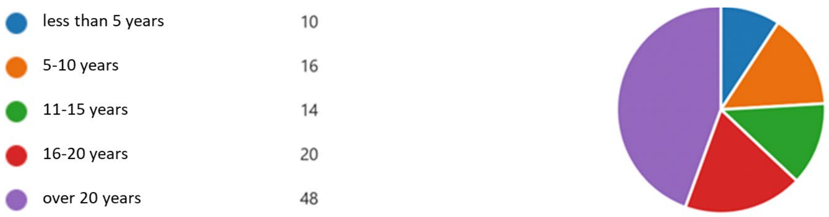


FIGURE 3. Years of teaching experience

Most responses to the question of which grade the respondent taught came from teachers of grades 7 to 9, second most from teachers of grades 3 to 6, and fewest from teachers of grades 1 to 2. It should be noted that only four teachers exclusively selected grades 1 to 2; in other words, the majority also teach older grades. The distribution is shown in Figure 2. Most responses (n = 48) to the question about teaching experience came from teachers with more than 20 years of teaching experience and the fewest responses (10) from teachers with less than 5 years of experience (see Figure 3).

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 4.

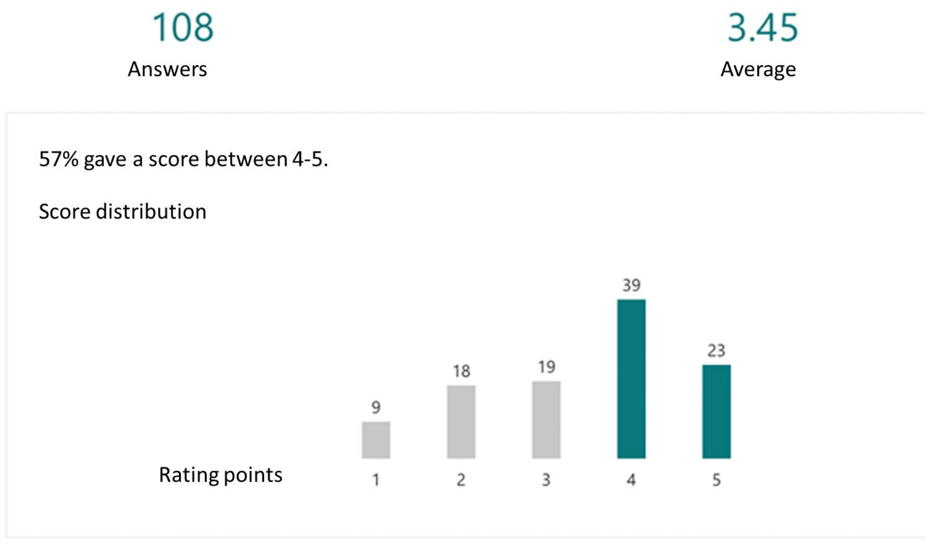


FIGURE 4. Inclusion of cybersecurity education in teachers' own subject.

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. 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. The majority of teachers in favour of separate cybersecurity education teach grades 7 to 9, which is in line with the answers to the previous question regarding the inclusion of cybersecurity education in teachers' own subject. Secondary school teachers may find it more difficult to include cybersecurity in a particular subject, while in primary school it may be easier since one teacher tends to teach more than one subject to the same class by default.

The survey examined whether primary and lower secondary schools have appointed a person responsible for information security, who ensures the information security skills and the secure behaviour of school staff and pupils. Teachers were asked to respond on a scale of 1 to 5 (fully disagree to fully agree). The answers averaged 2.9 and were very evenly distributed across the scale. The result indicates that the respondents found it difficult to clearly identify a person responsible for data security or that more than one person is responsible for the matter.

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.

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 options were the following:

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

- Grades 3 to 6: the pupils are guided in responsible and safe use of ICT, good manners, and knowledge of basic copyright principles.
- Grades 7 to 9: the pupils are guided to the safe and ethically sustainable use of ICT. They learn how to protect themselves from possible information security risks and how to avoid losing data. They learn, for example, the meaning of the concepts of information protection and copyrights and the potential repercussions of irresponsible and illegal activities.

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 5).

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 6). 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.

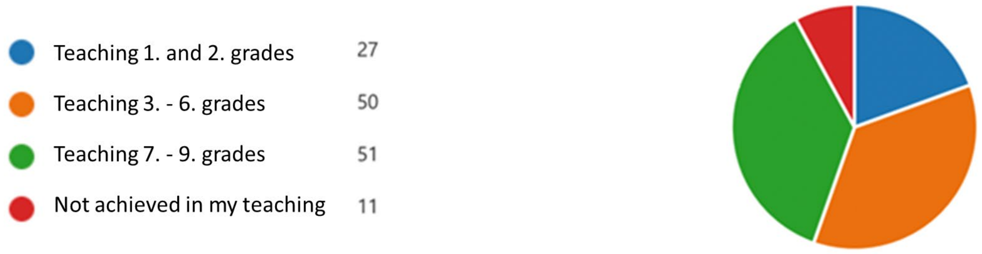


FIGURE 5. Objectives of secure use ICT in the curriculum by grade

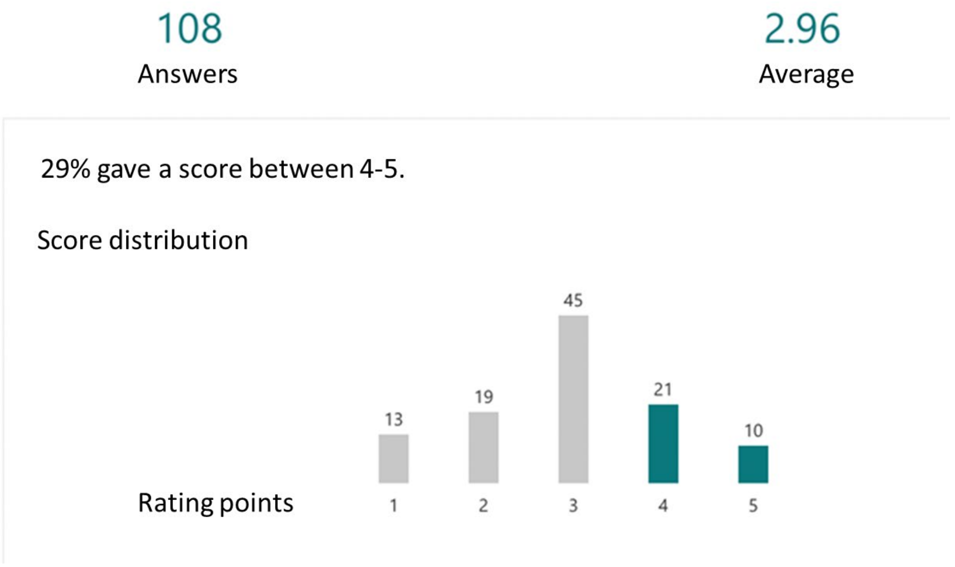


FIGURE 6. Curriculum guidelines for cybersecurity teaching

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 7 presents the teachers' view of their ability to teach cybersecurity.

The availability of on-the-job training related to cybersecurity was viewed in a relatively neutral way. The assessment was carried out on a scale of 1 to 5 (fully disagree to fully agree), and the average was 2.94. Of the teachers whose responses ranged between 1 and 2 (n = 34), that is, who feel that the availability of continuing education is poor, about 60% teach grades 7 to 9 (see Figure 8). Examining the answers to the various options on the scale does not reveal a certain age group that would find the availability of continuing training to be particularly poor or, accordingly, particularly good; the differences derive from the grades that the teachers teach.

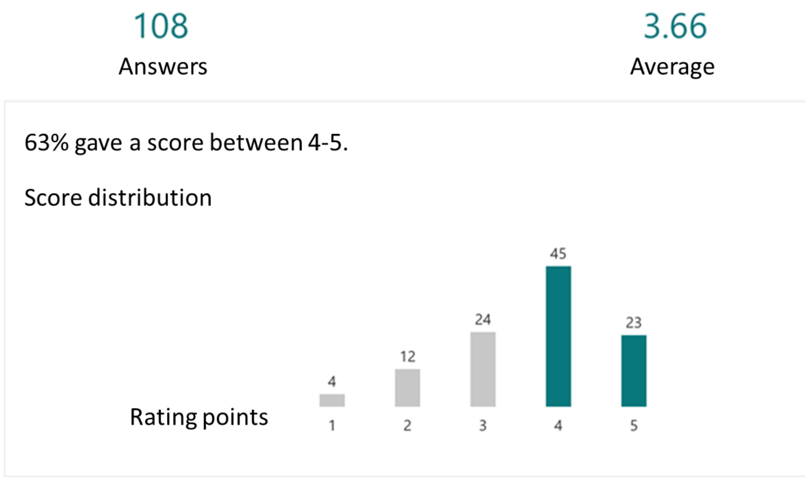


FIGURE 7. Teachers' self-assessment of their competence

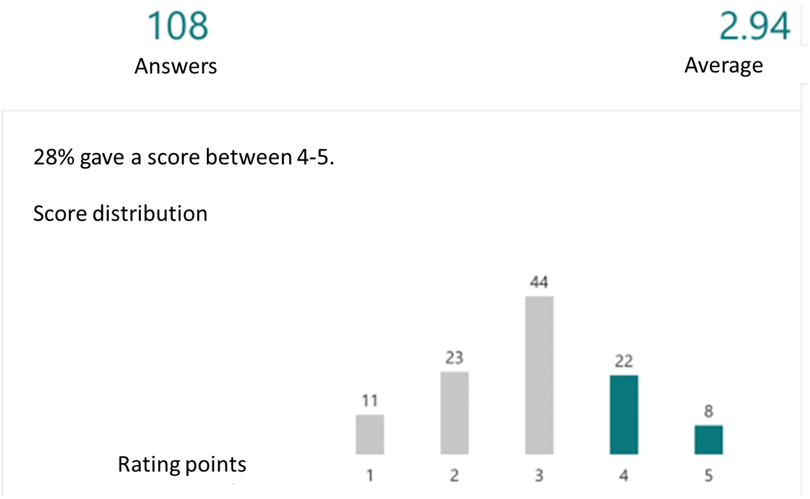


FIGURE 8. Availability of continuing education

2.5 Development of digital safety education in basic education

2.5.1 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.

Koskinen's study in 2009 showed, among other issues, that there are shortcomings in children's ability to identify material that is suitable for sharing. These challenges remain even today. The channels of communication and risks are constantly increasing, which is why it is very important that the challenge is met effectively throughout children's lives.

2.5.2 Conclusions of the survey

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. In this solution, the areas of transversal competence would be the following:

- Thinking and learning to learn (T1)
- Cultural competence, interaction, and self-expression (T2)
- Taking care of oneself and managing daily life (T3)
- Multiliteracy (T4)
- ICT competence (T5)
- Working life competence and entrepreneurship (T6)
- Participation, involvement, and building a sustainable future (T7)
- **Digital security (T8)**

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 (T5).

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. In this development plan, it would be important to pay attention to the following matters:

- In comprehensive school, it would be possible/mandatory to study ICT for a certain number of hours per week, and this teaching would also cover digital security to a greater extent than before.
- Teachers must have better opportunities to train as teachers of ICT; this also requires a reform of the educational content from the organiser of the training.
- Continuing education should also address digital security and its teaching.
- In addition, one line of development is to explore the possibility of increasing the emphasis on ICT in Finnish primary schools.

References

Bocharov, M. I., Mozharov, M. S. & Simonova, I. V. (2019). Systematic information security training in elementary school. In *Proceedings of the International Scientific and Practical Conference on Digital Economy (ISCDE 2019)*. Atlantis Press, pp. 600-605.

Eu, Z., Lim, S., Chong, K., Ting, T. & Tan, L. (2021). Information Security Awareness. Retrieved from: https://www.researchgate.net/publication/355663812 .

Jyväskylän kaupunki (2016). Jyväskylän perusopetuksen opetussuunnitelma: Tieto- ja viestintäteknologia. https://peda.net/opetussuunnitelma/ksops/jyvaskyla/luku12/12-22/tjv

Kaikkien kaupunkien opetussuunnitelmat.

Koivula, M. & Mustola, M. (2017). Digiloikka ja ei-kenenkään-alue varhaiskasvatuksessa. Retrieved from: https://jyx.jyu.fi/bitstream/handle/123456789/53753/koivula-mustoladigiloikka.pdf?sequence=1&isAllowed=y .

Lahden kaupunki (2016). Lahden kaupungin perusopetuksen opetussuunnitelma. *https://eperusteet.opintopolku.fi/-/fi/ops/54589/perusopetus/valinnaisetoppiaineet/11020123*

Lappeenrannan kaupunki (2016). Kesämäen koulu: Valinnaisaineet luokilla 7-9. https://www.kesamaenkoulu.fi/opiskelu/valinnaisaineet/valinnaisaineet-luokilla-7-9/

Madetoja, A. (2021). Tapaustutkimus perusopetusoppilaiden todentamismenetelmistä. Pro gradu -tutkielma, Jyväskylän yliopisto. Retrieved from: https://jyx.jyu.fi/handle/123456789/76525 .

Opetushallitus (2014). Perusopetuksen opetussuunnitelman perusteet 2014. *https://www.oph.fi/sites/default/files/documents/perusopetuksen_opetussuunnitelman_perusteet_2014.pdf*

Opetushallitus (2021a). Opetustoimen ja varhaiskasvatuksen turvallisuus. Retrieved from: https://www.oph.fi/fi/koulutus-ja-tutkinnot/opetustoimen-ja-varhaiskasvatuksen-turvallisuus .

Opetushallitus (2021b). Tieto- ja viestintäteknologinen osaaminen. *https://uudetlukutaidot.fi/wp-content/uploads/2021/03/Versio-1-Tieto-ja-viestintateknologinen-osaaminen-suomi.pdf*

Opetushallitus (2021c). Tietoturva ja -suoja koulussa. Retrieved from: https://www.oph.fi/fi/koulutus-ja-tutkinnot/tietoturva-ja-suoja-koulussa .

Oulun kaupunki (2015). Oulun kaupungin perusopetuksen opetussuunnitelman perusteet 2014 ja Oulun kaupungin paikalliset linjaukset.

https://eperusteet.opintopolku.fi/-/fi/ops/20650/perusopetus/valinnaisetoppiaineet/10612244

Paananen, R. (2021). Kyberturvallisuuden kehittämisohjelma. Liikenne- ja viestintäministeriö, Helsinki. *https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163219/LVM_2021_7.pdf?sequence=1&isAllowed=y*

Tekeret, M. & Tekerek, A. (2017). A research on students' information security awareness. *Turkish Journal of Education,* 2(3), 61-70.

Turvallisuuskomitea (2019). Suomen kyberturvallisuusstrategia. Retrieved from: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf .

Welling, A. (2020). Mietityttääkö lastesi tietoturva? Alakoululaisille tarkoitettu mobiilipeli opettaa, miten vastata häirikölle netissä. Retrieved from: https://yle.fi/uutiset/3-11179317 .

3 Cybersecurity education in general upper secondary school

3.1 General upper secondary school curriculum

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 (Opetushallitus 2019, 9).

The objective of the general upper secondary education reform is to improve the population's level of education in order to optimise Finland's potential for success in the decades to come. The aim is to increase the proportion of those with higher education, among the age class 25 to 34, from 41% at the time the Act was drafted to 50%. The reform aims to increase the attraction of general upper secondary schools as a form of education that provides general knowledge and ability and eligibility for further studies at higher education institutions. It also aims to improve the quality of education and learning outcomes and to facilitate the transition from secondary education to higher education. Key means for achieving these objectives include more individual and flexible study paths, provision of the guidance and support students need to follow such paths, interdisciplinary studies, and cooperation with higher education institutions. (See Opetushallitus 2019, 9.)

General upper secondary education promotes both the command of the various subjects' objectives and key contents and develops transversal competences. The components of transversal competence comprise the common objectives of all subjects:

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

Transversal competences help the students apply in practice the knowledge and skills they learn while studying the various subjects. Transversal competences refer to cognitive skills and meta skills that lay the foundation for learning and competence as well as the kind of attributes the students need in their studies, work, hobbies, and daily life. They also create the preconditions for acquiring the knowledge and skills which enable the students to cope with change in an increasingly digital and complex world. (See Opetushallitus 2019, 9–10.)

In the new national core curriculum, compulsory studies and national optional studies have been structured as modules for which one to three are awarded. These modules are used locally to put together either subject-specific or interdisciplinary study units. The scopes and forms of these study units, which replace the courses of the old system, may vary. (See Opetushallitus 2019, 10.)

3.2 Objectives of general upper secondary education

The objective is to promote students' well-being and provide them with better support in their studies. In the school culture of general upper secondary schools, more emphasis will be placed on the students' participation, cooperation, togetherness, and diversity while also addressing their individual needs. The student-centred nature and individualisation of general upper secondary school studies will be enhanced, improving study motivation and the meaningfulness of studies. (See Opetushallitus, 2019, 10.)

All providers of general upper secondary education for young people prepare a local curriculum based on the national core curriculum for general upper secondary education unless otherwise stated in an authorisation granted by the Ministry of Education and Culture. In addition, if the authorisation includes a special educational task, the regulations related to it must be taken into account when preparing the curriculum. The local curriculum determines how the teaching and education of the general upper secondary school(s) concerned are delivered. Based on the curriculum adopted by it, each education provider draws up a plan for the practical organisation of education for each school year. When preparing the local curriculum, the education offered at other educational institutions as well as the operating environment of the general upper secondary school, local strengths, and special resources should be taken into account. The local or regional nature and environment, history, linguistic conditions, and the economic and cultural life around the general upper secondary school add local colour to the curriculum. In addition, practical cooperation with experts in different fields increases the realistic nature and authenticity of studies. Drawing up the local curriculum makes it possible to embed current interpretations of the contents of the core curriculum. The education provider decides how to draw up the local curriculum based on the criteria of the upper secondary school curriculum. The local curriculum is prepared in cooperation with the general upper secondary school's staff, students, students' guardians as well as the authorities responsible for implementing the municipality's social and health care services to the extent required under the legislation. General upper secondary schools may also cooperate with other education providers and different stakeholders when preparing the curriculum. Through this cooperation, an effort is made to ensure the high standard of general upper secondary education, its relevance to society, and the commitment of the entire community to jointly determined objectives and procedures. (See Opetushallitus 2019, 13–14.)

The national core curriculum specifies the mission of general upper secondary education. One part of the mission is to strengthen transversal general knowledge and ability. In this context, general knowledge and ability consist of values, knowledge, skills, attitudes, and will which allow individuals capable of critical and independent thinking to act in a compassionate and responsible manner and engage in self-development. In addition, during the years spent in general upper secondary education, the students build their essential knowledge, agency, and competence related to people, cultures, society, and the environment. The aim of the education is also to prepare the students to understand the complex interdependencies prevalent in life and the world as well as to analyse extensive phenomena. (See Opetushallitus, 2019, 16.)

Teaching and educational tasks are an integral part of general upper secondary education. During their studies, students build their perception of humanity, identity, worldview, and philosophy of life as well as find their place in the world. At the same time, the students develop their relationship with the past and look to the future. General upper secondary education also develops students' capabilities for life management and working life skills and advances their interest in the world of sciences and the arts. General upper secondary education guides the students towards drawing up plans for the future, growing into global citizens, and continuous learning. (See Opetushallitus, 2019, 16.)

3.3 General objectives of instruction in general upper secondary education

The national core curriculum for general upper secondary education states that "Education and other activities in general upper secondary schools must be organised in accordance with the general national objectives defined in the Government Decree on General Upper Secondary Education (810/2018)" (Opetushallitus 2019, 58).

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. (See Opetushallitus, 2019, 58.)

During their studies, the students gather diverse experiences of building new knowledge and ability, extensively and crossing the boundaries of individual subjects. The students develop their capabilities for acquiring and applying information, and their problem-solving skills. They gather experiences of inquiry-based learning and participation in conducting science and research. The instruction also aims to reinforce the students' multiliteracy, allowing them to understand the language typical for different fields of science and arts as well as motivating them to examine, interpret, and produce different texts. 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. (See Opetushallitus 2019, 58.)

3.4 Transversal competences

The key task of transversal competences is to provide an integrative element to the general upper secondary studies. The areas of transversal competences comprise the common objectives of the general upper secondary school subjects (Opetushallitus, 2019, 60). The objectives of the transversal competences are the following:

- A good overall knowledge and skills base
- Building a sustainable future
- A readiness to move on to continued studies, the working life, and the internationalised world

At the centre of transversal competences is a good, balanced, and civilised human being. The transversal competences consist of six areas. The curriculum states:

> The underlying values, conception of learning, and school culture of general upper secondary education lay the foundation for the development of transversal competences. Achieving the objectives of the transversal competence areas is the aim of all general upper secondary studies. Each subject approaches the transversal competences from the starting points of its own fields of knowledge and science. Transversal competences are a key part of both subject-specific studies and those integrating the different subjects. (Opetushallitus, 2019, 61)

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 familiarisation 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 (see Opetushallitus, 2019, 61–62):

- Global and cultural competence
  - International competences and a global citizen’s disposition
  - Knowledge of Finnish, European, and global heritage, and appreciation of cultural diversity
  - Ethical agency in the globalised spheres of media and technology
- Well-being competence
  - Caring for oneself and others
  - Recognition and utilisation of own strengths and identity construction
  - Grit and resilience in a world of change and surprises
- Interaction competence
  - Emotional and empathy skills
  - Social and collaboration skills and collaborative learning skills
  - Language awareness and constructive communication skills
- Multidisciplinary and creative competence
  - Curiosity and motivation to learn, to find meanings and to combine things in new ways
  - Self-regulated learning, factual criticism, and continuous development of learning-to-learn skills
  - Multiliteracy in the digital era
- Societal competence
  - Democracy skills, influencing for a safe, just, and sustainable future
  - Using competences for one’s own benefit and for the benefit of society
  - Ability to transform as regards life in general, and the world of work; an entrepreneurial disposition
- Ethical and environmental competence
  - Value-based and ethical action for the common good
  - Appreciation of the diversity of nature and research-based climate action
  - Appreciation of circular economy and sustainable consumerism

3.5 Survey results

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.

Most responses were given by teachers of mathematics (n = 17) and the fewest came from teachers of physical education (n = 1), philosophy (n = 1), worldview studies (n = 1), and the visual arts (n = 0). Several teachers reported teaching more than one subject. Figure 9 presents the subjects taught by the teachers.

The survey asked whether the respondents teach information and communication technology in their school. Thirteen of the teachers who responded to the survey reported teaching ICT (see Figure 10).

Of the ICT teachers, 10 include cybersecurity and information security studies in their teaching. In contrast, three teachers stated that they do not include cybersecurity education in their ICT education (see Figure 11).

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. There was significant dispersion between the responses. The teachers whose responses ranged between 4 and 5 represent a number of different subjects. Apart from ICT, the data does not lend itself to the conclusion that representatives of a particular subject would include significantly more cybersecurity education than others. The teachers whose responses ranged between 1 and 2 also represent a number of different subjects (see Figure 12).

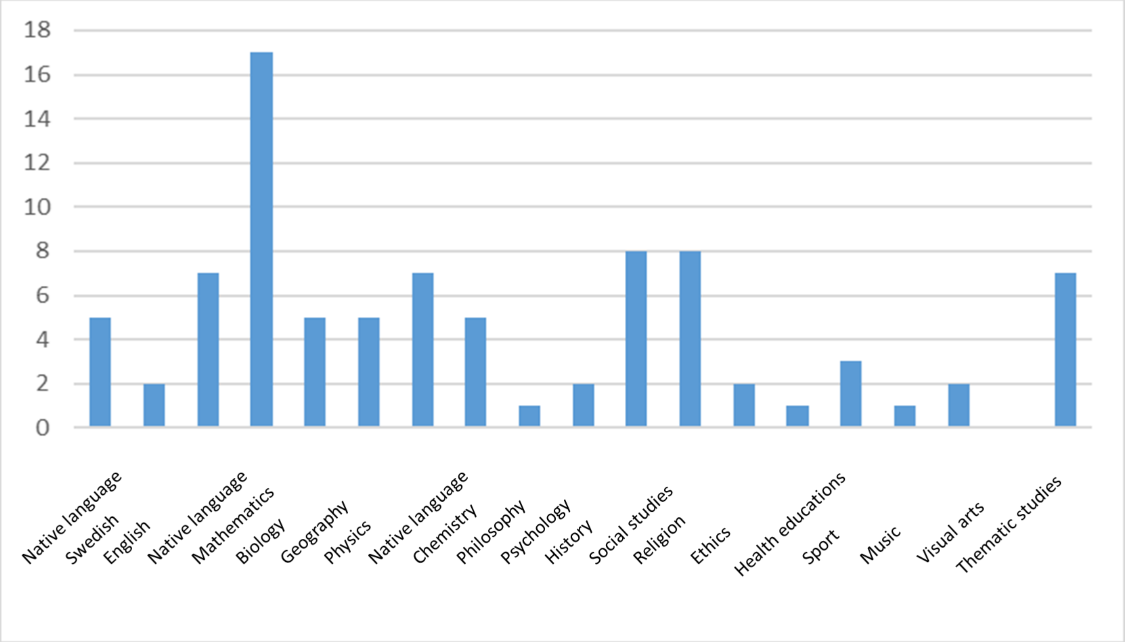


FIGURE 9. Subjects taught by the responding teachers

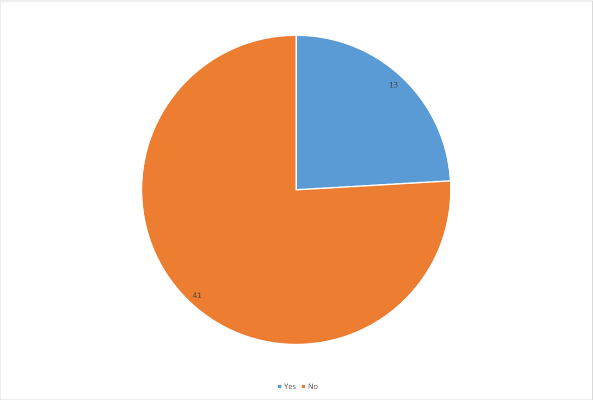


FIGURE 10. Number of ICT teachers in the sample

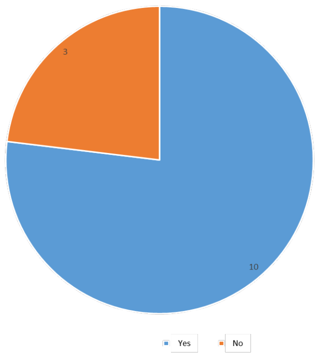


FIGURE 11. Cybersecurity education in ICT education

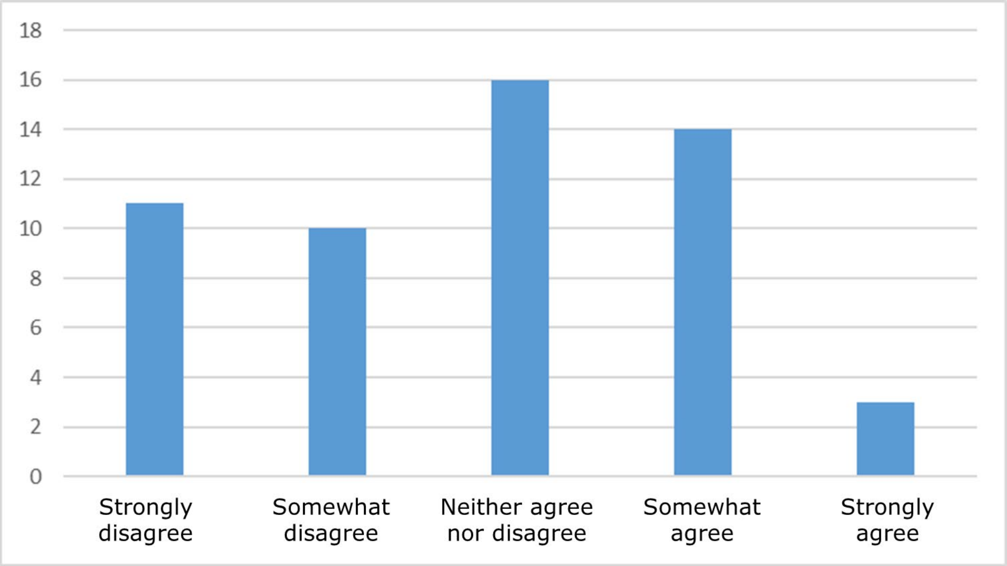


FIGURE 12. Inclusion of cybersecurity education in subject teaching

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. Five ICT teachers thought that cybersecurity education should in some way be included in each subject, while seven thought that it would be more sensible to differentiate cybersecurity education, for example, into IT education. Taken together, the majority of all respondents thought that cybersecurity belongs to all areas of the general upper secondary school. Figure 13 presents teachers' views on the inclusion of cybersecurity education in each subject.

The survey also examined whether general upper secondary schools have appointed a person responsible for information security who ensures the information security skills and the secure behaviour of school staff and students. The results show that there are significant differences between general upper secondary schools (see Figure 14).

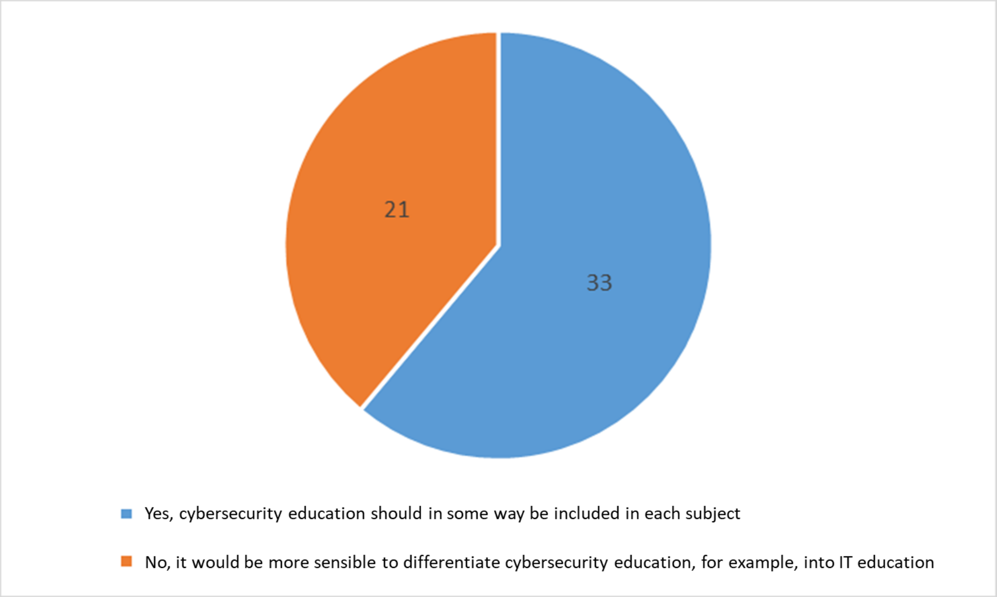


FIGURE 13. Inclusion of cybersecurity education in subject teaching

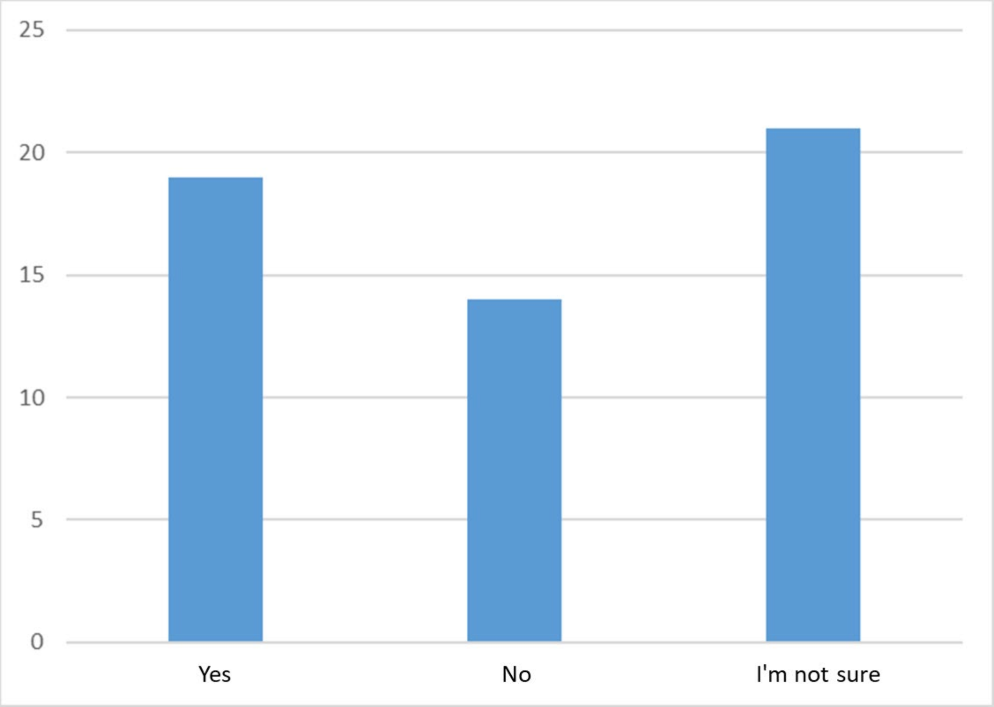


FIGURE 14. Person responsible for information security in the school

Teachers were asked to assess students' 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. The average was 3.05 (see Figure 15). The results indicate that, on average, the respondents are fairly neutral towards teachers' and students' knowledge of the secure use of equipment and study-related services.

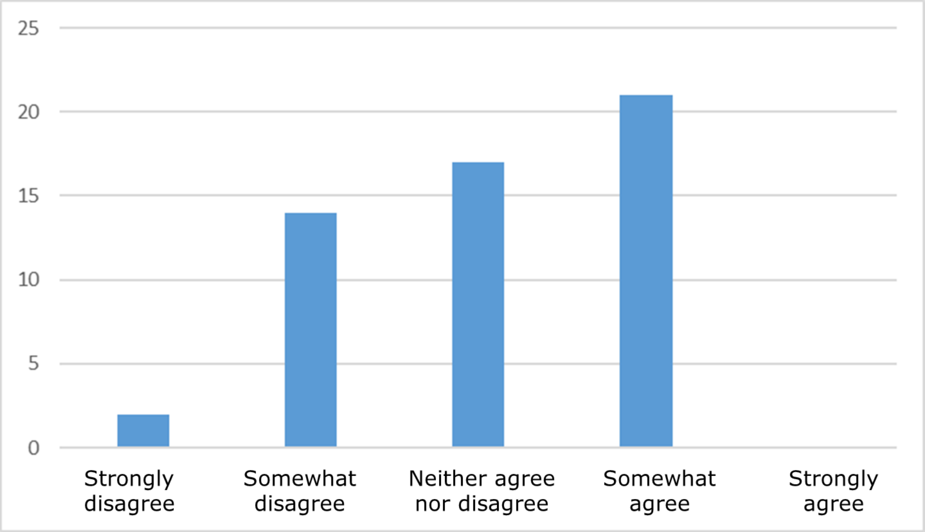


FIGURE 15. Cybersecurity competence of students and teachers

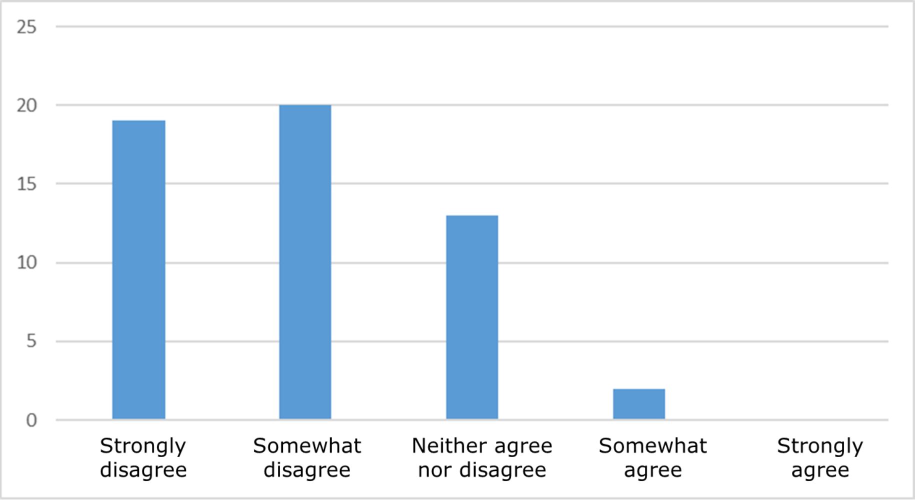


FIGURE 16. The clarity of the curriculum guidelines regarding cybersecurity teaching

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 16). 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.

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. Those rating their skills between 4 and 5 (n = 18) include eight respondents whose teaching includes ICT. The teachers whose responses ranged between 4 and 5 also represent a number of different towns and subjects. The most common subjects among these teachers are mathematics, history, social sciences, and physics, but also subjects such as biology, geography, music, and health education were included in the subjects taught by these teachers. The teachers whose responses ranged between 1 and 2 also represent a number of different towns and subjects (see Figure 17).

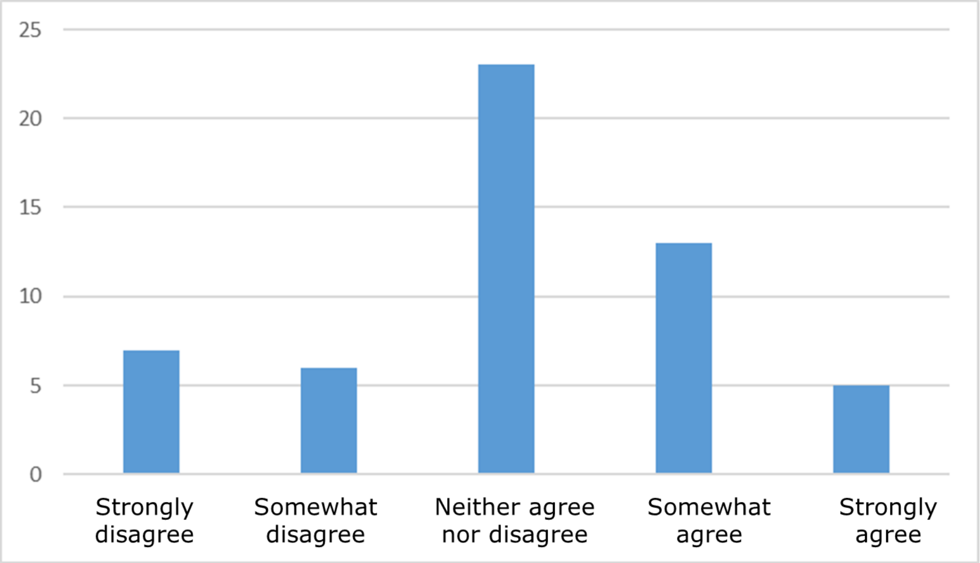


FIGURE 17. The level of knowledge and competence of teachers in cybersecurity teaching

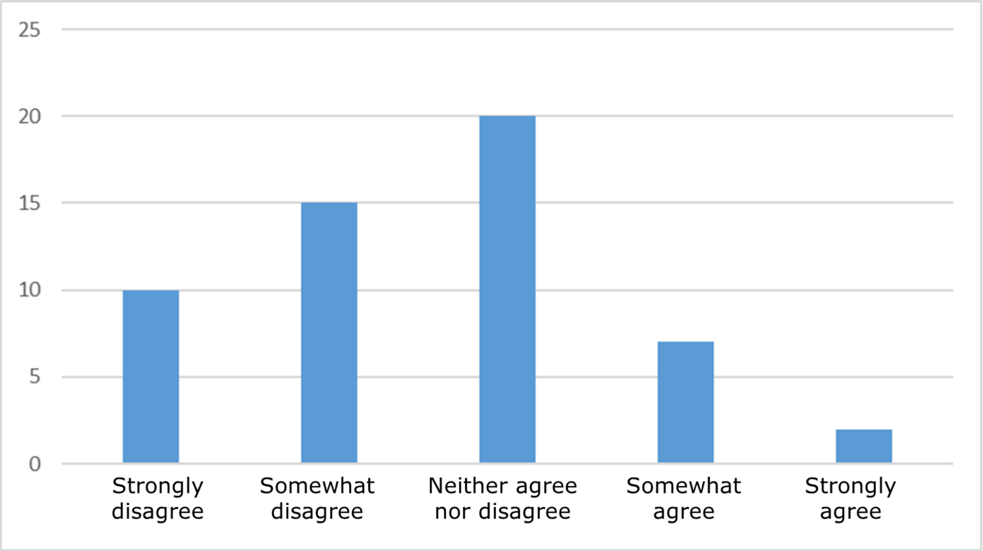


FIGURE 18. Availability of continuing education

The availability of continuing education in cybersecurity was viewed with reservations. The assessment was carried out on a scale of 1 to 5. The average score was 2.55. The nine teachers who answered between 4 and 5 represent six different towns and several different subjects. Of these nine, four also teach ICT among other subjects. The data does not show that teachers in a particular town would feel that continuing education is more accessible than average. In addition, teachers whose assessment ranged between 1 and 2 represent several different towns and disciplines (see Figure 18).

3.6 Examples by subject

The teachers had the opportunity to explain in more detail how cybersecurity is visible in their teaching. The list below presents the examples given by the teachers. The results show that cybersecurity education is included in many different subjects and courses although the curriculum does not take a clear stand on cybersecurity / information security / digital security and their teaching at the level of individual subjects. Some of the responses also illustrate that not all teachers feel that cybersecurity and its teaching are directly relevant to them or even entirely necessary.

History and social studies

“Topics such as cyber threats, cybersecurity, and hybrid warfare are discussed as part of social studies. Communication, media and source criticism, copyright, etc.”

“I include the topic in discussions about the problems of the modern world from a historical point of view and when talking about Cold War espionage, which I compare to the current situation. I strive to keep my educational content up to date and provide examples with recent articles and materials. I also instruct students in the use of the Internet as a source of information and, for example, in copyright / plagiarism issues / source-critical information search; this also includes a significant part of the reflection on data security topics.”

“As a teacher of social studies, I include cybersecurity at both the institutional and the individual level in the security policy theme of the YH3 course. For example, I often show short episodes of the Finnish series *Team Whack* as everyday examples. In the final part of the HI2 course in history, we discuss the world of interdependence and current threats, and cybersecurity is naturally and intrinsically connected to them. Here the topic is mostly approached from the national perspective.”

Geography

“In geography, in the geography of risks, the teaching covers cyber risks. These risks are also mentioned in the context of GPS positioning.”

Biology

“In biology, this is discussed, for example, in connection with DNA testing and individual identification.”

Health education

“In connection with assignments/projects, etc., I talk about what is worth publishing about yourself, how to use your passwords, etc.”

“In health education, cybersecurity is included, for example, in discussions about health-related databases and patient information systems, in the storage of research results and in connection with the processing of sexual harassment.”

“In health education class, I tell students not to post pictures about them online that they would not want to see there (for example, in relation to sexuality and nudity). I also tell them that they must not distribute pictures of others online. I tell them where to get help if they fall victim to a crime. Sometimes we get visits from the police about safe online behaviour, we have watched a police video about online safety and we watch riku.fi videos about situations/crimes that can happen in cases such as sexual health or bullying. I ask students to come up with versatile passwords when we log in to textbooks, for example, and to write them down."

Information and communication technology

"I also teach information technology, where it is discussed from the point of view of passwords, providing personal information, etc."

"At my school, I teach computer skills to first-year students, and we learn to use the new computers. My part of the course is only a half credit, and it takes place in the first period. We only have a little time to touch on cybersecurity. I also teach seventh-grade ICT classes in lower secondary school, where we have a little bit more time to touch on the topic. The resources are so minimal and there is so much content to cover during the course. A very important issue that should be invested in more."

Mathematics and physics

"Occasionally we talk about passwords and sometimes we encounter situations where the student's account has been hijacked. In these cases, the hijacking attempt is usually buried before we even have time to react."

Guidance counselling

"I am a guidance counsellor at a general upper secondary school. We have to work a lot with electronic documents, which is why cybersecurity would also be important in guidance counselling."

Psychology

"During the course, I also aim to raise awareness of how the media works and how to increase the safety of media use. Otherwise, I try to act as an example + take into account safety aspects in things like the media (use of cookies, being critical about what you read, etc.)."

3.7 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. Teachers gave examples from many different subjects of how cybersecurity is included in their teaching. In addition, one respondent raised the importance of cybersecurity in the work of the study counsellor.

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. The following aspects should be noted:

1. Access to ICT education in general upper secondary schools will be improved, and digital security will also be addressed as part of ICT education.
2. Teachers must be given the opportunity to train as ICT teachers
3. Continuing education should also address digital security and its teaching.

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.

3.8 Conclusions

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.

Observations on the curriculum in terms of cybersecurity/information security/digital security can be divided into three categories:

1. ICT and digital environments are used in subject teaching.
2. A couple of subjects take into account issues directly related to cybersecurity / information security / digital security.
3. Students practice skills that are also needed for safe activity in the digital environment, such as source criticism and media literacy.

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. The answers were clearly dispersed on the question of whether teachers include cybersecurity education within the framework allowed by the subject they teach. In addition, the availability of continuing education in cybersecurity was viewed with reservations.

Examples provided by teachers of the inclusion of cybersecurity in subject teaching show that it is covered in many different subjects and courses. On the other hand, as has been stated earlier, the teachers' answers were clearly dispersed in terms of whether they include cybersecurity education within the framework allowed by the subject. Therefore, cybersecurity currently appears to have been integrated into different subjects in many cases, but there is clear variation between teachers.

Increasing and developing cybersecurity education can be approached from several different perspectives. This report identified two 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.

References

Opetushallitus (2019). Lukion opetussuunnitelman perusteet 2019. https://www.oph.fi/sites/default/files/documents/lukion_opetussuunnitelman_perusteet_2019.pdf

4 Cybersecurity education in vocational education and training

4.1 Vocational education and training system in Finland

Vocational education and training (VET) in Finland is governed by Act 531/2017 (Finlex, 2017a), which is specified in Decree 673/2017 (Finlex, 2017d) and other decrees related to the act, in particular, the decree of the Ministry of Education and Culture on the qualification structure of vocational education and training (Decree 680/2017, see Finlex, 2017c), which was last updated by Decree 596/2021 (Finlex, 2021a). According to the act, vocational qualifications include initial vocational qualifications, further vocational qualifications, and specialist vocational qualifications. The decree on the qualification structure of vocational education and training further determines which titles are used for which vocational qualifications. The Finnish National Agency for Education determines, based on Act 531/2017 (Finlex, 2017a, Section 15), the national qualification requirements, which entails the competence areas included as compulsory and optional in each qualification title.

The scope of the qualifications is based on competence points. The extent of the competence point is not specified in the law, but the number of competence points is determined on the basis of the scope, difficulty, and significance of each unit in relation to the entire qualification (Act 531/2017, see Finlex, 2017a, Section 12). On the other hand, the entire qualification must correspond to the scope of the general upper secondary education syllabus (Act 531/2017, see Finlex, 2017a, Section 15). The definition will be specified in Government Decree 583/2021 (Finlex, 2021b), which enters into force on 1 August 2022. It states that one competence point will correspond to 12 hours of teaching and guidance if the student does not have previously acquired competence to complete the unit in question.

The scope of the initial vocational qualification is 180 competence points, the further qualification is 120, 150 or 180 competence points, and the specialist vocational qualification 160, 180 or 210 competence points. The initial vocational qualification includes 35 competence points of common units consisting of communications and interaction competence, mathematical and science competence, and citizenship and working life competence.

An initial vocational qualification provides broad, basic vocational competence and more specialised vocational skills in at least one field. A further vocational qualification provides more in-depth competence than an initial vocational qualification or focuses on a narrower set of tasks. A specialist vocational qualification provides even more in-depth competence than a further vocational qualification or multi-disciplinary skills. (See https://www.oph.fi/fi/koulutus-ja-tutkinnot/tutkintorakenne, in Finnish.)

The successful completion of vocational units is based on competence demonstrations through performing practical work tasks in actual work situations and work processes (Act 537/2017, see Finlex, 2017b, Section 52). In the interviewed VET institutions, the competence modules of the initial vocational requirements are mainly taught in the educational institution, while the further vocational qualification, and in particular the specialist vocational qualification, is mainly completed through competence demonstrations in the workplace.

A total of 156 educational institutions provide vocational education and training in Finland. Of these, 30% (n = 43) provide education and training in ICT:

1. Ael-Amiedu Oy
2. Ammattiopisto Spesia Oy
3. Axxell Utbildning Ab
4. Careeria Oy
5. City of Helsinki
6. City of Kajaani
7. City of Kouvola
8. City of Oulu
9. City of Tampere
10. City of Turku
11. City of Vaasa
12. City of Vantaa
13. Espoon seudun koulutuskuntayhtymä (Joint municipal authority for vocational education in the Espoo region)
14. Etelä-Savon Koulutus Oy
15. Helsinki Business College Oy
16. Hyria Koulutus Oy
17. Jokilaaksojen koulutuskuntayhtymä (Joint municipal authority for vocational education in the Southern Oulu region)
18. Jyväskylän koulutuskuntayhtymä (Joint municipal authority for vocational education of Jyväskylä)
19. Järviseudun koulutuskuntayhtymä (Joint municipal authority for vocational education in the Järviseutu region)
20. Kemi-Tornionlaakson koulutuskuntayhtymä Lappia (Lappia, Joint municipal authority for vocational education in the Kemi and Tornionlaakso region)
21. Keski-Pohjanmaan koulutusyhtymä (Joint municipal authority for vocational education in the Central Ostrobothnia region)
22. Keski-Uudenmaan koulutuskuntayhtymä (Joint municipal authority for vocational education in the Central Uusimaa region)
23. Kiipulasäätiö
24. Kotkan-Haminan seudun koulutuskuntayhtymä (Joint municipal authority for vocational education in the Kotka and Hamina region)
25. Koulutuskuntayhtymä Tavastia (Joint municipal authority for vocational education Tavastia)
26. Luksia, Länsi-Uudenmaan koulutuskuntayhtymä (Luksia, Joint municipal authority for vocational education of Western Uusimaa)
27. Länsirannikon Koulutus Oy
28. Optima Samkommun
29. Oulun seudun koulutuskuntayhtymä (Joint municipal authority for vocational education in the Oulu region)
30. Pohjois-Karjalan koulutuskuntayhtymä (Joint municipal authority for vocational education of Northern Karelia)
31. Raahen koulutuskuntayhtymä (Joint municipal authority for vocational education of Raahe)
32. Raision seudun koulutuskuntayhtymä (Joint municipal authority for vocational education in the Raisio region)

33. Rovaniemen koulutuskuntayhtymä (Joint municipal authority for vocational education of Rovaniemi)
34. Salon seudun koulutuskuntayhtymä (Joint municipal authority for vocational education in the Salo region)
35. Sasky koulutuskuntayhtymä (Sasky joint municipal authority for vocational education)
36. Satakunnan koulutuskuntayhtymä (Joint municipal authority for vocational education of Satakunta)
37. Savon koulutuskuntayhtymä (Joint municipal authority for vocational education of Savonia)
38. Seinäjoen koulutuskuntayhtymä (Joint municipal authority for vocational education of Seinäjoki)
39. Suupohjan koulutuskuntayhtymä (Joint municipal authority for vocational education of Suupohja)
40. Svenska framtidsskolan i Helsingforsregionen ab
41. Valkeakosken seudun koulutuskuntayhtymä (Joint municipal authority for vocational education in the Valkeakoski region)
42. Ylä-Savon koulutuskuntayhtymä (Joint municipal authority for vocational education of Upper Savonia)
43. Äänekosken ammatillisen koulutuksen kuntayhtymä (Joint municipal authority for vocational education of Äänekoski)

4.2 Cybersecurity instruction in VET

Cybersecurity competence areas are only included in the initial, further, and specialist vocational qualifications in ICT, and in all of them as an optional competence area. In the initial vocational qualification, the student can complete a unit called Maintaining Cybersecurity (30 competence points). As part of the further vocational qualification, students may complete the unit Working as a Cybersecurity Specialist (40 competence points). As part of the specialist vocational qualification, students may complete the unit Working as an Information Security Analyst (60 competence points). In addition to these units, cybersecurity competence has also been included in other ICT courses in the interviewed VET institutions when necessary, such as for the implementation of a functional and secure system. Since cybersecurity is an optional unit, some of the VET providers interviewed did not offer it at all.

Between 2011 and 2020, the ICT qualifications completed yearly were as follows: an annual average of 2,075 students (2,082 in 2020) completed an initial vocational qualification, an average of 186 students completed a further vocational qualification (312 in 2020), and an average of 12 students completed a specialist vocational qualification (27 in 2020) (Vipunen, 2022). The qualification title “information and communication technology” was adopted in 2020; the previous corresponding title was “information and telecommunications technology”. Exact information on how many students have completed cybersecurity competence areas is not available. Due to the low number of completions of further vocational qualifications and especially specialist vocational qualifications, this report focuses on the initial vocational qualification.

Initial vocational qualification

Training and education in ICT are currently based on the requirements that entered into force in 2020 (OPH-2596-2019, Part 16, *Maintaining cybersecurity*). They include the following vocational competence requirements:

- Students use techniques for managing and protecting against cyber threats:
    - They protect a device with updates and software.
    - They use system administration tools to manage a device.
    - They compare different encryption methods and select an appropriate one.
- Students manage cybersecurity risks:
    - They monitor the data network using various analytic tools.
    - They scan the agreed target network for vulnerabilities.
    - They validate system vulnerabilities.
    - They make development proposals for improving cybersecurity.
- Students promote cybersecurity solutions:
    - They are familiar with the acts, decrees, and other official regulations related to information security and data protection.
    - They illustrate cyber threats and the corresponding risks.
    - They comply with information security instructions in their work.
    - They provide guidance in cybersecurity or information security issues.

New qualification requirements will enter into force as of 1 August 2022, but the section on maintaining cybersecurity will not include any changes to the previous requirements (OPH-4948-2021, Part 16, *Maintaining cybersecurity*). The criteria for competence assessment and grades are defined only at a general level for all units.

The interviewed VET providers considered the national requirements for qualifications in cybersecurity to be a good starting point for teaching. The cybersecurity requirements were considered to be more abstract than many other ICT requirements. This was generally viewed positively, as it makes it possible to adapt the contents of teaching to other education and training as well as to keep contents up to date. However, the requirements were considered to be so demanding that there is little possibility of demonstrating competence in workplaces; rather, the demonstrations must be carried out in an educational institution. Examples of such competences included the selection of encryption methods, monitoring data networks, as well as scanning vulnerabilities.

Further vocational qualification

The 2021 qualification requirements for *Working as a cybersecurity specialist* (OPH-2639-2020, Part 3) include the following vocational competence requirements:

- Students are able to work in cybersecurity tasks.
- They are able to test cybersecurity.
- They are able to evaluate and develop cybersecurity solutions.

The qualification requirements also define the following criteria for successful performance for the assessment of competence:

- Students pay attention to ethics and professional secrecy, as well as the regulations in the field, in all activities.
- They monitor the general development of cyber threats.
- They use various operating systems, software, or other testing equipment.
- They configure testing programmes.
- They investigate security gaps and vulnerabilities in the customer's information system.
- They repeat the investigation after implementing corrective measures.
- They report detected vulnerabilities and deficiencies.
- They prepare a prioritised list of actions to correct detected vulnerabilities and shortcomings.

Similar observations can be made on the requirements for further vocational qualifications as for initial vocational qualifications. The criteria were considered suitably broad and abstract. The challenges were also similar: finding places to complete demonstrations in working life is not straightforward.

Specialist vocational qualification

The 2021 qualification requirements for *Working as an information security analyst* (OPH-2640-2020, Part 3) include the following vocational competence requirements:

- The students are able to take into account information and risk management.
- They are able to plan and manage access rights to the organisation's information systems.

The qualification requirements also define the criteria for successful performance for the assessment of competence:

- Students pay attention to ethics and professional secrecy as well as the regulations in the field in all activities.
- They monitor the development of information security solutions.
- They prioritise the value of data and determine the availability and integrity of mission-critical data.
- They acquire and test various data protection solutions.
- They take into account physical security as part of information and risk management.
- They maintain the organisation's information security guidelines.
- They plan methods for managing security incidents and their recovery.
- They plan the continuity of operations in situations following information security incidents.
- They participate in the activities of an information security group and in the preparation of risk management plans.
- They plan and manage access rights to the organisation's information systems.
- They plan the identification and authentication of people and devices.
- They plan the visibility and access rights of systems and data.
- They plan the licensing and license provisioning lifecycle.

The completion volumes of the specialist vocational qualification were relatively small in the interviewed VET institutions and do not therefore lend themselves to generalisations about the suitability of the qualification requirements.

4.3 Methods of study

4.3.1 Survey

The study was launched by identifying the VET institutions that offer ICT education and training. The process was divided into three phases.

The investigation was based on the Studyinfo service, which was searched with the Finnish term for "vocational education and training" using the field of education "ICT" as a search filter. The search criteria yielded five initial vocational qualifications with the title "Electronics specialist. ICT installer". These five organisations were Varia, Vamia, Sedu Lapua, Sedu Seinäjoki, Stadi Ammatti and Aikuisopisto. The search was repeated in April 2022, yielding 54 VET providers. Of these, one provider (Sasky) appears as five different results due to several different training locations. The difference in the search results is time-related, as the Studyinfo service only shows the qualifications that are available for application when the search is conducted. The information generated by this search method therefore time dependent.

The second search for training providers was carried out with the service ammattikoulut.fi (2021). The Finnish term for "information technology/programming" was used to search fields of education and training. The search yielded 54 qualifications offered by 28 different VET providers. This list is also incomplete, however, because institutions such as TAI, which offers ICT education and training, could not be found in the service. It should be noted that this service also includes VET providers that cannot be found in the Studyinfo service. An example of such a provider is the Finnish Institute for Enterprise Management.

The third search was made from the database of the Education Statistics Finland (Vipunen, 2021). The data used in the search was from the year 2020. The Finnish search term "information processing and telecommunications (ICT)" was used for the field of education. According to the search, 59 educational institutions offer ICT training, but the service does not provide information about what these educational institutions are. Therefore, a second search was carried out using the education providers filter, which yielded 156 educational institutions. In order to find which of these are the ones providing education and training in ICT (n = 59), the websites of all 156 educational institutions were analysed. The analysis resulted in 43 VET providers offering ICT training in Finland. The contact details of managers or team leaders of training and education were collected from the websites of the VET providers for sending the survey.

A request for research permission was sent to the principals of these 43 organisations. The research permission was granted by 14 of these. The survey was sent to 18 recipients in 14 organisations. The content of the survey was as follows:

- Is the respondent involved in providing training and education in information/cyber/digital security?
- To what extent is such training and education provided, and when did it begin at different qualification levels?

- Is the respondent willing to participate in a thematic interview?

Seven responses were received, and all indicated their willingness to participate in the interview. Of these, five were eventually carried out: with Oulun Seudun Ammattiopisto, Omnia, Tavastia, Turun ammatti-instituutti, and Business College Helsinki.

4.3.2 Thematic interviews

Five thematic interviews were carried out with educational institutions that had indicated their willingness to participate. The interview themes were selected to match the objectives of the study based on the group's discussions and a preliminary interview. The selected themes were the following:

1. The implementation of cyber education and training at different levels in the VET institution, the distribution and implementation of education in theory and practice, and the focus of education on technologies or, for example, privacy.
2. The scope of the qualification requirements in terms of cybersecurity, i.e., what topics should be taught and what areas should be covered.
3. Teachers' training needs in cybersecurity, what the current situation is, how teachers are supported, what kinds of resources are available, how teachers' competence development could be supported.

The following findings were obtained from the thematic interviews:

Implementation of teaching

The revised qualification requirements entered into force in 2018, which means that teaching is still transitioning into the new model. Some of the interviewees have provided instruction according to the old requirements as part of the unit "Maintaining information security" comprising 15 competence points. Some of the interviewees, on the other hand, will only begin instruction in autumn 2022.

The initial vocational requirements are completed at school, the traineeships, if possible, in working life. Further vocational qualifications and specialist vocational qualifications are more based on demonstrations in working life, but nevertheless in a manner that ensures that the competences included in the lower qualifications are also demonstrated. Naturally, only very few students have completed the further and the specialist vocational qualifications, and especially the specialist training is only now being launched in many institutions. It is not possible to arrange further and specialist vocational training for individual students.

Cyber training is mainly provided in the qualifications for IT support, IT installer, and network installer. In some VET institutions, cyber training is provided in two modules of 15 competence points each, with more demanding and more theory-based content in the second module.

The basics of cybersecurity are included in several educational programmes, and in some institutions all students receive short basic training as part of their common study units. Some interviewees suggested that cybersecurity should be integrated into other teaching in the future. For example, instruction in welfare technology should include information security training.

Contents of instruction and qualification requirements

The criteria set out in the qualification requirements are very diverse, and some are very challenging. Teachers may quite freely decide on the content of their instruction, and the interviewees especially commended the 2018 requirements for their lack of rigid guidelines. On the other hand, this may lead to differences to emerge between schools in how deeply the topic is covered. The requirements do not define which practical skills should be covered in the studies. The area is broad, and particularly students completing an initial qualification are only entering the field. The aim of the initial qualification is to provide a strong vocational foundation.

The demands of working life are in constant change, making open communication with it essential. Direct contacts with the world of work enables VET providers to know what to teach. Students become professionals of the future, so it is important to ensure that education is up to date, even though certain qualification requirements have been established a long time ago. Understanding threats and problems is an important part of competence. Students not only need linguistic competence in Finnish, but also in English, for example, to verify vulnerabilities in cybersecurity.

Education and training must also meet the needs of the students, and students of different age groups require different approaches. With adult students, the content of instruction may even exceed the qualification requirements.

Teacher training needs

Teachers' interest in developing their own competence is necessary and must be supported, and in an ever-evolving field, keeping up to date and developing oneself is a vital necessity. Teacher training was perceived to have sufficient resources, but a greater challenge was perceived to lie in finding suitable training. For example, courses offered by private training institutions rarely meet teachers' needs directly. The training should in some way benefit the entire teaching team. The training could also make use of certifications and existing frameworks.

Mentoring and networking among teachers was seen as important, both in working life and among other teachers in the field. The challenge is that teachers can focus on cybersecurity instruction in only a few educational institutions; most often they have teaching responsibilities in other fields as well. This means that they have correspondingly less time available to develop their cybersecurity competence.

Teachers are offered traineeships in working life funded by their educational institution. The interviewees' estimate of the duration of the traineeship varied greatly. Some mentioned that already one day is beneficial, but some found that only about 2 to 4 weeks allows for the everyday life to be experienced properly. The traineeship should be repeated every 3 to 4 years. Opportunities for teachers to participate in research groups in the field should be explored. It is increasingly challenging to recruit teachers in cybersecurity, since education may not seem like a personally relevant field for many professionals. However, professionals transitioning from work to education would bring with them fresh knowledge.

Workplace education and training

The interviewees considered the availability of places for workplace education and training to be a challenge. The expectations that the world of work has towards education and students are often higher than what education can provide. On the other hand, workplaces may not be able to offer tasks in traineeships in which students could use the education and training they have acquired. For example, confidentiality regulations and client agreements may prevent fully engaging the student in work tasks. One way to clarify students' competence level for the workplaces would involve certificates obtained by the students.

The interviewees had contradictory views in terms of the ideal size of the workplace for traineeships: some of the respondents felt that a smaller workplace may better take into account the student's competence and offer more versatile work tasks. Others felt that a larger workplace may have taken resources into account better, for example, in terms of guidance, which is an essential part of workplace education and training.

Overall, interviewees considered it important to communicate with potential traineeship providers. They also felt that traineeships could be productised, and that more information could be provided about the related demonstrations, which would also lead to more traineeship providers. There are plenty of opportunities, since traineeships are not only carried out at large organisations dedicated to cybersecurity; also places such as large industrial plants may offer good opportunities for workplace education and training. It is also worth keeping in mind that good traineeships may be found in the third sector. A well-completed traineeship can lead to a job in the organisation. Even if traineeships cannot be carried out in actual workplaces, all educational institutions have both teaching/laboratory networks and administrative networks where traineeships can be carried out. The maintenance of a laboratory network can be carried out as exercises for students of IT maintenance.

Collaboration

The interviewees highlighted the importance of collaboration between cybersecurity teachers and between VET institutions in many respects. Collaboration would allow for best practices to be shared and for VET institutions to carry out comparative analyses. From an educational perspective, VET institutions are not in competition. The interviewees discussed themes such as working together and having annual face-to-face meetings. A reference point is offered by the annual event organised in the field of education and training in business administration (Tradenomikoulutuksen päivät). Cooperation requires some platform or forum. The interviewees also perceived opportunities for cooperation in the construction of training/laboratory environments. Through cooperation, educators could also share the contacts they have with companies.

Training material

Several interviewees mentioned the programme *Team Whack* by the Finnish broadcasting company YLE. The programme's episodes are commonly used in instruction because the approaches and themes presented in the series appeal to students, even if actual work rarely offers equally fast-paced tasks. Another material in general use was the Cyber Weather service produced by the Finnish National Cyber Security Centre. This material was used to introduce students to cyber threats. The interviewees felt that VET providers could collaborate in producing teaching materials, since the qualification requirements are the same for everyone. On the other hand, the interviewees recognised that teachers wish to choose their own way of teaching. Many use materials produced by Cisco.

Synchronisation of teaching with universities of applied sciences

The interviewees mentioned that the differences between levels of education should be minimised. Study units at vocational schools should be designed in a way that would allow students to substitute first-year studies at universities of applied sciences. The interviewees estimated that the cybersecurity module encompassing 30 competence points in the initial vocational qualification studies would correspond to approximately 10 to 15 university ECTS credits.

Remote/hybrid teaching

Students are future professionals in the IT industry, so the interviewees generally considered that students need to master different distance learning practices as a basic requirement. On the other hand, many students were considered to need improvement in these basic skills. Remote practices are widespread in working life, so education must address the development of these skills. Distance learning also offers better opportunities for experts in the field to participate in teaching and to tell students about their work. Distance learning requires a lot from students. Those who have been in remote instruction during their basic education have weaker study skills.

4.4 Conclusions and development suggestions

Cybersecurity training is mainly provided in the qualifications for IT support specialists, ICT technicians, and network installers. The interviewed VET providers considered the national requirements for qualifications in cybersecurity to be a good starting point for teaching. The cybersecurity requirements were considered to be more abstract than many other ICT requirements. This was generally viewed positively, as it makes it possible to adapt the contents of teaching to other education and training as well as to keep the contents up to date. However, the requirements were considered so demanding that there is little possibility of demonstrating competence in workplaces; rather, the demonstrations must be carried out in an educational institution.

Cybersecurity competence areas are only included in the initial, further and specialist vocational qualifications in ICT, and in all of them as an optional competence area. In order to increase national cybersecurity competence in Finland, we recommend that cybersecurity training become a compulsory part of vocational training and education in ICT. In addition, cybersecurity instruction should be systematically integrated into all other vocational education and training as well.

Teachers’ interest in developing their own competence is necessary and must be supported, and in an ever-evolving field, keeping up to date and developing oneself is a vital necessity. Universities must be provided with resources to organise opportunities for continuous learning for vocational teachers. Measures should be taken to promote teachers' familiarity with working life.

The cooperation between educational institutions, teacher to teacher, must be developed and a platform and a forum created for it. Such cooperation would bring many benefits. If the qualifications are based on the same criteria, it is possible to use the same training materials. The development of educational environments can be carried out in cooperation. It is easy to share up-to-date information on technological developments. Jointly created models will also lower the threshold for starting education in new educational institutions.

Cooperation with working life should be developed. Awareness of the three levels of vocational qualifications and the traineeships included in them should be shared with the world of work.

References

Ammattikoulut.fi (2021). Ammattikoulut. https://www.ammattikoulut.fi/ . Retrieved 21.9.2021.

Finlex (2017a). Laki ammatillisesta koulutuksesta. 531/2017.

Finlex (2017b). Laki ammattikorkeakoululain 25 ja 26 §:n muuttamisesta. 537/2017.

Finlex (2017c). Opetus- ja kulttuuriministeriön asetus ammatillisen koulutuksen tutkintorakenteesta. 680/2017.

Finlex (2017d). Valtioneuvoston asetus ammatillisesta koulutuksesta. 673/2017.

Finlex (2021a). Opetus- ja kulttuuriministeriön asetus ammatillisen koulutuksen tutkintorakenteesta annetun opetus- ja kulttuuriministeriön asetuksen liitteen muuttamisesta. 596/2021.

Finlex (2021b). Valtioneuvoston asetus ammatillisesta koulutuksesta annetun valtioneuvoston asetuksen muuttamisesta. 583/2021.

Opetushallitus (2019). Tieto- ja viestintätekniikan perustutkinnon perusteet. Määräys OPH-2596-2019 19.12.2019.

Opetushallitus (2020a). Tieto- ja viestintätekniikan ammattitutkinnon perusteet. Määräys OPH-2639-2020 9.9.2020.

Opetushallitus (2020b). Tieto- ja viestintätekniikan erikoisammattitutkinnon perusteet. Määräys OPH-2640-2020 9.9.2020.

Opetushallitus (2021). Tieto- ja viestintätekniikan perustutkinnon perusteet.docx (sic). Määräys OPH-4948-2021 15.12.2021.

Opetushallitus (2022). Tutkintorakenne. https://www.oph.fi/fi/koulutus-ja-tutkinnot/tutkintorakenne. Retrieved 28.4.2022.

Opintopolku (2021). Opintopolku haku. https://opintopolku.fi/konfo/fi/. Retrieved 20.9.2021.

Opintopolku (2022). Opintopolku haku. https://opintopolku.fi/konfo/fi/ . Retrieved 16.4.2021.

Vipunen (2021). Koulutuksen järjestäjä- ja oppilaitosverkko. Opetushallinnon Tilastopalvelu. https://vipunen.fi/fi-fi/ammatillinen/Sivut/Koulutuksen-j%C3%A4rjest%C3%A4j%C3%A4--ja-oppilaitosverkko.aspx. Retrieved 23.9.2021.

Vipunen (2022). Ammatillisen tutkinnon suorittaneet. Opetushallinnon Tilastopalvelu. https://vipunen.fi/fi-fi/_layouts/15/xlviewer.aspx?id=/fi-fi/Raportit/Ammatillinen%20koulutus%20-%20tutkinnot%20-%20koulutusala.xlsb. Retrieved 29.4.2022

5 Cybersecurity education in universities of applied sciences

Universities of applied sciences in Finland are steered and measured according to the fields of education determined by the Ministry of Education and Culture (Eduuni Wiki, 2021). These fields of education are derived from the ISCED subcategories that are also used in UNESCO statistics (UNESCO-UIS, 2015). The same fields of education have also been adopted by the European Union to be used in its Member States (Eurostat, 2020). Therefore, these fields of education are also used by Statistics Finland, the national statistics institute (Statistics Finland, 2022).

5.1 Research data

The data collection was limited to information and communication technologies (ICT). This field of education most likely covers the majority of degree programmes related to cybersecurity. Similarly, students who would choose cybersecurity as optional studies would select it from the courses on offer in these degree programmes. In general, ICT as a field of education at universities of applied sciences include the following degree programmes:

- UAS Bachelor of Engineering, Degree Programme in Information and Communication Technologies
- UAS Bachelor of Business Administration, Degree Programme in Business Information Technology

Both degree programmes also offer UAS master's degree studies (UAS Master of Engineering and UAS Master of Business Administration). The names of the degree programmes producing these degrees vary considerably in each UAS.

The data collection was mainly restricted to this field of education, and it produced a large number of degree programmes and their curricula for analysis. In individual cases this restriction was overlooked, however, if cybersecurity was clearly detected in the instruction offered in other fields, such as security services.

The examination of curricula mainly focused on the names of courses rather than the learning objectives or course contents in the course description. Occasionally, course descriptions were examined for curriculum topics potentially related to cybersecurity. Based on these selection criteria, the number of degree programmes analysed are presented in Table 1. In addition to these degree programmes, the analysis covered the specialisation education, further education, and conversion training offered at each UAS.

TABLE 1. Number of degree programmes analysed

Degree programme	Quantity	Intake 2022
UAS master's degree	29	711
Engineer (UAS master's)	17	412
Business administration (UAS master's)	12	269
Police (UAS master's)	1	30
UAS bachelor's degree	64	3,830
Engineer (UAS bachelor's)	17	2,035
Business administration (UAS bachelor's)	12	1,375
Police (UAS bachelor's)	1	400
Kandidatexamen	2	20

5.2 Curricula

The degree programmes and curricula were collected first in autumn 2021 from the websites of each educational institution (e.g., www.lapinamk.fi) and from the published curricula (e.g., ops.vamk.fi). During and after the spring 2022 joint application period, the data were again compared with those reported in the Studyinfo system. At the same time, we examined the curricula published in spring for students starting in the academic year 2022–2023 for possible changes.

There was an overall lack of clarity in the initial intakes between different systems. For example, the website of a UAS may have given the initial intakes for spring 2021 even though they had clearly been increased or decreased in the Studyinfo service for spring 2022. When comparing these figures with the initial intakes reported in the survey, it was clear that also the heads of degree programmes had only approximate numbers of new students relative to the actual intake.

In addition, the Studyinfo.fi system offered separate applications for some UAS degree programmes. These include, for example, *open UAS tracks* for studying in the degree programmes, *applications to finish incomplete degrees*, and *intakes for international students*, for example, in dual degree programmes. These *separate applications* were excluded in the data collection, and the analysis focused on the intakes of the actual direct application (joint application procedure), as these separate applications were likely to compensate for issues such as the numbers of students discontinuing their studies.

5.2.1 Analysis

The curricula were analysed through a method of categorisation. The curriculum structures were categorised in terms of whether cybersecurity had been placed in compulsory, specialisation (or professional studies), or elective studies. This was used as a basis for determining into which model each curriculum could be categorised. The categorisation and specifications of these curricula are explained in Table 2.

TABLE 2. Categorisation models used in the analysis of degree programmes

Model	Specification
Model A	Degree programme aiming at cybersecurity and application available through Studyinfo
Model B	The degree programme offers specialisation studies oriented towards cybersecurity
Model C	The curriculum included cybersecurity in compulsory courses, but aimed at a different field (e.g., robotics or game development)
Model D	The curriculum included one or more cybersecurity-related courses in specialisation or elective studies
Model E	The curriculum did not offer cybersecurity, but it was found in the parallel curricula of the UAS
Model F	The curriculum or parallel curricula (of the same degree level) did not offer cybersecurity

The analysis of the curricula also revealed combinations of these models. For example, the compulsory courses in a degree programme curriculum may have included a course titled “Organisational Information Security” that was joint for all specialisations, but the degree programme also offered a specialisation dedicated to cybersecurity. In this case, the curriculum was decided to represent the combined model CD.

5.2.2 Model analysis of UAS master’s programmes

A UAS master’s degree usually consists of 60 or 90 ECTS credits, depending on which degree qualifies for the application: a UAS Bachelor’s Degree in Engineering consists of 240 credits and the same level of degree in Business Administration consists of 210 credits. The majority of this small number of credits is reserved for a master’s thesis of 30 credits. Very often, the remaining credits are precisely determined. Table 3 presents how the curricula of the analysed degree programmes divided between the analysis models.

TABLE 3. Degree programmes and initial intakes in each model in UAS master’s degrees

Model	Number of degree programmes	Initial intake	% of intake
Model A	4	79	11.11%
Model B	0	0	0%
Model C	8	150	21.10%
Model D	2	70	9.85%
Model E	6	182	25.60%
Model F	10	230	32.35%

Four-degree programmes in cybersecurity clearly represented Model A (in alphabetical order):

- JAMK, Master's Degree in Information Technology, Cyber Security, Engineer (UAS Master's)
- TurkuAMK, Software Engineering and ICT
  - Engineer (UAS Master's)
  - Business Administration (UAS Master's)
- XAMK, Cyber Security, Engineer (UAS Master's)

No degree programmes were categorised into Model B, because UAS master's degree programmes rarely include specialisations due to their small number of credits. Several degree programmes were categorised into Models C and D. These were parallel programmes at the same UAS. The UAS master's degrees in Model C had some compulsory part in cybersecurity, and those in Model D provided students with the opportunity to select elective courses from the compulsory studies offered in a parallel degree programme. Finally, a great number of degree programmes were categorised into Model F. These UAS master's programmes did not offer any courses in cybersecurity.

5.2.3 Model analysis of UAS bachelor's programmes

The UAS bachelor's degree programmes comprised the largest set of data, because the degree consists of 240 credits and many involved complex curriculum structures. The curricula seemed to have been compiled in order to present available courses to students (e.g., hundreds of elective courses listed in the XAMK curricula). Alternatively, the specialisations were built into a single curriculum, from which students could make modular choices (e.g., JAMK and ICT at Metropolia). In these cases, it was often necessary to interpret which modules were compulsory for which specialisation with the help of the UAS website. Another case at the other extreme were curricula consisting of precisely 240 credits, including only modules that were compulsory for the specialisation in question (e.g., the information management specialist programme at Lapland UAS). Table 4 presents how the curricula of the analysed degree programmes were divided between the analysis models.

TABLE 4. Degree programmes and initial intakes in each model in UAS bachelor's degrees

Model	Number of degree programmes	Initial intake	% of intake
Model A	3	85	2.22%
Model B	5	390	10.18%
Model BC	1	20	0.52%
Model C	11	752	19.63%
Model CD	12	618	16.14%
Model CDE	1	40	1.04%
Model CE	1	40	1.04%
Model D	13	1,163	30.37 %
Model E	12	447	11.67%
Model F	5	275	7.18%

The more extensive degree programmes at the bachelor's level clearly provide more opportunities for specialisation. As a result, they include considerably more Model B curricula. Most commonly, this meant that the degree programme was in IT or ICT, but the specialisation was cybersecurity (or equivalent). However, the problem with Model B curricula is to identify how much of the initial intake is actually allocated to cybersecurity. In Model A, this is clearer because cybersecurity is the direct study programme that students apply for.

In fact, the Model A curricula deviate from the selection criteria recommended by the Rectors' Conference of Finnish Universities of Applied Sciences (Arene) (Ammattikorkeakoulujen rehtorineuvosto, 2021), because cybersecurity is given as a direct study programme at Studyinfo. The 2016 selection criteria recommendations clearly set out the models for study programmes that should be used at Studyinfo (e.g., ICT). However, when examining the selection criteria recommendations over several years, Arene's guidance in the national selection criteria recommendations has clearly become less strict in this respect. Their report no longer maintains such a detailed list of degree programmes and related fields. This "slackening of control" in terms of the study programmes available for application clearly shows in the Studyinfo service and in this analysis. Curricula in Models A and B were concentrated in the following universities of applied sciences (in alphabetical order):

- JAMK, ICT, Engineer (UAS bachelor's)
- Laurea, Computer Science, Cyber Security, Business Administration (UAS bachelor's)
- TurkuAMK
  - ICT, Engineer (UAS bachelor's)
  - Data Processing, Business Administration (UAS bachelor's)
- XAMK, Cyber Security, Engineer (UAS bachelor's)

The majority of curricula are categorised as Model C and D degree programmes. These are often parallel degree programmes at the same UAS, with one compulsory course of cybersecurity or one or two courses offered as elective studies. However, a large number of degree programmes represented Models E and F: cybersecurity was not even mentioned in the course names.

5.2.4 Diversity of courses in UAS bachelor's and master's studies

Courses offered at universities of applied sciences are named in a variety of ways. The same topics can be taught under an entirely different or only slightly different course name. The study found 135 different names for UAS courses of different sizes having to do with cybersecurity. However, the topics are often very closely connected. For example, a course on the basics of cybersecurity may be called "Basics of Cybersecurity", "Introduction to Cybersecurity", or "Cybersecurity". Most courses comprise five ECTS credits. This may be an indication of a desire to make the courses conform with the standard. The distribution of course credits is presented in Table 5. If the number of credits is this similar, it may also be possible to allocate the contents under one name.

TABLE 5. Extent of cybersecurity courses in ECTS credits

Credits	Occurrences
15	1
10	2
5	115
4	4
3	9
2	2
1	2

The courses have previously been studied in the Kyberturvaaja project, which has listed the courses offered by Finnish higher education institutions participating in the project by theme (Tampereen ammattikorkeakoulu, 2020, 13–14). In addition, the project has designed course packages for different target groups (Tampereen ammattikorkeakoulu, 2020, 20). The framework clearly described in the project has not been adopted, as the naming practices continue to vary from institution to institution.

5.3 Implementation of the survey study

The survey was sent to 51 heads of degree programmes or heads of education at the end of 2021. The survey was targeted at the heads of bachelor's and master's degrees in ICT in all universities of applied sciences. In many institutions, that person may have been the head of other degree programmes as well. In other cases, the institution's public website may have directed contacts to the relevant degree programmes to the applications office or student services. However, in the majority of cases the survey was sent directly to the head of the degree programme. The total number of responses to the survey was 19, making the response rate approximately 37%.

When comparing the distribution of the respondents with the structures of the degree programmes, it can be clearly detected that the institutions that responded more actively also offer the most teaching in cybersecurity (degree programme models A and B). In the case of other institutions, it was relatively clear that only one head of degree programme responded to the survey or that no response was given. We examined the distribution of respondents between UAS master's and bachelor's degree programmes. Figure 19 presents the degree levels per responding UAS.

According to the survey respondents, UAS master's degrees are awarded by JAMK, Metropolia and XAMK. UAS bachelor's degrees are distributed in several institutions. It can clearly be seen that nearly three-quarters of the respondents represent the UAS bachelor's degree level. The responses for UAS master's degree programmes also clearly represent those institutions that emphasise cybersecurity in their instruction.

The question of whether the aim of the degree programme is to produce experts particularly specialising in cybersecurity was used to profile the main focus of the degree programmes and to identify those with an emphasis on cybersecurity. Figure 20 clearly presents three universities of applied sciences that focus on producing cybersecurity experts in their degree programme.

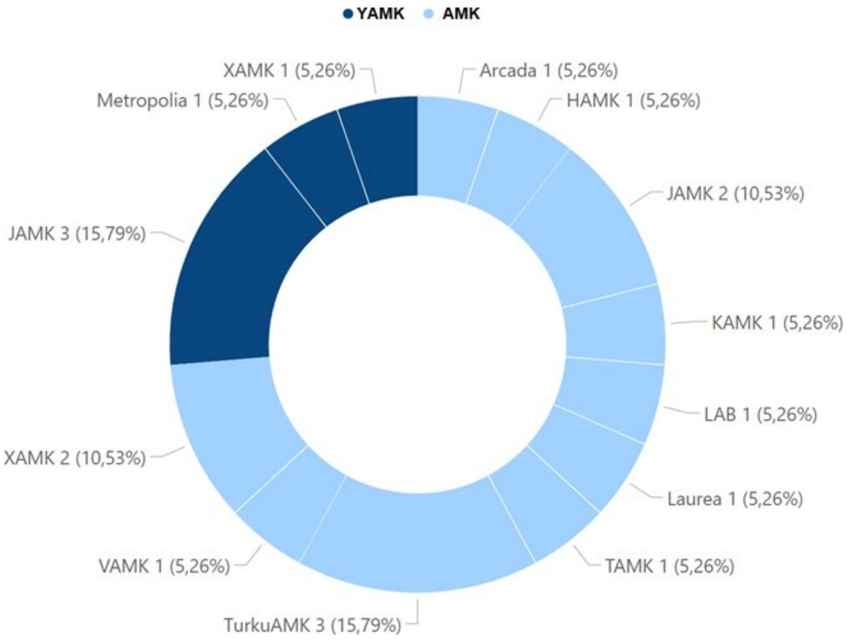


FIGURE 19. Distribution between UAS bachelor’s/master’s programmes

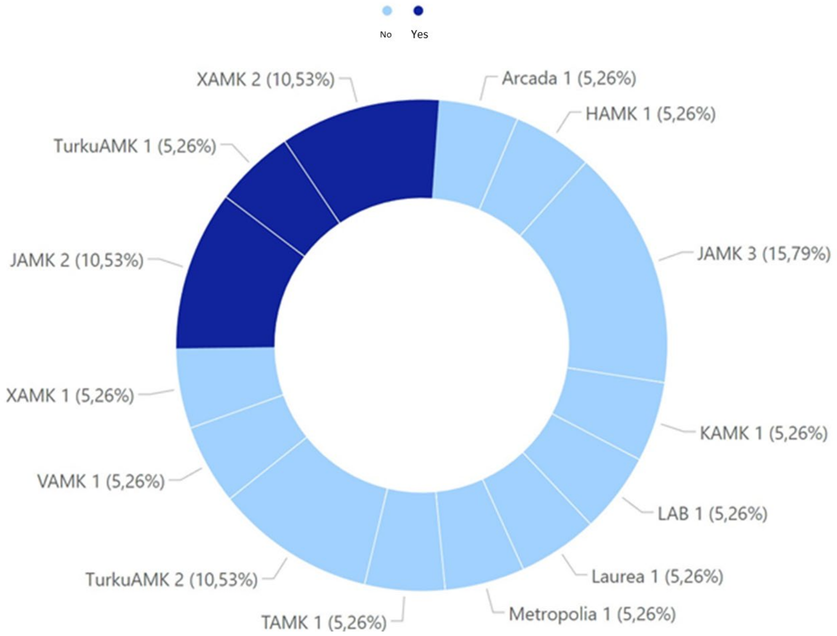
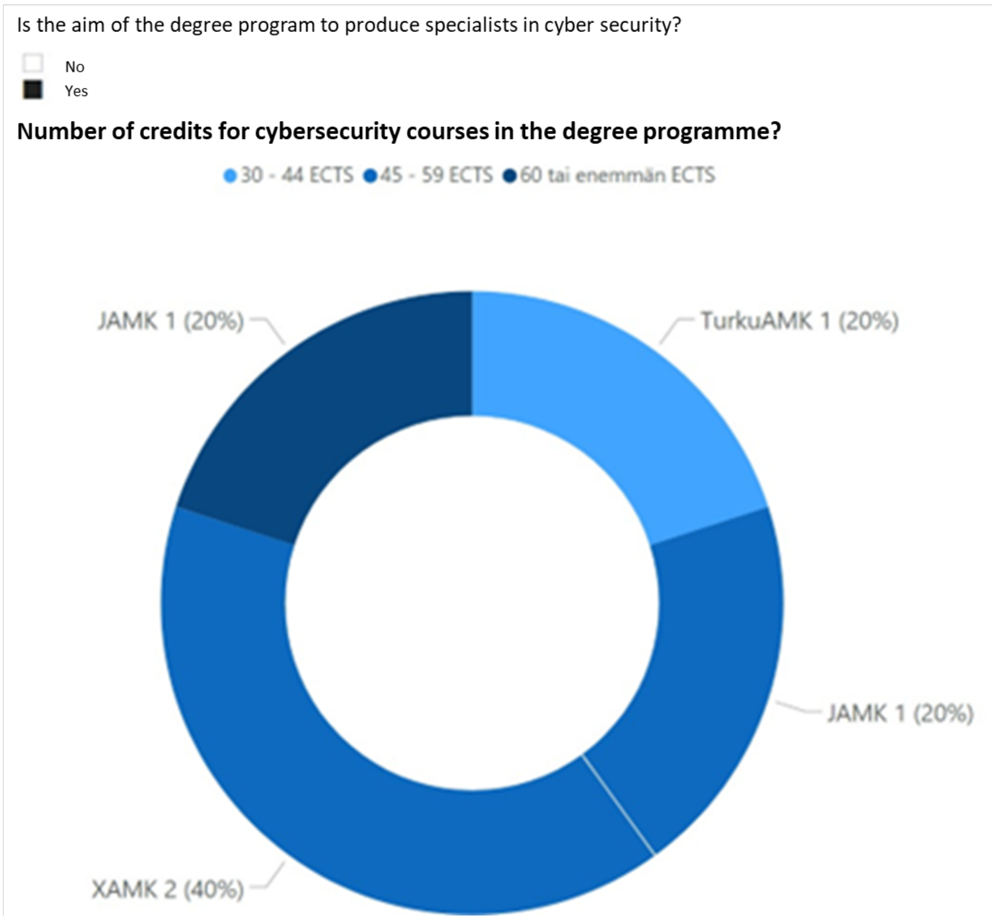


FIGURE 20. Is the degree programme aimed at cybersecurity?



Is the aim of the degree program to produce specialists in cyber security?

□ No
■ Yes

Number of credits for cybersecurity courses in the degree programme?

FIGURE 21. Cybersecurity degree programmes

Figure 21 shows only the degree programmes focused on cybersecurity. The degree programmes gave information on the number of credits for courses focusing on cybersecurity. However, the data in Figure 21 should be interpreted as indicative. It remains open to interpretation whether this emphasis is purely on compulsory studies or whether the degree programme offers a range of cybersecurity studies from which students may choose a suitable amount for their own degree. However, it is clear that the degree programmes focusing on cybersecurity also offer a significantly higher number of credits in the topic.

Figure 22 shows the number of credits in cybersecurity courses when the degree programme does not specialise in cybersecurity. Based on Figure 22, it is clear that in many degree programmes, cybersecurity plays a smaller role. Most degree programmes offer between 1 and 14 credits. In these cases, cybersecurity comprises one course, and the credits are between 1 and 14. Two degree programmes had between 15 and 29 ECTS credits of cybersecurity studies, but in these cases the modules were likely offered as advanced studies.

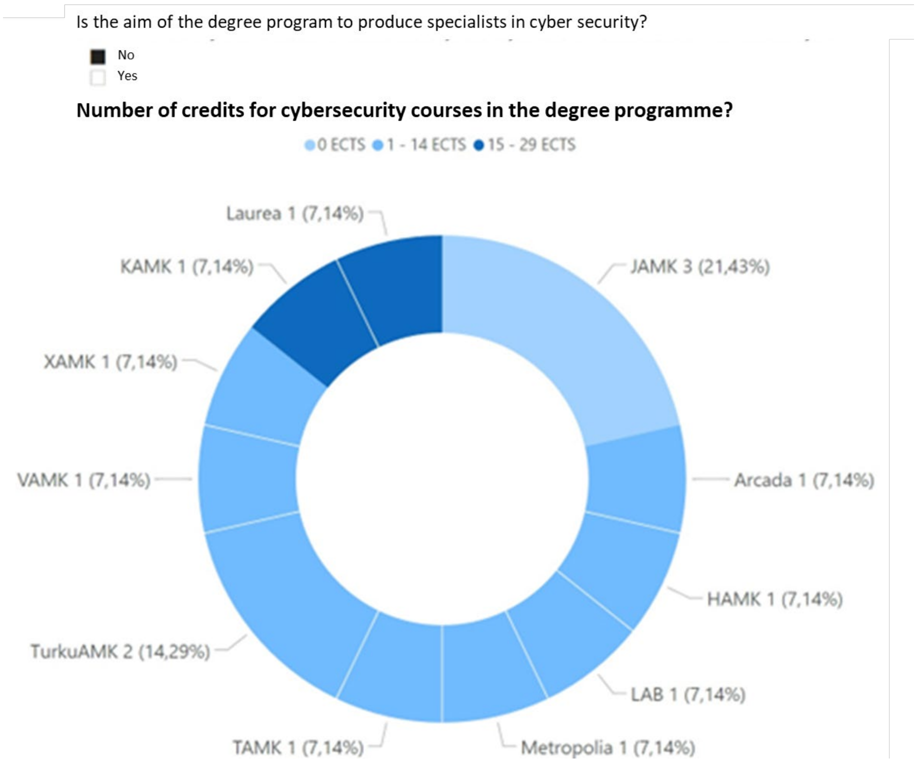


FIGURE 22. Cybersecurity credits in other degree programmes

High dropout rates are a well-known problem, especially in the field of engineering. In order to investigate why engineering studies are often delayed or interrupted, a study was commissioned by The Union of Professional Engineers in Finland, The Rectors' Conference of Finnish Universities of Applied Sciences (Arene), Finnish Energy, the Technology Industries of Finland, the Chemical Industry Federation of Finland, the Finnish Forest Industries Federation and the Association of Finnish Construction Engineers and Architects RIA. The research was carried out by E2 Study (E2 Tutkimus, 2021). The results of the study were as follows:

- Only one in four students completes their degree in four years.
- According to statistics, only a little more than 60% of engineering students complete their degree.

Since the current report focuses on ICT studies, this has a direct impact on the graduation of cybersecurity experts from universities of applied sciences and their availability in the labour market. As a response to this issue, universities of applied sciences often have larger initial intakes than graduation objectives. It is difficult to verify this larger initial intake, however, because the agreements between the Ministry of Education and Culture and the UAS combine different fields, such as natural sciences, ICT, engineering, and agricultural and forestry sciences, into average degree objectives.

The survey asked the heads of degree programmes for their estimates of dropout rates. Figure 23 shows indicative estimates of the graduation rate given by the heads of degree programmes.

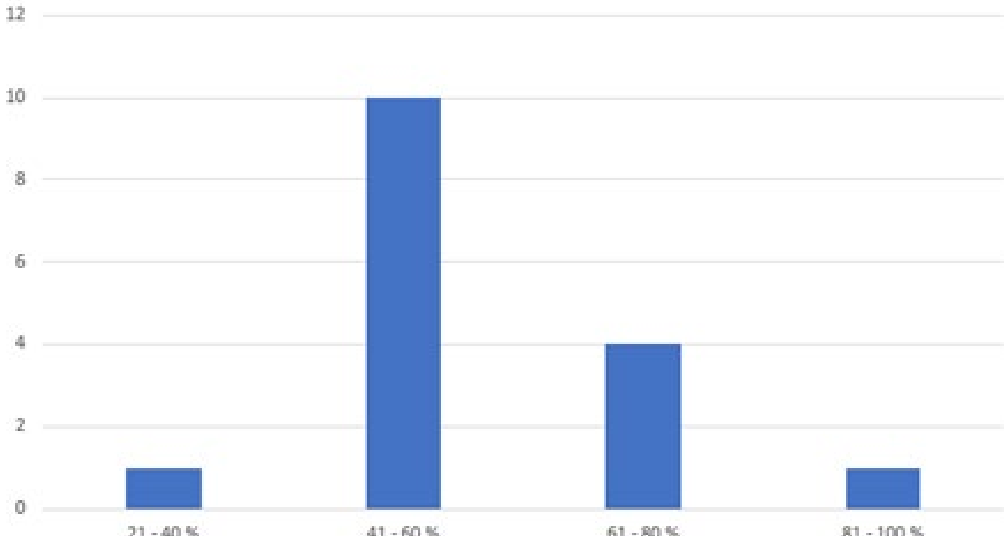


FIGURE 23. Estimated graduation rate

The survey also clearly indicates an estimated 41%–60% graduation rate. As a calculated average, graduation on the basis of this survey is slightly closer to 60%, which is in line with the E2 study. It should be noted that not all degree programmes in Finland responded to the survey, and the answers are based on the respondents' perceptions, not on official information. However, as a generalisation, the survey suggests that slightly more than half of the initial intake will graduate.

The aim of the question was to find out whether the heads of degree programmes are familiar with the frameworks concerning the field of cybersecurity. This was used to conclude whether the degrees focus on a standardised structural model of cybersecurity teaching. The answer is presented in Figure 24. Three heads of degree programmes (JAMK, XAMK, LAB) recognised the NICE framework, but no one knew the JSEC2017.

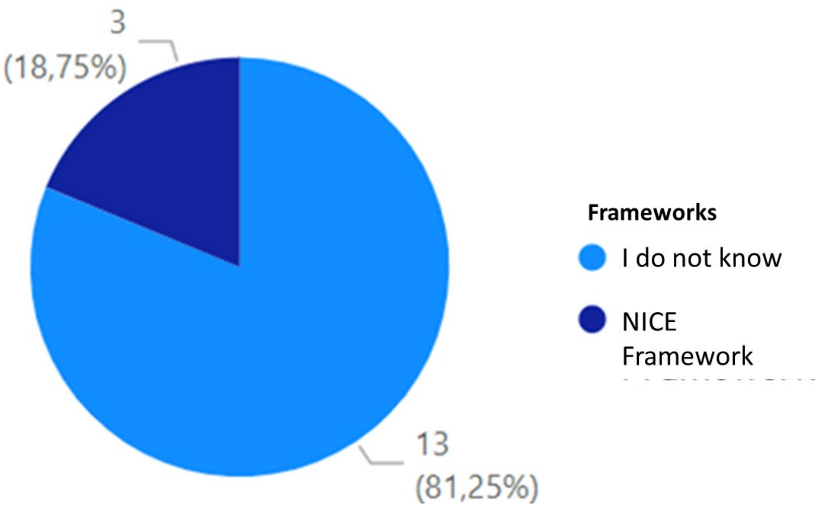


FIGURE 24. Knowledge of frameworks by heads of degree programmes

5.4 Results of the interview study

For the study, heads of degree programmes in four universities of applied sciences were interviewed. The question about increasing teaching strongly highlighted the national skills shortage. A particular concern was the lack of resources in cybersecurity teaching. As the greatest problem, the interviewees mentioned the difficulty of getting enough skilled teaching staff due to the general shortage of experts in the field. Recruitment was seen as further complicated by competition with the industry in terms of tasks and salaries. Another problem mentioned by the interviewees concerned teachers' ability to keep up with development in the field, as the cybersecurity industry and potential cyber threats are constantly changing.

The interviewees considered that education in the field of cybersecurity and information security should aim to produce skilled engineers for business life and to educate cybersecurity experts for the needs of society in general. Understandably, they felt that education should provide students with the skills they need at work. They also considered that the aim of the UAS was to provide the service of producing experts for society. Table 6 shows the most frequent topics that emerged in the interviews.

TABLE 6. Most frequent topics in the interviews

Topic	Occurrences
Shortage of resources in cybersecurity teaching	8
Cybersecurity management	3
Cybersecurity of the information network	3
UAS master's degree: obstacles to studying alongside work	2
The amount of teaching has increased	2
Technical implementation is emphasised	2
Cybersecurity education will increase in quantity	2
Trend: the role of AI	2
World situation, or the Russian invasion of Ukraine	2
Lack of skilled educators	2
Continuing education: updating degrees	2

Currently the most significant topics of cybersecurity regarded its management and the cybersecurity of information networks. The actual technical implementation was also seen as a current priority, probably in contrast to administrative aspects. The interviewees mentioned that experts need problem-solving skills in such a way that cybersecurity provides solid background knowledge: offensive and defensive actions, business perspectives and project competence are the desired competence. They also considered it important to teach students about how to operate in a security operations centre (SOC). In the programmes focused on cybersecurity, it was sometimes felt that everything else that needs to be studied may come in the way of building competence in the actual subject matter. For example, orientating towards general management skills might take away from a student's technical competence. Fewer students were estimated to graduate per year than are admitted. Several reasons for this disparity were given. Students seeking a UAS master's degree often pursue their degree while working, which was seen to hinder their studies. However, employment rates among students in the field are high. The interviewees also mentioned a lack of technical skills among newer applicants and the importance of programming skills. The amount of teaching was seen to have increased, but there were two opinions about the future: on the one hand, teaching was expected to increase, and on the other hand, it was not, in which case the interviewees tended to refer to problems with resources.

Among future trends, the role of AI was mentioned twice. Other future topics seen as important included modern networks, critical infrastructure, the impact of remote work, identity, and access management, zero trust, situational awareness, cybersecurity management, and cybercrime investigation. The interviewees also mentioned that critical applied areas, such as seafaring, energy, and health care, should be better taken into account. In addition, educating the general public about information security emerged as a necessary objective for future development. Among current topics, the world situation, or the Russian invasion of Ukraine, was cited as a factor potentially increasing the popularity of cybersecurity education.

In terms of continuing education, the most important observation was the need to update earlier degrees. The interviewees also reported that training is offered to the unemployed in order to update their cybersecurity skills. Open university studies were also mentioned, as they often offer the same courses as degree studies. However, there is rarely a general course for all fields, and here, too, the lack of competent educators is an issue.

As a general observation on cybersecurity education, the guidance from the Ministry of Education and Culture was mentioned. Ministry guidance was seen as a top-down practice that limits the supply of education, for example, in terms of resourcing: the degree objectives given by the Ministry determine the amount of teaching. The costs of increasing the number of students for universities of applied sciences would require funding to be differently allocated, because the Ministry’s degree objectives determine the amount of teaching. On the other hand, the interviewees had taken note of the already existing provision of cybersecurity training initiated by higher education institutions.

5.5 Overall analysis of universities of applied sciences

The curriculum contents of degree programmes leading to UAS degrees and the interviews with heads of degree programmes indicate that cybersecurity education is provided comprehensively at the UAS bachelor’s and UAS master’s level, but teaching is strongly concentrated in specific institutions.

In terms of their extensive content of cybersecurity education and their response to the demands of working life, the following institutions stand out: Jyväskylä University of Applied Sciences, South-Eastern Finland University of Applied Sciences, Laurea University of Applied Sciences, and Turku University of Applied Sciences. Based on the curricula, these institutions offer extensive studies and meet the needs of society, industry, and business. One point that needs to be improved, however, would be to harmonise what may be called the basic “cybersecurity course” in all degree programmes. In other words, this would be a similar course on the basics of cybersecurity. The curricula suggest that every institution offers such a course, but with a slightly different name, a slightly different number of credits, and at least different learning outcomes.

Despite this, although in general modular curriculum contents do respond to identified competence gaps, the issue on a national level lies more in the area of educational resources: for example, initial intakes and the amount of teaching resources are insufficient. The threat posed by the lack of available work force is strongly linked to the number of dropouts. In the current study, the number of dropouts relative to the initial intake would mean that approximately 332 of the 554 students who started their studies in the Model A and B UAS bachelor's and master's programmes in cybersecurity would graduate (with a 60% dropout rate). This number is somewhat generous, however, because it is not entirely clear how many of the Model B programmes are actually oriented towards cybersecurity.

To respond to the skills shortage, educational policy decisions have been made already during this study at the end of 2021. In December 2021, the Ministry of Education announced, based on the proposals of higher education institutions, that it would increase their initial intake by 2,300 students, of which universities of applied sciences will receive a total of 822, divided between 21 universities of applied sciences for programmes starting in 2022. This measure aims to respond to the shortage of highly skilled professionals and to implement the Government's objective of raising the level of competence and education in the population. The increase will secure the availability of higher education in different parts of Finland, especially for fields of education suffering from labour shortages, to strengthen the vitality of the regions. (See Opetus- ja kulttuuriministeriö, 2021b.)

The distribution of the added initial intake numbers shows that the field of ICT will receive a total of 185 extra students divided between 9 universities of applied sciences (5 to 40 extra students, depending on the institution) (Opetus- ja kulttuuriministeriö, 2021a). Table 7 shows how the increase in the initial intake was directed at cybersecurity degree programmes. Of the Model A and B degree programmes, only JAMK and Turku University of Applied Sciences received an increase in the initial intake.

The current study suggests that the decision of the Ministry of Education and Culture is beneficial, but increased intakes and additional resources for education will also be needed in the future, as digitalisation will further develop and create requirements for cybersecurity experts in different industries.

TABLE 7. Impact of the 2021 increase in initial intakes on cybersecurity degree programmes

UAS	Degree programme	Increase	Model
Haaga-Helia	Business Administration (UAS Bachelor's), Data Processing	40	D
HAMK	ICT, Engineer, multiform	20	CD
JAMK	ICT, Engineer (UAS Bachelor's)	20	B
XAMK	Engineer (UAS Bachelor's), Game Technology	30	D
KAMK	Engineer (UAS Bachelor's), ICT	20	CD
Metropolia	Engineer (UAS Bachelor's)	25	C
OAMK	Business Administration (UAS Bachelor's), Data Processing	15	F
SAMK	Business Administration	5	D
TurkuAMK	ICT, Engineer (UAS Bachelor's)	10	B

As regards cybersecurity competence, it must be taken into account that the ongoing digital transformation means that an ICT expert will not acquire all the skills needed in working life during their education. They will continue to accumulate sector-specific competence alongside work, and they will need to update their competence throughout their careers as the operational environment changes and develops. However, education will provide them with the necessary basic competence, which enables new knowledge and skills to be studied and new competences to be acquired.

It remains to be considered how much sector-specific cybersecurity should be taught. For example, a course named "Data protection and security in the social and health care system" was detected in the analysed curricula. How many other courses, targeted to specific fields, should be created? In addition, it was clear that cybersecurity was featured as a form of specialisation or continuing education at different universities of applied sciences with quite a large number of courses.

5.6 Conclusions and recommendations

In cybersecurity, one of the most important and valuable assets to protect is skilled personnel. No matter the quality of technical solutions and processes in an organisation, it does not have cyber resilience without skilled personnel. This is true for all employee roles because incompetence or lack of knowledge among the staff may subject the organisation to vulnerability in cyberspace.

Organisations need technical cybersecurity experts for tasks such as designing secure systems, maintaining systems, acquiring secure systems, or identifying attacks and intrusions, and carrying out a variety of cyber incident management measures.

There is a global recognition of a shortage of skilled cybersecurity experts. This same shortage applies to both Europe and Finland. Globally, the need of skilled workforce is in the millions; for Finland, it is safe to say that it is several thousands.

Regarding this skills shortage, it is important to take into account the different skills needed in different jobs. The identification and incident management of cyberattacks requires different cybersecurity expertise than cybersecurity management or the acquisition of new systems. This division is still quire rough compared to a cybersecurity workforce framework. For example, the knowledge, skills, and abilities defined in the NICE Framework suggest that the range of competences is quite wide and that workers need to specialise in a specific area.

This must be taken into account in the training, that is, in which jobs graduating students are expected to be employed. Of course, it must be kept in mind that training provides certain basic competences which may be developed later into deeper expertise through work assignments, specialisation, and possible specialist training in the area.

The cybersecurity education provided by universities of applied sciences (bachelor's and master's degrees as well as specialist education, continuing education, and conversion training) is comprehensive in content and is able to adapt to the needs of industry due to its modular structure. However, investments are needed in education resources in order to meet the demands of continuously expanding digitalisation. As a result, cybersecurity expertise is increasingly needed in various digitalising industries. The competence needs of the industries will also expand strongly as cybersecurity is combined with robotic process automation (AI, neural networks, deep learning).

When considering education resources, it must also be taken into account that universities of applied sciences generally provide technical cybersecurity training, which aims for technical competence. Such engineering instruction requires extensive and complex learning environments, which are expensive to acquire and maintain. In order to guarantee sufficient technical expertise, the acquisition, development, and maintenance costs of the necessary learning and training environments must be taken into account in resource allocation.

It is necessary to increase the number of teachers if cybersecurity education is to be increased. The challenge in increasing the number of teachers and recruiting sufficiently skilled experts lies in the attractiveness of teaching careers. In this rapidly developing sector, topics must support working life and therefore also partly stem from its needs.

Cybersecurity education should also be targeted at different areas of working life. In this way, the necessary skills would be available to society in general. Continuing education that updates degrees also requires teaching resources. Education must produce enough experts so that society is prepared to respond to the challenges of today's world.

Since universities of applied sciences operate on the basis of predetermined teaching volumes, it must be possible in the future to allocate resources to cybersecurity education through administrative decisions, as this is the greatest actual incentive for the UAS field to start increasing production.

References

Ammattikorkeakoulujen rehtorineuvosto (2021). Ammattikorkeakoulujen valintaperustesuositukset 2021. https://www.arene.fi/julkaisut/raportit/ammattikorkeakoulujen-valintaperustesuositukset/. Viitattu 02.04.2022.

CC (2020). Computing Curricula 2020 – CC2020: Paradigms for Future Computing Curricula (Draft, Version 36). https://cc2020.nsparc.msstate.edu/.

CSEC (2017). Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (Version 1.0). ACM, IEEE, AIS, IFIP. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

E2 Tutkimus (2021). Miksi opinnot viivästyvät ja keskeytyvät? Selvitys AMK-insinööriopiskelijoiden opintojen viivästymisen ja keskeyttämisen syistä. https://www.ilry.fi/wp-content/uploads/2021/11/Miksi-opinnot_viivastyvat-ja-keskeytyvat-selvitys.pdf. Viitattu 02.04.2022.

ECSO (2017). Gaps in European Cyber Education and Professional Training. European Cyber Security Organisation (ECSO) https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf.

ECSO (2021). European Cybersecurity Education and Professional Training: Minimum Reference Curriculum. European Cyber Security Organisation (ECSO). https://www.ecs-org.eu/documents/publications/61967913d3f81.pdf.

Eduuni Wiki 2021. OKM:n korkeakoulujen ohjauksen alat. https://wiki.eduuni.fi/display/cscsuorat/7.2+OKM%3An+ohjauksen+alat+2021. Viitattu 22.04.2022.

ENISA (2021). Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

Eurostat (2020). International Standard Classification of Education (ISCED). https://ec.europa.eu/eurostat/statistics-explained/index.php?title=International_Standard_Classification_of_Education_(ISCED). Viitattu 02.02.2022.

ISC2 (2021). A Resilient Cybersecurity Profession Charts the Path Forward. 2021 Cybersecurity Workforce Study, International Information Systems Security Certification Consortium (ISC)^2. https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

Jyväskylän ammattikorkeakoulu (2022). CYBERDI. https://www.jamk.fi/fi/projekti/cyberdihttps://www.jamk.fi/fi/projekti/cyberdihttps://www.jamk.fi/fi/projekti/cyberdi. Viitattu 02.02.2022.

Lehto, M. & Niemelä, J. (2019). Kyberalan tutkimus ja koulutus Suomessa 2019. Jyväskylä: Jyväskylän yliopisto. Informaatioteknologian tiedekunnan julkaisuja 83/2019.

Opetus- ja kulttuuriministeriö (2015a). Opetus- ja kulttuuriministeriön tarkentavat ohjeet sopimuskauden 2017–2020 valmisteluun ja vuonna 2016 käytäviin neuvotteluihin. https://okm.fi/documents/1410845/4169434/OKM+ohje+https://okm.fi/documents/1410845/4169434/OKM%2Bohje%2B2016%2Btarkentavat%2Bohjeet%2Bsopimuskauden%2B2014-2020%2Bvalmisteluun%2Bja%2Bvuonna%2B2016%2Bkäytäviin%2Bneuvotteluihinhttps://okm.fi/documents/1410845/4169434/OKM%2Bohje%2B2016%2Btarkentavat%2Bohjeet%2Bsopimuskauden%2B2014-2020%2Bvalmisteluun%2Bja%2Bvuonna%2B2016%2Bkäytäviin%2Bneuvotteluihinhttps://okm.fi/documents/1410845/4169434/OKM+ohje+2016+tarkentavat+ohjeet+sopimuskauden+2014-2020+valmisteluun+ja+vuonna+2016+käytäviin+neuvotteluihin. Viitattu 02.02.2022.

Opetus- ja kulttuuriministeriö (2015b). Opetus- ja kulttuuriministeriön tarkentavat ohjeet sopimuskauden 2017–2020 valmisteluun ja vuonna 2016 käytäviin neuvotteluihin. Liite 1: Kauden 2017–2020 sopimusvalmistelua koskevat ohjeet https://okm.fi/documents/1410845/4169438/OKM%2Bohje%2B2016%2C%2BLiite%2B1%2BKauden%2B2017-2020%2Bsopimusvalmistelua%2Bkoskevat%2Bohjeet. Viitattu 02.02.2022.

Opetus- ja kulttuuriministeriö (2019). Ohjauskäytänteiden uudistaminen sopimuskaudelle 2021–2024, rahoituslaskelmat ja vuoden 2019 toimintaa koskeva raportointi. Ohjaus- ja palautemenettelyn uudistaminen sopimuskaudella 2021–2024. https://okm.fi/documents/1410845/15969577/OKM+kirje+2019+Ohjausk%C3%A

4yt%C3%A4nteiden+uudistaminen+sopimuskaudelle+2021-2024,+rahoituslaskelmat+ja+vuoden+2019+toimintaa+koskeva+raportointi.pdf/4f8e2a50-10f8-a883-aebd-84afee806d6c/OKM+kirje+2019+Ohjausk%C3%A4yt%C3%A4nteiden+uudistaminen+sopimuskaudelle+2021-2024,+rahoituslaskelmat+ja+vuoden+2019+toimintaa+koskeva+raportointi.pdf?version=1.1&t=1583225886000. Viitattu 02.02.2022.

Opetus- ja kulttuuriministeriö (2021a). Ammattikorkeakouluille myönnetyt uudet lisäpaikat vuodelle 2022. https://okm.fi/documents/1410845/4392480/https://okm.fi/documents/1410845/4392480/AMK-uudet%2Blisäpaikat%2B2022.pdf/7a9befe4-8019-135c-fbb1-381094f5d67f/AMK-uudet%2Blisäpaikat%2B2022.pdf?t=1639985949325https://okm.fi/documents/1410845/4392480/AMK-uudet%2Blisäpaikat%2B2022.pdf/7a9befe4-8019-135c-fbb1-381094f5d67f/AMK-uudet%2Blisäpaikat%2B2022.pdf?t=1639985949325https://okm.fi/documents/1410845/4392480/AMK-uudet+lis%C3%A4paikat+2022.pdf/7a9befe4-8019-135c-fbb1-381094f5d67f/AMK-uudet+lis%C3%A4paikat+2022.pdf?t=1639985949325.

Opetus- ja kulttuuriministeriö (2021b). Korkeakoulujen aloituspaikkoja lisätään vuodelle 2022 noin 2 300:lla. https://okm.fi/-/korkeakoulujen-aloituspaikkoja-lisataan-vuodelle-2022-noin-2-300-llahttps://okm.fi/-/korkeakoulujen-aloituspaikkoja-lisataan-vuodelle-2022-noin-2-300-llahttps://okm.fi/-/korkeakoulujen-aloituspaikkoja-lisataan-vuodelle-2022-noin-2-300-lla.

Schmidt, C. (2004). The analysis of semi-structured interviews. In U. Flick, E. von Kardorff & I. Steinke (eds.), A Companion to Qualitative Research. London, Thousand Oaks, New Delhi: SAGE Publications, pp. 253–258.

Statistics Finland (2022). National classification of education 2016. ⟨URL:https://tilastokeskus.fi/fi/luokitukset/koulutusala/koulutusala_1_20160101/⟩.

Tampereen ammattikorkeakoulu (2020). Kyberturvaaja-hanke. Loppuraportit, tulokset, yhteenvedot ja tuotokset. https://projects.tuni.fi/uploads/2020/10/91c0d668-20201029_kyberturvaaja_tuotokset.pdfhttps://projects.tuni.fi/uploads/2020/10/91c0d668-20201029_kyberturvaaja_tuotokset.pdfhttps://projects.tuni.fi/uploads/2020/10/91c0d668-20201029_kyberturvaaja_tuotokset.pdf.

Tilastokeskus (2022). Kuntapohjaiset tilastointialueet. Aineisto on ladattu Tilastokeskuksen rajapintapalvelusta 9.3.2022 lisenssillä CC BY 4.0.

UNESCO-UIS (2015). International Standard Classification of Education: Fields of education and training 2013 (ISCED-F 2013) – Detailed field descriptions. UNESCO Institute for Statistics. http://dx.doi.org/10.15220/978-92-9189-179-5-en

6 Cybersecurity education in universities

This part study describes the current state of cybersecurity education at Finnish universities. The study was carried out by examining the degree programmes of universities through their websites and a structured survey. The part study also involved interviews with four cybersecurity experts in the university sector. The study also investigated the situation of continuing education offered by universities and the cybersecurity courses offered by the FITech Network University. The analysis was informed by the Cybersecurity Curricula 2017 (CSEC, 2017) and the areas of cybersecurity defined in it:

- Data Security, Software Security
- Component Security
- Connection Security
- System Security
- Human Security
- Organisational Security
- Societal Security

The number of degree programmes dedicated to cybersecurity is small, and teaching is concentrated in the master’s level. Universities produce relatively few cybersecurity experts in relation to the identified skills shortage. A great number of degree programmes have integrated cybersecurity into the degree structure as elective or compulsory studies worth 1 to 15 ECTS credits. Universities provide further education in the cyber field to a small extent. The interviews revealed that students’ interest in studying cybersecurity has increased in recent years and that it would be worth increasing resources in developing educational cooperation between universities. Additional resources for teaching and research would improve cybersecurity education in Finland. One challenge for resources was the recruitment of experts in the field.

6.1 Collection of data

The first phase of the data collection involved the examination of the degree programmes in different faculties and departments of the universities. This phase resulted in a list of degree programmes which was used to select the recipients of a structured survey. Respondents to the survey were selected among heads of degree programmes / coordinating teachers in degree programmes including teaching on cybersecurity / information security / digital security. The study also included four interviews with cybersecurity experts from four universities.

The analysis was informed by the Cybersecurity Curricula 2017. The curriculum defines standard criteria for cybersecurity degree programmes and identifies the following areas of cybersecurity competence: Data Security, Software Security, Component Security, Connection Security, System Security, Human Security, Organisational Security, and Societal Security. (CSEC, 2017)

As a result of the data collection and analysis, we compiled a list of courses on cybersecurity and information security and the degree programmes where they are taught. There may be more cybersecurity courses than reported here. In addition, cybersecurity education may be offered in degree programmes that are not included in this report.

The project has also described the current situation of continuing education provided by universities in the field of cybersecurity. The description of continuing education is based on information acquired through the universities' websites and the interviews. In addition, this part study describes the number of applicants and the initial intakes in key degree programmes. The figures are based on the applicant statistics for spring 2022 and the results of the survey. The figures presented in this report are indicative, as the figures do not take into account possible intakes via the open university route or transfers. In addition to the joint right to complete a bachelor's and master's degree, it is often possible to apply only for a master's degree, which has a separate intake quota. These factors make it difficult to estimate the definite numbers of applicants and intakes, making the figures indicative.

The survey examined how many new students are selected for the degree programme, how many students graduate from the degree programme in relation to the initial intake, and how many cybersecurity courses the degree programme includes. Finnish universities have a great number of degree programmes that have integrated cybersecurity into the degree structure as elective or compulsory studies worth 1 to 14 ECTS credits. In contrast, there are few degree programmes where cybersecurity is the main focus or plays a significant role in the content of the degree programme. Figure 25 presents the number of cybersecurity courses in the degree programmes.

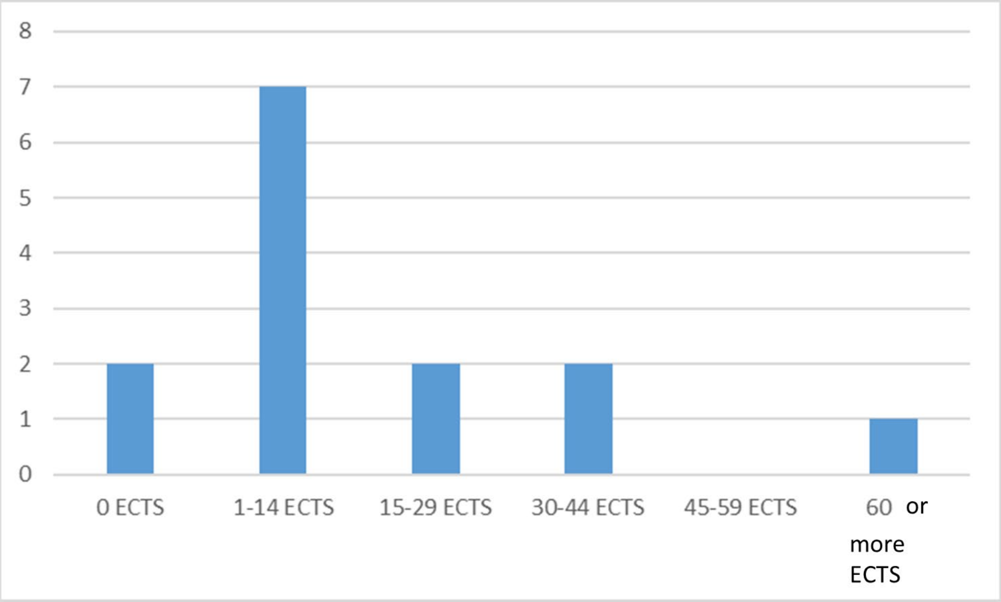


FIGURE 25. Number of cybersecurity courses in the degree programmes

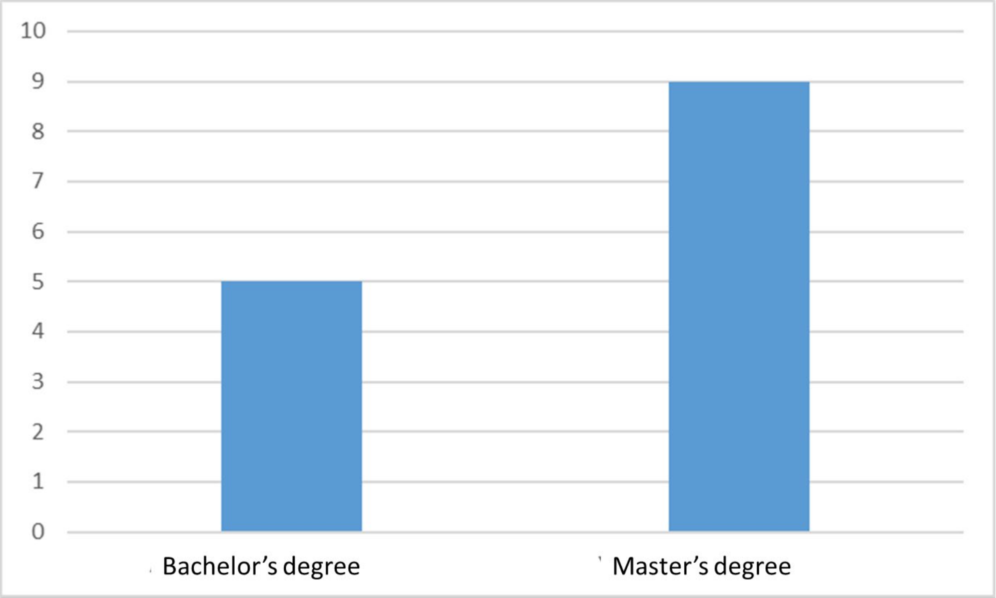


FIGURE 26. Distribution of degree programmes into bachelor’s and master’s degrees

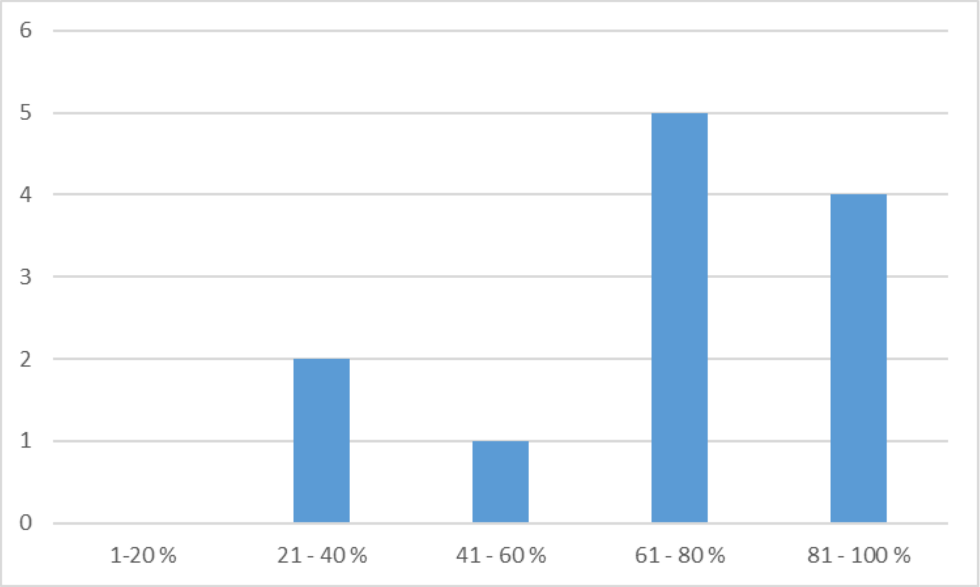


FIGURE 27. Estimated annual graduation rate of students relative to the initial intake of the degree programme

Most courses were offered at the master’s level. According to Figure 26, cybersecurity education at Finnish universities is concentrated in this level.

Respondents were asked to assess the annual graduation rate of students in relation to the initial intake in the degree programme. The results show that it is quite typical that the number of students graduating each year from the degree programme is lower than the number of admitted students (see Figure 27).

6.2 University analysis

6.2.1 Aalto University

Cyber education

Aalto University's Department of Computer Science has a Master's Programme in Computer, Communication and Information Sciences, which includes several major subjects/specialisations including Security and Cloud Computing (Security). This major subject/specialisation provides students with a broad understanding of the latest and future technologies concerning secure mobile and cloud computing systems. Students gain both practical engineering knowledge and theoretical insights into secure systems engineering, distributed application development, network and service architectures, and cloud and mobile platforms. The degree programme pays special attention to security and privacy issues as they are critical requirements in developing and deploying services in open networks and distributed systems. (See Aalto University, 2021.)

The specialisation offers several cybersecurity and information security courses as compulsory and elective studies. There were 194 applicants for the degree programme in 2022, of which 11 were selected.

Aalto University also coordinates the Erasmus Mundus Joint Master's Degree Programme in Security and Cloud Computing (SECCLO) with five other universities. The degree programme has a two-stage structure. During the first academic year, 60 ECTS are completed at Aalto University and during the second academic year, specialisation studies are completed at another collaborative university. The specialisation alternatives include communications systems (the Royal Institute of Technology in Sweden), information security (the Norwegian University of Science and Technology in Norway), reliable distributed systems (the Technical University of Denmark in Denmark), cryptography (the University of Tartu in Estonia), and Big Data security (EURECOM in France). Based on the degree programme's website, a total of 735 people applied for the degree programme in the first round (24 November 2021–05 January 2022), 76 of whom were selected as degree students. (See SECCLO, 2022).

Individual courses in cybersecurity and information security are also available as elective or compulsory studies in several other degree programmes. For these, the title of the degree programme is described and whether the cyber-related course in the degree programme is compulsory or elective.

Further education in the cyber sector

Aalto PRO (Aalto, 2022) offers training in various fields, both for those at the beginning of their careers and for those with a longer work history in demanding expert positions. A wide range of training courses are offered, including training in security management and digital security. Currently, at least the following security training courses are available:

- Diploma in Digital Security, 21 September 2022–08 March 2023
- Diploma in Safety and Security Management, 09 November 2022–17 May 2024
- Digital responsibility and technologies, social responsibility and ethics, 21 April 2022–22 April 2022

6.2.2 University of Helsinki

Cyber education

The University of Helsinki does not offer any degree programmes focused on cybersecurity or information security. However, it is possible to study cybersecurity and information security at the Faculty of Science as part of the master's programme in computer science. Students in the degree programme may specialise in information networks, which also includes courses focused on cybersecurity.

Bachelor's students of computer science must select either the basics of cybersecurity or the introduction to AI as a compulsory course. The basics of cybersecurity is also organised as an openly available MOOC. In addition, the master's programme in data science includes an optional course called "Trustworthy Machine Learning".

Further education in the cyber sector

The University of Helsinki (2022a) offers the MOOC on the basics of cybersecurity mentioned in the previous chapter. It does not currently offer any other further education in the cyber field. The continuing education company owned by the university's funds, HY+ Ltd. offers continuing education in the following subjects:

- Communication and interaction
- Leadership, management, and guidance
- Teaching and learning
- Wellbeing and health
- Sustainable development

HY+ also offers continuing professional training as well as specialist training in various fields (Helsingin yliopisto, 2022b).

6.2.3 Tampere University

Cyber education

Tampere University offers a specialisation called Advanced Studies in Information Security (80 ECTS). Degree programmes that offer specialisations in information security also have a number of other specialisation alternatives. The degree programmes offering this specialisation are the following:

- Master's Programme in Information Technology
- Master's Programme in Computing Sciences
- Master's Programme in Computer Science

The aim is for students to gain a good understanding of digital security and privacy; ability to assess the security and privacy of existing systems; ability to analyse, design, and implement secure systems; and ability to contribute to scientific research on security and privacy (Tampereen yliopisto, 2022a). The number of students selected annually for the specialisation is estimated to be 1 to 30.

The Faculty of Management and Business of Tampere University has a master's programme in security and safety management, which offers two specialisations:

- Safety Management and Engineering
- Security Governance

Students with a major in security governance will develop into experts in security governance and management in societies and communities in international, national, and local security environments in public organisations and the third sector. Students will be highly qualified professionals with a thorough understanding of security and safety management, risk management, governance, and leadership in both the public and private sectors at a local, national, and global level. (See Tampereen yliopisto, 2022b.) The degree programme had 45 applicants in 2022, of which 8 were selected.

Students specialising in safety management and engineering will develop their expertise in production, products, and services that involve the management of safety, health, and environmental risks. In addition, they will develop their expertise in corporate safety, risk management and planning, where typical tools are used. (See Tampereen yliopisto, 2022b.) The degree programme had 76 applicants in 2022, of which 8 were selected.

The Faculty of Engineering and Natural Sciences at Tampere University offers a master's programme in automation engineering, which has a number of specialisations, including information technology in automation. This specialisation includes courses linked to cybersecurity and information security as compulsory and elective studies. In addition, the degree programme includes courses where information security is not the main focus, but one part of the course content.

Tampere University also offers a number of smaller elective modules as part of the degree programmes. These include courses on cybersecurity and information security as elective studies, or alternatively courses where technology-related security is one part of the course content. These modules can be studied in several degree programmes. These modules include the following, at minimum: Intermediate Studies in Communication and Networking as free choice studies, Intermediate Studies in Health Informatics as free choice studies, Intermediate Studies in Aircraft Engineering as free choice studies, Intermediate Studies in Safety Engineering as free choice studies, Advanced Studies in Software Engineering as free choice studies, and Intermediate Studies in Communications Engineering as free choice studies. Individual courses in cybersecurity and information security are also available as elective or compulsory studies in several other degree programmes.

Further education in the cyber sector

Tampere University (2022d) offers a wide range of continuing education courses in several disciplines, but currently none are in cybersecurity. The fields of education of the continuing education programmes at Tampere University are the following:

- Management and leadership
- Health and welfare
- Education
- Technology

- Business and organisational development
- Culture and media

6.2.4 University of Jyväskylä

Cyber education

The Faculty of Information Technology at the University of Jyväskylä offers a master's degree programme in cybersecurity. The objectives of the degree programme are "to provide students with solid competence for working in demanding management and development tasks that require comprehensive mastery of cybersecurity. The programme examines the cyber world and its security from an administrative and technological perspective. The master's programme focuses on the areas of cybersecurity planning, leadership, and the management of information security risks from the perspectives of both management and technology" (Jyväskylän yliopisto, 2022a). The initial intake in the degree programme is 45 new students and it had 184 applicants in 2022.

The Faculty of Information Technology also offers a master's programme in security and strategic analysis, which includes courses related to cybersecurity. The description of the degree programme states the following: "The master's programme trains security experts with a wide range of competences who are able to analyse changes and phenomena affecting security in the global environment. The studies cover the security environment and its changes, crises and conflicts, and the role of globalisation, technological development, and digitalisation. A key part of the master's programme is also competence in strategic analysis: the master's programme provides the capability to acquire, process and analyse security-related information in order to understand, manage and predict an increasingly complex security environment" (Jyväskylän yliopisto, 2022b). The initial intake in the degree programme is 25 new students and it had 390 applicants in 2022.

The faculty also offers a master's programme in mathematical information technology, which includes two specialisations:

- Software and telecommunications technology
- Mathematical modelling in science and decision analytics

The specialisation in software and telecommunications technology offers cybersecurity and information security courses as elective studies. The faculty also has a bachelor's programme in information and software engineering, which includes courses related to cybersecurity and information security as compulsory and elective studies. The faculty also offers studies in computer science, educational technology, and cognitive science. In addition, it has two English-language master's programmes: Information Systems, and Cognitive Computing and Collective Intelligence.

Further education in the cyber sector

The University of Jyväskylä does not offer continuing education in cybersecurity and information security. It offers a wide range of continuing education, such as the Avance Executive MBA in management, studies in the Summer University, studies in educational leadership, continuing education projects aimed at teachers (Department of Teacher

Education), psychotherapy training, continuing education for PE and health studies teachers, and continuing education in ICT. At the time of the study, the university did not offer any cybersecurity courses as part of ICT continuing education for 2022. (See Jyväskylän yliopisto, 2022c.)

6.2.5 University of Turku

Cyber education

The University of Turku has degree programmes focused on cybersecurity and information security. Cybersecurity education is concentrated in the Faculty of Technology, which offers degree programmes in information technology – BSc (Tech) and MSc (Tech) – and computer science (BSc and MSc). Open for international applicants, the University of Turku offers a master's programme in information and communication technology, which offers the following major subjects starting in 2022:

- Cyber Security
- Cryptography
- Smart Systems
- Software Engineering
- Data Analytics

The cybersecurity major can be studied entirely in Turku. The degree programme is also part of the EIT Digital Master School Dual Degree Programme. The EIT Digital Master School is a two-year master's programme involving 20 European universities of excellence. Students begin their cybersecurity studies at one university. The first academic year provides all students with a common core of knowledge, and in the second academic year, students complete specialisation studies at another university. No other degree programmes in Finland participate in the EIT Digital Master School Dual Degree Programme. The cybersecurity major provides students with knowledge, expertise, and practical experience in security, technology, and networked systems. The specialisation focuses on networked systems and applications of the future. The technological topics covered include security of smart environments, system and network security, security of communication systems and applications, and designing secure systems. Students will explore both technological and theoretical scientific advances in the field and apply them to practice. The graduates will have a strong technological, theoretical, and practical understanding of cybersecurity. (See Turun yliopisto, 2022a.)

The cryptography specialisation aims to educate future experts in the field of research and ICT with a thorough and profound knowledge of the mathematical aspects of cryptography and cybersecurity. The cryptography specialisation offers a solid background in classical and modern aspects of mathematical cryptography. A deep understanding is developed of modern symmetric and asymmetric cryptosystems. Students are provided with strong academic education to proceed in post-graduate studies as well as to work as cybersecurity experts in the IT sector. The students learn to assess the strengths and weaknesses of cryptographic solutions based on a deep understanding of the underlying theory. The students also gain the ability to pursue applying cryptographic algorithms and protocols for real-life environments. (See Turun yliopisto, 2022b.)

The master's programme in information and communication technology had 522 applicants in 2022, of which 130 applied for the cybersecurity major and 13 for the cryptography major. In addition, the first round of the EIT Digital Master School had 16 applicants for the cybersecurity dual degree programme in spring 2022. The second round of EIT applications (for EU applicants) is still open at the time of writing. The initial intake for the cybersecurity major is 35 new students (including the intake for the EIT Digital Master School degree programme) and five new students for cryptography.

The Faculty of Technology also offers a degree programme in information and communication technology: MSc (Tech). The degree programme offers the following major subjects beginning in 2022:

- Communication and cybersecurity engineering
- Software engineering
- Smart systems
- Data analytics

Prior to the update of the curriculum in 2020, the major in communication and cybersecurity technology was focused on communications technology. As a result of a long development process, the degree programme has moved closer to the content of the cybersecurity specialisation and is now almost identical in content to it. The description of the degree programme states: "The Internet of Things and the sensoring of everything (e.g., smart spaces and cities), as well as autonomous systems/robotics, have brought a heightened need for expertise ICT and cybersecurity. The studies currently have a special focus on sensor networks, IoT and autonomous systems, as well as low-power solutions. Sector-specific specialisation can be done through a thematic module, for example, in data analytics, health technology, mechanical engineering, and intelligent and autonomous systems. In the thematic module, students can also focus on business and innovation activities, or expand their knowledge in cryptology and cybersecurity management." (See Turun yliopisto, 2022c.)

The initial intake for the programme in information and communication technologies – MSc (Tech) – is 30 new students. An estimated 6 to 8 of them will specialise in communications and cybersecurity engineering.

Through the joint application process, students can apply for joint study rights to both bachelor's and master's degree programmes in information and communication technologies, which have a joint initial intake of 120 new students. After completing the bachelor's degree, students can choose from a number of specialisations, including cybersecurity, cryptography, and communications and cybersecurity engineering.

Several other degree programmes also offer cybersecurity studies as part of the degree programme. The software engineering specialisation of the ICT programme – MSc (Tech) – includes compulsory and elective courses related to cybersecurity and information security. The faculty's master's programme in computer science (MSc) and its specialisation in interaction design allows for the choice of communication and cybersecurity engineering (20 ECTS) as one of the thematic modules. The major in information systems science at the Turku School of Economics also offers courses on cybersecurity.

Further education in the cyber sector

At the moment, the University of Turku does not offer further education focused on cybersecurity and information security. The University of Turku offers continuing education through the Brahea Centre and several faculties, with training in three categories in 2022:

- Migration and cultural diversity
- Sea and maritime
- Education

The following faculties of the University of Turku offer continuing education: Faculty of Education, Medicine, Law, Social Sciences, and the Turku School of Economics. (See Turun yliopisto, 2022d.)

6.2.6 University of Oulu

Cyber education

The University of Oulu does not currently have a degree programme dedicated to cybersecurity and information security. In contrast, several degree programmes offer courses on the topic as compulsory and elective studies. The Faculty of Information Technology and Electrical Engineering offers degree programmes in computer science and engineering: a Bachelor and a Master of Science (Technology). The bachelor's degree studies include artificial intelligence, applied computing, and computer engineering. The master's degree studies offer specialisations in AI, applied computing, computer engineering/hardware, and computer engineering/software.

Both degree structures contain cybersecurity courses either as compulsory or elective studies. Computer science and engineering offers several special courses in information technology, many of which in cybersecurity and information security. The university's Faculty of Humanities offers degree programmes in information studies (BA and MA), which also include courses connected to the cyber field.

Further education in the cyber sector

The University of Oulu (2022) offers continuing education in several different disciplines, including technology. The University of Oulu's special expertise in the field of technology includes fields such as 6G research, development of programming expertise, and project management competence. Cybersecurity and information security are taken into account as part of the DigiHealth continuing education programme (25 ECTS), which will be organised at least during the academic year 2021–2022. The studies are offered in the categories of continuous learning, further education, and non-degree studies. The study module provides comprehensive insights into medical device regulation and data security, the basics of digital healthcare, applications, and development, as well as to health data modelling and utilisation. The study module comprises the following courses:

- Medical Device Regulation and Quality Management 5 ECTS
- Connected Health and mHealth 5 ECTS
- Principles of Machine Learning in Medicine 5 ECTS

- Biosignal Processing 5 ECTS
- Basics in eHealth 5 ECTS

6.2.7 University of Eastern Finland

Cyber education

The University of Eastern Finland does not offer a degree programme dedicated to cybersecurity and information security. The Faculty of Science and Forestry offers degree programmes in computer science – BSc (Tech) and MSc (Tech). The bachelor's degree studies in computer science include "Introduction to Data Security" (5 ECTS). The master's programme in computer science offers courses in topics such as AI, pattern recognition, deep learning, machine vision, and eye tracking.

Further education in the cyber sector

The University of Eastern Finland (2022a) does not offer continuing education focused on cybersecurity and information security. The fields of continuing education offered at the University of Eastern Finland are listed below.

- Business growth and development
- Management and staff development
- Law
- Pharmaceutics
- Education
- Environment and technology
- Health and welfare
- Internationality

The university also offers specialisation studies and separate studies in several different disciplines, including the SmartICT specialisation training and a master's programme in automation technology – MSc (Tech). At the time of the study, the trainings did not include specialisations dedicated to cybersecurity. (See Itä-Suomen yliopisto, 2022b.)

6.2.8 Lappeenranta University of Technology (LUT)

Cyber education

LUT University does not offer a degree programme dedicated to cybersecurity or information security. The BSc (Tech) programmes in computational engineering and industrial engineering as well as the MSc (Tech) programmes in data analytics in decision making and operations management offer software engineering (20 ECTS) as minor studies. This module includes elective courses on the cybersecurity of software systems and fundamentals of software testing. These two courses connected to cybersecurity are also offered in the bachelor's studies in software engineering as well as in software and systems engineering (Lahti).

In addition, the master's programme in software engineering and digital transformation and the master's programme in product management and business

(Lahti) include the compulsory course “Requirements Engineering” (6 ECTS) and the elective course “Quality Assurance in Software Development” (6 ECTS).

Further education in the cyber sector

LUT University does not offer further education dedicated to cybersecurity and information security. The university offers the following programmes as continuing education: LUT EMBA, KATI 16 – Continuing Education Programme in Management, the Controller Expert Programme, the Expert Programme in Procurement Management, the Expert Programme in Knowledge Management, the Economics and Finance Programme, the Leadership and Management Programme, and the Expert Programme in Innovation Management (Lappeenrannan teknillinen yliopisto, 2022).

6.2.9 Åbo Akademi University

Cyber education

Åbo Akademi University does not have a degree programme dedicated to cybersecurity and information security. Individual courses on the topic are offered as compulsory and elective studies in several degree programmes. In addition, Åbo Akademi University offers an optional thematic module called *Safety-Critical and Autonomous Systems* in several degree programmes. The thematic module includes courses on cybersecurity and information security. Individual courses related to the cyber field are described in a separate table.

Further education in the cyber sector

Åbo Akademi University does not have further training focusing on cybersecurity and information security. At the time of the study, Åbo Akademi University offers at least two specialist education programmes:

- University pedagogy
- Forensic psychology

Åbo Akademi University has a Centre for Lifelong Learning (Centret för livslångt lärande, CLL), which is Finland’s largest Swedish-language adult education and training institute. The centre is run in cooperation between Åbo Akademi University and University of Applied Sciences Novia. The purpose of the Centre is to provide research-based development and training services in a number of fields. (See Åbo Akademi, 2022.)

6.2.10 University of Vaasa

Cyber education

The University of Vaasa does not offer a degree programme or study module dedicated to cybersecurity or information security. Individual courses linked to cybersecurity and information security are offered as compulsory and elective studies in several degree programmes, such as the bachelor’s programme in automation and computer science, and the master’s programmes in information systems and technical communication.

Further education in the cyber sector

At the moment, the University of Vaasa does not offer further education focused on cybersecurity and information security. It offers several Executive MBA programmes, one of which is focused on risk management and safety. These programmes offer two specialisation alternatives (Vaasan yliopisto 2022):

- Risk management process and methods in the business environment, 10 ECTS
- Development of risk management as part of legal obligations and compliance, 10 ECTS

6.2.11 University of Lapland

Cyber education

The Faculty of Law of the University of Lapland offers studies in administrative sciences and legal informatics. The Bachelor of Laws Degree contains one compulsory course in administrative sciences and legal informatics, whereas the Master of Laws degree contains two elective courses in legal informatics.

Further education in the cyber sector

The University of Lapland did not offer continuing education in cybersecurity and information security at the time of the study. Further training is available for professionals in the fields of education, law, and social services. The university also offers further education through the open university and MOOCs. (See Lapin yliopisto, 2022.)

6.2.12 National Defence University

The National Defence University offers studies in military sciences at the bachelor's, master's, and doctoral levels. It also offers post-graduate studies for general staff officers. Cybersecurity is addressed in both bachelor's and master's level courses, mostly in the master's programme.

6.2.13 FITech Network University

The Finnish Institute of Technology (FITech) was founded in 2017. It operates as a network university in the field of technology, and its founding members are seven Finnish universities, Technology Industries of Finland, and Academic Engineers and Architects in Finland. The University of Jyväskylä joined the network in 2019. The aim of the network university is to guide engineering experts to respond to competence demands arising in the field. (See FITech, 2022.)

Initially the FITech network was solely focused on serving the competence demands of industrial companies in Southwestern Finland. As a result, the FITech Turku project was founded in autumn 2017. FITech operations expanded to adult education along with the FITech ICT project, which aims to supplement the ICT competence of thousands of Finnish professionals. In addition, the FITech Energy Storage project was launched to meet the competence needs caused by the global energy transition. The latest project focuses on 5G studies. These projects, funded by the Ministry of Education and Culture, will continue until the end of 2023, with the exception of the FITech Turku project, which will conclude at the end of the academic year 2021–2022. (See FITech, 2022.)

Cybersecurity courses offered by network universities in the academic year 2021–2022 are

- Aalto University
  - Information Security 5 ECTS 14 Sept. 2021–28 Oct. 2021
  - Cybersecurity 5 ECTS 19 Apr. 2022–24 May 2022
  - Digital ethics and sustainability 1 ECTS 01 Mar. 2022–03 Jun. 2022
- Tampere University
  - Cybersecurity II: Specialisation 5 ECTS 10 Jan. 2022–29 Apr. 2022
  - Cybersecurity I: Basics 5 ECTS 13 Jan. 2022–31 Jul. 2022
  - Secure Programming 5 ECTS 10 Jan. 2022–31 May 2022
  - Standards, interoperability, and regulations in health informatics 5 ECTS 10 Jan. 2022–27 Feb. 2022
- University of Jyväskylä
  - System vulnerabilities 5 ECTS 10 Jan. 2022–13 Mar. 2022
- Lappeenranta University of Technology (LUT)
  - Personal data security, part 1: How we are tricked 1 ECTS, continuous
- University of Oulu
  - Data security 5 ECTS 11 Jan. 2022–13 Mar. 2022
- University of Turku
  - Privacy and Security for Software Systems 5 ECTS 25 Oct. 2021–20 Dec. 2021
  - System and Application Security 5 ECTS 30 Aug. 2021–24 Oct. 2021
  - Technologies and Security 5 ECTS 10 Jan. 2022–27 Feb. 2022.
  - Network Infrastructure Technologies and Security 5 ECTS 10 Jan. 2022–27 Feb. 2022
  - Protocol Processing and Security 5 ECTS 10 Jan. 2022–31 May 2022
- University of Vaasa
  - Management of Cyber Security 5 ECTS Spring 2022
  - FITech 5G 30 ECTS

The University of Helsinki and Åbo Akademi University did not offer cybersecurity education in the academic year 2021–2022. In turn, the universities of Lapland and Eastern Finland are not part of the FITech network university. (See FITech, 2022.)

6.3 Analysis of the interviews

The study included four interviews with cybersecurity experts from four universities. The interviews focused on topics such as the situation of cybersecurity education in the interviewee’s degree programme and overall views about cybersecurity education in Finnish universities.

Three interviewees stated that students’ interest in studying cybersecurity has increased in recent years in their degree programme. One interviewee did not address this topic. Interviewee 2 represented a degree programme where cybersecurity is not the main focus and said that the increase in interest is visible in concrete terms, for example, in students selecting information security as the topic of their bachelor's or master's thesis.

The responses highlighted the need for additional resources to promote and increase cybersecurity education in the degree programmes. In practice, the responses suggest that this could be seen as an increasing number of courses, but also as an increase in various practical training exercises in cybersecurity skills. One challenge related to resources was the recruitment of cybersecurity professionals in universities. Interviewee 4 mentioned that universities may not be able to offer competitive salaries compared to the private sector. Interviewee 3 mentioned that there are few cybersecurity experts in Finland whose skills meet the needs identified in the degree programme, such as the need for practical cyber exercises based on scientific knowledge.

The interviewees were asked to describe the current state of cybersecurity education in Finnish universities. The descriptions highlighted the fragmented nature and small quantity of teaching, and a near complete lack of teaching cooperation between universities. The development of cooperation was also seen as an area of development that merits additional resources. Interviewer 4 pointed out that the promotion of cooperation could be approached, for example, through a project that would create a network of higher education in cybersecurity, which would generate and intensify cooperation between different actors and stakeholders. Interviewee 3 also highlighted the development of international cooperation. They also stressed that in developing cooperation, care must be taken to ensure that it brings real added value to teaching. Interviewee 2 also highlighted the development of cooperation between cybersecurity experts in different universities. The interviewees also mentioned universities' areas of specialisation in cybersecurity and their importance. From the perspective of teaching, interviewees 1 and 4 pointed out that the cybersecurity courses currently offered by the universities would enable students to have more versatile specialisation options if cooperation in teaching were stronger.

Interviewee 3 highlighted the need to devote more resources to cutting-edge research, so that universities would focus on different areas of cybersecurity. They specified this by saying that the field for cybersecurity is very wide, which is why university specialisations should cover as many parts of the field as possible. In addition, the interviewee stated that it would be important to bring the discussion on cybersecurity to a more specific level, because at the moment the discussion concentrates on the general topic of cybersecurity, which does not reveal which areas Finland is currently good at and which need improvement.

Taking into account the aims and disciplines of their degree programme, the interviewees were asked about potential trends related to cybersecurity, the teaching of which should specifically require additional resources. Various topics were raised, which also testifies to the interdisciplinary nature of cybersecurity. In addition, interviewee 1 pointed out that trends could also be taught as a special course, but it is more important to focus on basic skills and good questions that enable students to face a variety of challenges in working life because in the long run, trends will change.

6.4 Conclusions and recommendations

Table 8 summarises the key degree programmes and trends in the field that were identified in the study. In addition, in the case of universities without a degree programme in cybersecurity, programmes close to the cyber field has been taken into account. The initial intakes and the number of applicants are not entirely accurate. This is because the figures do not take into account possible intakes via the open route and via transfer application. In addition to the joint right to complete a bachelor’s and master’s degree, it is often possible to apply only for a master’s degree, which has a separate quota. These factors make it difficult to estimate the definite intake numbers, making the figures indicative.

Table 8 shows that there are relatively few degree programmes dedicated to cybersecurity. Universities’ cybersecurity degree programmes or those closely related to the field vary in content. In other words, universities have different specialisations in cybersecurity. It is also noteworthy that the teaching is concentrated in the master’s level. Individual cybersecurity studies are generally available in a number of degree programmes as compulsory or elective studies.

Cybersecurity and security degree programmes based entirely in Finland and partly abroad have an estimated total intake of roughly 250 in 2022. Based on the study, we can estimate that the number of cybersecurity and security experts who graduate from universities each year is slightly lower than the intake. The above-mentioned figure only includes the initial intake of cybersecurity and security degree programmes and therefore excludes degrees in related fields, such as computer science. Overall, the number of experts produced by universities is relatively small when considering the identified skills shortage.

The number of applicants for key degree programmes in the field, such as the Master’s Degree in Cyber Security at the University of Jyväskylä, studies in Security and Cloud Computing (Security) at Aalto University and in Cyber Security at the University of Turku, show that cybersecurity as a field of education attracts significant interest.

At the time of the investigation reported here, Finnish universities offered little continuing education and specialist education in cybersecurity. The exception was Aalto University, which offered more further training in the field. Several cybersecurity courses can be studied in the academic year 2021–2022 through the FITech Network University. Its selection, however, consists of individual courses, and it does not offer entire study modules on cybersecurity.

The interviews revealed a lack of cooperation between universities in cybersecurity education, but the benefits of developing such cooperation were seen as significant. Additional resources would improve teaching, and this would be reflected, for example, in an increase of exercises developing practical cybersecurity skills. One challenge for resources identified in the interviews is the recruitment of experts in the field.

TABLE 8. Summary of key cyber degree programmes

University	Degree programmes/Key course modules	Intake 2022	Applicants 2022
Aalto University	Security and Cloud Computing (Security)	11	194
Aalto University	Security and Cloud Computing (SECCLO)	76 in the first round of applications	735 in the second round of applications
University of Helsinki	Master's Programme in Computing Sciences	45	452
Tampere University	Specialisation: Advanced Studies in Information Security 80 ECTS	1–30	-
Tampere University	Master's Programme in Security and Safety Management – Safety Management and Engineering	8	76
Tampere University	Master's Programme in Security and Safety Management – Security Governance	8	45
University of Jyväskylä	Master's Programme in Cybersecurity	45	184
University of Jyväskylä	Master's Programme in Security and Strategic Analysis	25	390
University of Turku	Cyber Security major + EIT Digital Master School Dual Degree Programme	35 (includes the intake for the EUT Digital Master School Dual Degree Programme)	130 + applicants for the EIT Digital Master School Dual Degree Programme
University of Turku	Cryptography major	5	13
University of Turku	Communication and cybersecurity technology major	Selected by an estimated 6–8 of the applicants for the master's programme in ICT.	The master's programme in ICT with several specialisations had 37 applicants.
University of Oulu	Information technology BSc (Tech) + MSc (Tech)	100 (DIA joint selection)	522 (DIA joint selection)
University of Lapland	Bachelor and Master of Laws	140	2,888
Åbo Akademi University	Thematic module: Safety-Critical and Autonomous Systems 20 ECTS	-	-
University of Eastern Finland	Computer science BSc + MA (Joensuu)	68	261
University of Vaasa	Automation and information technology BSc (Tech) + MSc (Tech)	52	279
LUT University	Information technology BSc (Tech) + MSc (Tech)	82	444 (DIA joint selection)

The number of cybersecurity experts in society can be increased by influencing several factors. One way is to increase the number and initial intakes of degree programmes in the field. However, these measures require an increase in human resources. In addition, the number of cybersecurity experts can be increased by developing university-level continuing education and the course selection of the FITech Network University. The University of Vaasa organised the FITech study module on 5G (30 ECTS), and along the same lines, similar study modules on cybersecurity could be offered in the future through the network university. In addition, improving educational cooperation between universities would enable students to acquire more versatile specialisations in different areas of cybersecurity.

This description of the current state of cybersecurity education at universities is not perfect. Cybersecurity education is offered in several faculties, and individual courses are offered in a number of degree programmes, which makes it difficult to gain a comprehensive view of the matter. As a result, some cybersecurity courses may not have been identified and some degree programmes may have been excluded if cybersecurity has been integrated in the structure of the degree programme. The picture could be improved in a further study that would categorise the existing cybersecurity courses in accordance with frameworks such as the Cybersecurity Curricula 2017 (CSEC, 2017) and the areas of cybersecurity defined in it: Data Security, Software Security, Component Security, Connection Security, System Security, Human Security, Organisational Security, and Societal Security. This would reveal if the teaching of these areas has quantitative differences between universities or if they are evenly distributed.

References

Aalto University (2022a). Koulutusohjelmat. Aalto University. https://www.aaltopro.fi/avoimet-ohjelmat

Aalto University (2022b). Security and Cloud Computing – Computer, Communication and Information Sciences, Master of Science (Technology). https://www.aalto.fi/en/study-options/masters-programme-in-computer-communication-and-information-sciences-security-and

CSEC (2017). Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. ACM, IEEE, AIS, IFIP. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

FITech. (2022). FITech. https://fitech.io/en/ Retrieved 20.01.2022

Helsingin yliopisto (2022a). Täydennyskoulutus. https://www.helsinki.fi/fi/hakeminen-ja-opetus/taydennyskoulutus Retrieved 06.04.2022

Helsingin yliopisto (2022b). Tutkintoa täydentävä koulutus. https://www.helsinki.fi/fi/hakeminen-ja-opetus/hae-tutkintoa-taydentaviin-koulutuksiin Retrieved 06.04.2022

Itä-Suomen yliopisto (2022a). Täydennyskoulutus. https://www.uef.fi/fi/taydennyskoulutus?gclid=Cj0KCQjwl7qSBhD-ARIsACvV1X2Qwd07cj6731Bk-

4IHI4Cpd9Y6071GL2jEdfYcceVisCHUzfsu9woaAl8oEALw_wcB Retrieved 20.01.2022

Itä-Suomen yliopisto (2022b). Erikoistumiskoulutukset ja erilliset opinnot. https://www.uef.fi/fi/erikoistumiskoulutukset-ja-erilliset-opinnot Retrieved 07.04.2022

Jyväskylän yliopisto (2022a). Kyberturvallisuuden maisteriohjelma, filosofian maisteri (2v). https://www.jyu.fi/fi/hakijalle/koulutustarjonta/kyberturvallisuuden-maisteriohjelma-filosofian-maisteri-2-v Retrieved 11.03.2022

Jyväskylän yliopisto (2022b). Turvallisuus ja strateginen analyysi -maisteriohjelma. https://opinto-opas.jyu.fi/2021/fi/tutkintoohjelma/tsama2020/ Retrieved 11.03.2022

Jyväskylän yliopisto (2022c). Täydennyskoulutus. https://www.jyu.fi/fi/jatkuva-oppiminen/taydennyskoulutus Retrieved 19.04.2022

Lappeenrannan teknillinen yliopisto (2022). Täydennyskoulutus. https://www.lut.fi/taydennyskoulutus#:~:text=LUT%2Dt%C3%A4ydennyskoulutus%20tuo%20yliopiston%20huippuosaamisen,my%C3%B6s%20tekniikan%20ja%20talouden%20rajapinnoilla. Retrieved 14.01.2022

Lapin yliopisto (2022). Jatkuva oppiminen. https://www.ulapland.fi/FI/Yhteistyo-ja-palvelut/Jatkuva-oppiminen Retrieved 18.03.2022

Oulun yliopisto (2022). DigiHealth-täydennyskoulutus. https://www.oulu.fi/fi/joy/koulutushaku/digihealth-taydennyskoulutus Retrieved 20.01.2022

SECCLO (2022). Selection results. https://www.secclo.eu/admission/selection-results/ Retrieved 15.03.2022

Tampereen yliopisto (2022a). Advanced Studies in Information Security. https://www.tuni.fi/opiskelijanopas/opintotiedot/opintokokonaisuudet/otm-31975feb-1d19-4168-aec5-183ea80a56e2?year=2021 Retrieved 10.01.2022

Tampereen yliopisto (2022b). Security Governance, Security and Safety Management. https://www.tuni.fi/en/study-with-us/security-governance-security-and-safety-management#expander-trigger--field-degree-study-objectives Retrieved 10.01.2022

Tampereen yliopisto (2022c). Safety Management and Engineering, Security and Safety Management. https://www.tuni.fi/en/study-with-us/safety-management-and-engineering-security-and-safety-management#switcher-trigger--information Retrieved 10.01.2022

Tampereen yliopisto (2022d). Täydennyskoulutus. https://www.tuni.fi/fi/tule-opiskelemaan/taydennyskoulutus?utm_source=google&utm_medium=cpc&utm_campaign=TAU_JOP_2020-2021_Taydennyskoulutus_GNX&gclid=Cj0KCQjwl7qSBhD-ARIsACvV1X2LGLAZXGADoeVjih3szRuYgioyhw0oHGp33UPy9Ju0sNHNlFxiE1IaAm34EALw_wcB Retrieved 01.03.2022

Turun yliopisto (2022a). MDP in Information and Communication, Cyber Security (Tech), 2020-2022. https://opas.peppi.utu.fi/en/programme/16075?period=2020-2022 Retrieved 12.03.2022

Turun yliopisto (2022b). MDP in Information and Communication, Cryptography (Tech), 2020-2022. https://opas.peppi.utu.fi/en/programme/16118 Retrieved 12.03.2022

Turun yliopisto (2022c). *Tieto- ja viestintätekniikka, Tietoliikenne- ja kyberturvallisuusteknologia (DI), 2020-2022. https://opas.peppi.utu.fi/fi/ohjelma/16282 Retrieved 12.03.2022

Turun yliopisto (2022). Turun yliopiston täydennyskoulutustarjonta. https://www.utu.fi/fi/opiskelijaksi/turun-yliopiston-taydennyskoulutustarjonta Retrieved 15.01.2022

Åbo Akademi (2022). Elinikäisen oppimisen keskus. https://www.abo.fi/fi/centret-for-livslangt-larande/ Retrieved 17.02.2022

Vaasan yliopisto (2022). Jatkuvan oppimisen koulutustarjonta. https://www.uwasa.fi/fi/koulutus/jatkuva-oppiminen/jatkuvan-oppimisen-koulutustarjonta?field_editors_target_id=All&lang=All&field_education_pricing_target_id=All&field=All&field_education_method_target_id=All&year=All&items_per_page=10 Retrieved 18.02.2022

7 Cybersecurity training by other educational providers

This section examines the provision and need of cybersecurity/digital security competence development for citizens. The study began with a survey and analysis of the current situation, after which material and a process aiming to strengthen the skills of citizens were designed based on previous data and reports, as well as ongoing projects.

7.1 Collection of data

Data on the current situation was collected from companies, the third sector (associations, organisations, liberal adult education), and state and municipal actors that provide cybersecurity training. Previous surveys (e.g., Lehto & Niemelä, 2019) have identified educational providers among which data collection started. The study also examined whether new providers have emerged.

The data was collected by searching the web, as well as through interviews and surveys. First, online material was used to create an overview of the current situation, which was then specified with surveys and interviews.

In the next phase of the study, interviews were carried out with organisations that provide a significant amount of cybersecurity training. The interviews provided more detail to data gathered online and also addressed ongoing training developments and the intended target audiences.

The study then proceeded to interviews with experts with an understanding of the current situation and the target state of cybersecurity training. These expert interviews were especially used in the assessment of development needs.

Finally, a survey form was sent to smaller organisations, which are numerous and do not particularly advertise providing cybersecurity-related training on a larger scale (adult education centres, summer universities, and local business organisations) in order to identify the extent to which cybersecurity training relates to their other educational content, among other topics.

7.2 Provision of education by the third sector

In the third sector, the most extensive training related to cybersecurity is organised by the National Defence Training Association of Finland (MPK). In addition, some adult education centres provide training related to cybersecurity, but the training provided by organisations such as business associations is sporadic and very limited.

National Defence Training Association (MPK)

The MPK is a strategic and operational partner of the Defence Forces. It participates in national preparedness and information and educational work regarding security issues. The information presented here is based on an interview with an MPK representative, the MPK Cybersecurity Training Programme (Maanpuolustuskoulutusyhdistys, 2021), and the information found on the MPK website.

In 2022, the MPK has established itself as a cybersecurity educator for citizens, and it trains thousands of people every year. The aim of cyber training is, on the one hand, to provide ordinary citizens with basic skills and, on the other hand, to provide training that serves military capabilities and to create cyber expertise in the Defence Forces reserve. The MPK organises low-threshold training for everyone at affordable prices and has the potential to increase the number of trainees. However, the problem is that people who are unaware of cybersecurity issues also lack information on how to access training. The MPK has created a cybersecurity training programme with the following parts:

1. Training module on basic cybersecurity competence
2. Training module on advanced cybersecurity competence
3. Training package on the application of cybersecurity competence
4. Training led by the Defence Forces and other training activities
5. Cybersecurity trainer training

Basic courses are generally informational or preparedness courses that are open to everyone, and advanced and special courses are mainly courses that serve military preparedness. Basic knowledge is a requirement for advanced and special level courses, which participants may have acquired through their civil profession or through the training path of MPK courses. The association also organises other training courses and seminars related to cybersecurity. Anyone can participate in the basic courses, and no prior knowledge is required. (See Maanpuolustuskoulutusyhdistys, 2021.)

The description of the MPK training programme states that its aim is to provide reservists and other citizens with an ascending cybersecurity training path, which meets the needs of Finnish society and its overall security, as well as the needs of the Defence Forces in terms of cyber competence. The cyber education programme also has an informational and educational perspective. According to the law, the training offered by the MPK takes the forms of publicity and education provision, preparedness and security training as an independent association, and training that promotes military preparedness under the guidance of the Defence Forces, provided as a public administration organisation. The online material of the first course of the training programme is freely available to all citizens for independent skills development. In addition, the MPK has published together with the University of Jyväskylä a guide on cybersecurity aimed at all citizens called *Kyberin taskutieto – keskeisin kybermaailmasta jokaiselle* (Cyber Pocket Information – The Core of the Cyber World for Everyone). It contains key cybersecurity tips that can be useful for anyone in their everyday life and in preparing for crises. (See Maanpuolustuskoulutusyhdistys, 2021.)

The challenge of MPK training is that people who need it do not necessarily seek it. The national defence dimension of the association can also deter some people. Courses may be difficult to find unless a person already knows about the MPK, and people may be unaware that they do not need to be reservists to participate. In other words, they may not know that the courses are available to them.

The challenge is therefore to communicate about the training to all those who are interested, which would require more extensive marketing. This applies both to cybersecurity and other training courses. One solution would be to gather all information about openly available training in one place so that it would be easier to find. For example, a website dedicated to cyber information and training could be set up for this purpose. (Sources: Interviews with Panu Moilanen, the MPK website, the MPK training programme)

Women's National Emergency Preparedness Association

The Women's National Emergency Preparedness Association organises training together with its partners, such as the MPK, the Defence Forces, the Lotta Svärd Foundation, the National Defence Support Foundation, Vapepa, SPEK, and the Kova Committee.

The training offered by the Association includes safety-centred courses on current topics for women. Each year, it organises two major NASTA training exercises as well as several smaller PikkuNASTA training exercises. Currently, the Association offers a course related to information influence, which introduces participants to different forms of information influence, information warfare, and protection against propaganda. (See Naisten valmiusliitto, 2021.)

The Finnish Association for the Welfare of Older People (VTKL)

The SeniorSurf website encourages senior citizens to use computers and the Internet. The website contains instructional materials and information on how to make an appointment for guidance in person. The website and the in-person guidance also address cybersecurity skills. (See Vanhustyön keskusliitto, 2021.)

Chamber of Commerce

On its website, the Finland Chamber of Commerce provides all Finnish businesses the Cyber Security Guide for Business produced by the International Chamber of Commerce (ICC). The guide is aimed at business owners, employees, and managers (Keskuskauppakamari, 2015).

The Chamber of Commerce also provides on its website an online training course on information security for a fee. In addition, local Chambers of Commerce have organised or are organising individual cybersecurity training courses. For example, the Tampere Chamber of Commerce has organised courses in preparing for security risks and in reacting to a data trespass. (See Kauppakamari, 2021.)

Suomen yrittäjät

Suomen yrittäjät, an interest and service organisation for SMEs, has occasionally offered cybersecurity training. However, the courses have had to be cancelled due to a low number of enrolments. The organisation did not respond to the present survey. Cybersecurity and information security are perhaps incorporated into other ICT courses, in which case they may not be recognised as distinct from other topics.

7.3 Adult education centres and summer universities

There are 177 adult education centres and 18 summer universities in Finland. Based on information published online, many of them offer some training related to cybersecurity, information security or digital security. We carried out a survey in order to investigate the available training courses in more detail and to also include courses that are being planned. The survey was sent to all adult education centres and summer universities, of which 39 responded.

7.3.1 Analysis of the survey responses

1. Do you currently offer courses that are mainly dedicated to cybersecurity, information security or digital security?

   - Yes: 10.3% of respondents
   - No: 89.7% of respondents

2. What kind of courses and what are their contents? Course name, brief description of content, and target audience.

   - Information security and cybersecurity: crime and scams on the Internet
     - In this lecture, you can learn the basics of information and cybersecurity from the perspective of ordinary people and get information about the kinds of crimes and scams that are committed over the Internet.
   - Digital workshop on information security
     - Information security is important in today's age of multiple devices and accounts. Join the workshop and learn how to avoid the worst pitfalls and set up secure passwords among other topics.
   - Course on e-services
   - Everyday IT
   - Competitive skills course

Information security is also often addressed in basic courses on tablets, computers, and smartphones. The target group consists of senior citizens; topics mainly cover issues related to IT security. Usernames, passwords, authentication. Viruses, worms, malware, etc. Course titles vary. In addition, short lectures on information security have been offered.

3. Are issues related to cybersecurity, information security or digital security discussed as part of another course?

   - Yes: 64% of respondents
   - No: 36% of respondents

4. In which courses are these topics addressed? The names of the courses, brief description of the content related to cybersecurity, and the target groups.

   - Digital courses targeted at senior citizens cover information security issues in general.
   - Information technology clinics.

Course description: The student is offered three 45-minute sessions of teaching as individual instruction. Students bring their own personal devices (laptop, tablet, or smartphone) that they want to learn to use better. The course is tailored to the student's needs. This course is also suitable for beginners.

The target group is all citizens using IT devices (smartphone, tablet, computer), but especially older people, for whom the use of smart devices is a new challenge. Information security is a central topic in these courses. Training focusing solely on information security has been organised in the past, but today it is integrated into device training.

5. Are you planning to increase the range of training related to cybersecurity, information security or digital security in the future?
    - Yes: 43.6% of respondents
    - No: 56.4% of respondents
6. What kind of training content are you planning, and for which target groups?

Training has been planned for senior citizens and, for example, working-age people as continuing education. In addition, there are plans to organise training for teachers. On the other hand, training providers would also need more information on the topic, as they may not be able to plan training in the subject area.

7.3.2 Challenges and development needs

Adult education centres have an extensive student base and established marketing channels for their courses. However, only a few respondents currently provide training related to cybersecurity, information security or digital security.

The current contents are suitable for acquiring basic skills, and these basic courses should be made available more widely in different adult education centres. Cybersecurity is currently addressed in 64% of the respondent organisations as part of other courses, but this portion should be increased if courses specifically dedicated to cybersecurity themes cannot be organised due to a lack of resources or other reasons.

Many senior citizens study at adult education centres, and courses designed for them are, in fact, on offer. Adult education centres are also familiar places of study for many senior citizens. It would therefore be a good idea to organise and market more training content that reaches them in these educational institutes.

Less than half of the respondents planned to increase training related to cybersecurity, information security or digital security in the future. It is worth noting, however, that the survey was carried out at the end of 2021. The situation may since have improved, as the war in Ukraine has given cyber issues significantly more media coverage and attracted public interest.

Those who planned to increase training mentioned topics such as continuing education for people of working age and on-demand training, both of which are needed, since employees of SMEs in particular may not have access to training for economic reasons, and adult education centres offer inexpensive, low-threshold training.

The responses also mentioned that smaller communities lack interest in participating in cybersecurity training and that adult education centres themselves lack sufficient information about providing training in cybersecurity.

7.4 Cybersecurity training by state and municipal organisations

Finnish Institute of Public Management HAUS

HAUS maintains the eOppiva site, which is a joint learning platform of the central government. The courses are intended for government employees, and access to the learning environment requires a login. However, eOppiva also provides freely available courses.

HAUS offers cybersecurity courses and courses that include cybersecurity content (the term *digital security* is used on the website) (HAUS, 2021).

Since HAUS is a significant training provider, it was interviewed on their current and planned cybersecurity-related training. HAUS's target group is especially those working in public administration, although the courses in eOppiva are largely open to everyone and could be used by SMEs or other organisations if they so wished.

HAUS started training related to the cyber world, more precisely data protection, in 2018. Since then, the range of courses they offer has expanded to a wide range of cybersecurity areas. HAUS markets the courses to its target groups, and some of the courses are what could be called mandatory for them.

HAUS plans to increase cybersecurity training in the future. If possible, they will also organise non-web-based training on the topic. For example, joint training over Teams and coaching sessions could be organised for experts, and more advanced training and longer modules could also be offered as a form of further education that prevents cyber threats for people working in critical positions. The cybersecurity training offered by HAUS reaches more than 100,000 people. More than 50,000 courses have been completed by April 2022.

HAUS continuously measures its training activities, for example, through participant feedback. Participants are very satisfied with the courses (on a scale of 1 to 5, a total of 92% of respondents give a grade of 4 or 5). The content is also considered useful for the participants' work. The participants gave positive feedback on the content, which they said was presented in an interesting way, and they said the questions or assignments help them consider the topics in practice. The trainees especially liked the videos that were included in the online courses. (Source: Interview with Petteri Kallio, PhD.)

Digital and Population Data Services Agency

The Digital and Population Data Services Agency offers training courses called Digitally Secure Life. Their aim is to teach citizens how to operate safely in the face of threats in the digital world. The training includes online courses for the management of organisations, digital security experts and all organisation personnel. The training is complemented by a mobile game that allows trainees to practice digital security skills in practical situations. The training module is freely available and free of charge. (See DVV, 2021.)

In addition, the agency has a JUDO project, which aims to develop the management of digital security in public administration and the digital security competence of personnel and to provide support for the development of safer services. The project supports public administration in developing safe and reliable services in 2019–2023. The project has produced outputs such as webcasts and workshops, where experts explain best practices and give concrete advice on how to implement digital security. (See DVV, 2021.)

The TAISTO exercises are also part of the activities of the agency. In these digital security exercises, public administration personnel practice operating in cybersecurity incidents through imaginary situations (DVV, 2021).

National Emergency Supply Agency

In cooperation with other organisations, the National Emergency Supply Agency organises the nationwide *Tieto* exercise. It is a cooperation exercise between companies and authorities in the event of large-scale cyber incidents. The exercises are held every two years and are specifically targeted at selected industries. The exercises support companies' continuity management and preparedness and develops contractual cooperation. (See Huoltovarmuuskeskus, 2021.)

Defence Forces

The Finnish Defence Forces have separate cyber conscript training. Cyber conscripts receive instruction from cyber defence professionals and get access to jobs related to cybersecurity. During the service, conscripts participate in blue team / red team training activities, build services and test their safety, and carry out programming projects. (See Puolustusvoimat, 2022.)

In addition, the Defence Forces have established a school of management systems, which serves as an industry school for the management systems industry, cyber defence, and information defence. The school supports the activities of the Finnish Defence Forces and cooperates closely with the National Defence University and the schools of the different branches of the Defence Forces in matters related to the school's area of responsibility. (See Puolustusvoimat, 2021.)

7.5 Cybersecurity training provided by companies

2NS

2NS offers basic level training for personnel and information security training for software developers. The information security training for personnel is sold as an online training product called Cyber Study, which is intended for both private companies and public organisations. Cyber Study is available in 14 languages and the product has about 100,000 users. The training allows students to learn about different information security situations through humour and to test their skills. (See 2NS (2022).)

Almatalent

Almatalent (2021) trains experts and decision-makers live and online. The following training units are related to cybersecurity in companies:

- Privacy courses, information security courses related to products (such as MS365)
- Privacy Pro Certificate
- Certified Information Privacy Professional/Europe (CIPP/E)
- Certified Information Privacy Technologist (CIPT)
- IT risk management
- Training programme for data protection officers
- Certified information privacy manager
- Carry out a successful cyber exercise

Arrow ESC

Arrow ECS is the only official EC-Council training centre in Finland. The purpose of the hacking and security courses produced by the EC-Council is to expand the competence of IT experts regarding security threats and their protection (Arrow ESC, 2021).

Arter

The company offers courses for information security professionals. Course offered: ISO 27001:2017 Building an Information Security System (Arter, 2021).

CGI

CGI provides personnel training for companies related to cybersecurity, among other topics. In addition, the company offers a cybersecurity-focused, mobile escape room game. The escape room game can be delivered to an organisation's parking lot anywhere in Finland. The game is tailored to the organisation's security guidelines. (See CGI (2021).)

Cyberwatch Finland

Cyberwatch Finland provides e-training services and consulting to improve cyber awareness and competence at all levels of an organisation. They offer a game exercise in cyber management, which produces competence at the strategic level of cybersecurity. They also offer training packages tailored to each company. (See Cyberwatch (2021).)

Elisa Santa Monica

Elisa Santa Monica (Elisa, 2021) offers courses and training services under the name SantaCare Training Services. The cybersecurity-related courses they provide include the following:

- Information security training for personnel
- Orientation of management and supervisors to corporate cyber threats and threat protection
- Introduction to cyber threat prevention
- Cyber threat intelligence and threat hunting
- Basics of cybersecurity of production networks
- Corporate network security

F-Secure

Cyber Security Base with F-Secure is a series of courses organised by the University of Helsinki in cooperation with the F-Secure Cyber Security Academy. The series focuses on building core knowledge and capabilities related to the work of a cybersecurity professional. The course series is free and openly available. It does not require enrolment and allows an unlimited number of participants. (See MOOC.fi, 2021.)

In addition, F-Secure (2021) offers custom-tailored training to companies, as well as established professional-level courses and Capture the Flag events. Established course contents include the following:

- Proactive Web Defence
- Proactive Network Defence
- Proactive First Response
- Proactive Mobile Defence

Granite

Granite (2022) offers training on the basics of information security for company personnel. According to the website, the training service has more than 200,000 users. The course modules include the following:

- Basics of Information Security 1: Technological security
  - Online training on the technological basics of information security for all personnel.
- Basics of Information Security 2: Information security at work
  - The principles of information security in the workplace as an easy-to-understand online course.
- Basics of Information Security 3: Everyday life and commuting
  - Principles of information security through practical examples for the needs of all personnel.
- Basics of Information Security 4: Information security when working remotely
  - The most critical security issues of remote work as a clear online course.

Insta

Insta provides cybersecurity training for company personnel. The training offered by Insta is mainly intended for IT professionals, but it also arranges more basic-level training for companies on order. The courses mainly consist of further training courses related to safe application development. In addition, Insta conducts dozens of cybersecurity exercises a year. This type of training is planned to be continued in the future.

Cybersecurity skills should be civic skills, and training should start at the primary school level. The public sector could offer more training related to citizens' skills and their own personal information security. Many people receive training at work, at least in larger companies. For employees of smaller companies, there is plenty of free training content available, but it is often difficult to find. (Sources: Insta, 2021; interview with Elina Niemimaa.)

JYVSECTEC by JAMK

JYVSECTEC (Jyväskylä Security Technology) is a research, training, and development centre for cybersecurity and AI development that belongs to the Jyväskylä University of Applied Sciences. JYVSECTEC offers cybersecurity courses and cybersecurity exercises for companies and the public sector. JYVSECTEC has developed a national cyber range in Finland, which is a technical training and exercise infrastructure for cybersecurity. The national cyber range environment called RGCE (*Realistic Global Cyber Environment*) is used in almost all courses and exercises organised by JYVSECTEC.

JYVSECTEC offers versatile training in various areas of cybersecurity and information security. The purpose of the training is to increase the knowledge and skills of personnel to adapt to the constant change in digitalisation and to cyber threats. The training develops the participants' competence in selected subjects with modern training methods and practical exercises. The offered courses include Ethical Hacking and Penetration Testing (3 days), Threat Hunting (2 days), Cyber Incident Response (2 days), Cyber Security Operations Centre (3 days) and additional training packages customised to customer needs.

JYVSECTEC organises cybersecurity exercises for companies and the public sector. Since 2013, JYVSECTEC has organised the national cybersecurity exercise KYHA. The need for and number of KYHA exercises has increased every year, and in 2022, four national KYHA exercises will be organised (Security Authorities, Central Government, Health Care, as well as the Municipal Sector and Critical Infrastructure). In addition to the KYHA exercises, JYVSECTEC offers cybersecurity exercises for companies and the public sector. These include Live Exercise, Digital Forensics and Incident Response (DFIR) Exercise, and Threat Hunting Exercise.

JYVSECTEC also offers the Finnish Cyber Security Certificate (FINCSC). FINCSC is a certification system created for companies and other organisations to secure information and ensure business continuity. It is specifically targeted at the SME sector but is suitable for organisations of all sizes and all fields. Especially in terms of training needs, it is worth noting that the FINCSC certification provides a comprehensive situational picture of an organisation's level of cybersecurity. (See JYVSECTEC, 2022; FINCSC, 2022.)

KPMG

KPMG (2021) offers security courses and training programmes. The courses either aim at a vocational qualification such as CISSP, CISM or CPTE or relate to a specific topic, such as the role of the data protection officer. The trainers are information security and data protection experts at KPMG. The training includes the following courses and programmes:

- Preparatory training courses for vocational qualifications in information security (CISSP, CISM, CPTE)
- Comprehensive training programme in information security, 10 days (or individual training courses)
- Training programme in information security in application development
- Information security in automation
- Management of data protection risks in an organisation
- Information security seminars and current events
- Information security or data protection orientation for all personnel
- Information security of procurement/application development
- Training programme for data protection officers
- Regular and continuous training programmes (e.g., every two months per subject or target group).

Navisec

Navisec offers information security and data protection training online for different target groups. The training courses are especially aimed at companies, municipalities and public organisations, social and health care services, education providers and early childhood education and care providers. Navisec (2022) offers the following training:

- Information security and data protection training for personnel
- Information security and data protection for employees' representatives
- Secure information management
- Information security and data protection in social services
- Information security and data protection in education
- Information security and data protection in early childhood education and care
- Secure password checklist

Nixu

Nixu offers customised training and cyber exercises for organisations' personnel. The training consists of lectures, exercises, group work, and games, among other activities. Nixu also provides training materials and e-learning products for personnel training. The training also includes services such as the simulation of phishing attempts and information security escape rooms. The training is designed to meet the customer organisation's needs and, when requested, to meet certification requirements. Nixu also organises data security events and provides services for the development of personnel's data security awareness. The cyber exercises are tailored to the needs of the client organisation; the exercises range from extensive functional exercises to smaller-scale desktop exercises. (See Nixu, 2021a.)

The Nixu Challenge traineeship programme gives young people the opportunity to work in genuine cybersecurity jobs alongside Nixu professionals. The application for the traineeship programme begins with solving a technical challenge, which allows candidates to demonstrate their technical skills and problem-solving abilities. (See Nixu, 2021b.)

Recruitment training for the cybersecurity industry is also available through the AW Academy. The training lasts for 12 weeks, after which the trainees start working for Nixu as trainers. (Source: Interview with Anu Laitila.)

Professio

Professio provides cybersecurity-related training, especially for IT professionals, for both public and private sector needs (Professio, 2022).

Salus Qualitas Consulting

Salus Qualitas Consulting is a consultancy and training company specialising in safety and quality. The company's services include information security and data protection training in the field of social welfare and health care (Salus, 2021).

Saranen Cyber Security Academy

Saranen Cyber Security Academy is a recruitment training programme in the field of information security. The five-month training programme includes contact teaching, distance learning, and on-the-job learning. The aim of the training programme is to enable students to be employed in partner companies in different job roles. The training is primarily targeted at clients registered as unemployed who have completed a higher education degree in ICT or have the corresponding professional skills through previous work experience and who wish to develop their skills. (See Saranen, 2021.)

Silverskin

The Silverskin Academy offers cybersecurity training for companies. Its cybersecurity awareness training develops motivation and the ability of individuals to detect cyber risks and operate safely in everyday life. Training courses for administration and specialists are designed to develop the organisation's capability and defence skills. Silverskin (2021) offers the following training courses:

- Cybersecurity awareness
- Safe application development
- Practical exercises
- Cybersecurity demos
- Lectures and reviews

Sovelto

Sovelto provides information security training for the needs of organisations. The training includes a wide range of courses on topics such as web service vulnerabilities, database security, PKI, and certificates (Sovelto, 2021).

Sulava Oy

Sulava is an official training partner with Microsoft, offering class-form and online training, surveys, testing, lectures, and training materials. It offers training courses on Microsoft 365, which also address security issues, as well as more general training sessions such as "Information security for remote workers" (Sulava, 2021).

7.6 Other actors

Technology Industries of Finland

The MyTech programme offered by Technology Industries of Finland is a learning module aimed at lower and upper secondary schools and vocational schools. The programme includes a cybersecurity escape game that was published in collaboration with MAOL, the Finnish association for teachers of mathematical subjects. This is a virtual learning unit in which young people get to know the world of cybersecurity, the cybersecurity industry, and related professions in the form of an escape game. (See Teknologiateollisuus, 2021.)

The Finnish Information Processing Association TIVIA

TIVIA organises IT trainings on various topics. Some of the courses are organised by TIVIA and some by its partners. The training content also includes information security. (See TIVIA, 2021.)

7.7 Models from other EU countries

The National Cyber Security Index (NCSI) measures the cyber capability of different countries. Finland ranks tenth in the list, and the EU countries ahead of Finland are 1. Greece, 2. Lithuania, 3. Belgium, 4. Czech Republic, 5. Estonia, 6. Germany, 7. Portugal, 8. Spain, and 9. Poland (NCSI, 2022).

Greece

The Greek Cybersecurity Strategy states that appropriate and targeted cybersecurity awareness training should be provided to citizens. This work should make use of different channels to ensure that education reaches different target groups. Greece has established a "user-citizen" cybersecurity programme, and its implementation is supervised by the national cybersecurity authority. The programme includes information campaigns and training in cooperation with universities. (See Cyberwiser, 2022; Greek Republic Ministry of Digital Governance 2020, 12.)

Lithuania

The Lithuanian Cybersecurity Strategy emphasises the creation of a national cybersecurity culture, and places responsibility not only in the public sector but also in the private sector, to ensure that businesses and other organisations would ensure citizens' cybersecurity skills. Training is offered for public sector employees, and the number of trainers increases every year (Ministry of National Defence Republic of Lithuania, 2018, 12–13).

Belgium

The Belgian Cybersecurity Strategy states that different training courses focusing on cybersecurity should be tailored to different age groups and citizens with varying levels of competence. Campaigns to raise cybersecurity awareness should also be organised. The Centre for Cybersecurity Belgium (CCB) provides guidance and training material on cybersecurity in the home and for schools, the government, and sectors critical to society. Belgium has a website (www.sefeonweb.be) for the coordinated collection of information and training. Belgium's national cybersecurity responsibilities are fairly well defined. The CCB is responsible for managing projects, coordinating cooperation, and raising awareness of threats and protection against them. It also regularly consults Internet service providers on how to increase cybersecurity for citizens. (See CCB (2021).)

Czech Republic

In the Czech Republic, efforts are being made to raise awareness of cybersecurity in all aspects of citizens' lives. Continuing education in the form of non-degree studies is offered especially to teachers, so that they are better able to teach their students. In addition, public sector employees are trained in cybersecurity. Older people are offered training in the safe use of technology and the identification of disinformation. In addition, all high-risk groups need customised training, regardless of age. The Czech Republic also conducts either expansive or more targeted cyber awareness campaigns. The public sector cooperates extensively with the private sector, academia, and the third sector in education and awareness work. (See National Cyber and Information Security Agency, Czech Republic, 2021, 18–19.)

Estonia

In Estonia, cybersecurity awareness and competence in both the private and the public sector need to be developed so that everyone understands their responsibilities. The Ministry of Education and Research is responsible for planning lifelong learning activities, including the development of cyber competence. In Estonia, the goal is to create a "cyber-literate society". A common platform is being planned that contains material for independent study. Similarly to Finland, Estonia has also faced the challenge of knowledge and education being dispersed and fragmented. In the future, the main responsibility for raising public awareness lies with the Estonian Information Security Authority (RIA). More targeted training will also be provided for key people. Currently, the RIA regularly organises educational campaigns for citizens. For example, in 2019 they focused on training the older population and in 2020 on small and medium-sized enterprises, on remote working skills and on reskilling seniors. (See Republic of Estonia Ministry of Economic Affairs and Communications, 2019, 65–71; Republic of Estonia Information System Authority, 2021.)

Germany

In Germany, the aim is to focus on ensuring that small and medium-sized enterprises, training providers, organisations, foundations, and ordinary citizens acquire the necessary knowledge and skills to operate safely in the digital environment. The training takes place not only in formal educational institutions, but also in the workplace. In addition, target-group-specific training content is available to users. In Germany, it is also possible to obtain a "DsiN digital driving licence" certificate for digital skills (including safety skills). A number of projects are also under way to improve the cyber skills of certain target groups, such as senior citizens in sparsely populated areas. (See BMI (2021).)

Portugal

Portugal has launched a National Digital Skills Initiative e.2030. Part of this project aims to improve citizens' cybersecurity skills. However, this work will also be done separately by cybersecurity organisations. Educational content and information are provided especially for children, young people, senior citizens, and other groups at risk.

Cybersecurity training programmes are also offered to organisations and ordinary citizens. (See Portugal Resolution of the Council of Ministers, 2019, 2891–2893.)

Spain

In Spain, awareness-raising campaigns are conducted for citizens and businesses, and tailored information and training is provided for different target groups. Particular attention is paid to self-employment and to small and medium-sized enterprises. In addition, efforts are being made to increase the understanding of cybersecurity, in particular among managers of organisations, so that they can better understand what measures and training are needed to protect their organisations. Cooperation is carried out with the media in order to reach young people in particular. (See Gobierno De Espana, 2019, 56–57.)

Poland

In Poland, the continuing training of teachers in cybersecurity is seen as important for educating citizens who recognise threats and know how to operate in the digital world. The government aims systematically to raise citizens' awareness of cybersecurity in cooperation with the third and private sectors. Training is organised on topics such as the rights and obligations in the digital environment, the rights of victims of cybercrime, and the rights of victims of data leakage or other privacy violations. Cybersecurity campaigns are targeted at different target groups, such as children, parents, and senior citizens. Efforts are being made to educate citizens so that they can identify disinformation and attempts to influence. (See Ministry of Digital Affairs Poland, 2019.)

7.8 Ongoing development projects

Digivisio 2030

According to the project description, Digivisio is a joint project of all Finnish higher education institutions, which opens national learning data reserves for use by individuals and society (Digivisio, 2022). The ecosystem created in the project will also bring educational content to the use of companies and society. The aim is also to enable each learner to accumulate their competence in a meaningful way. The aim is to provide content for continuous learning. (See Digivisio, 2022.)

The Cybersecure Europe Project

The Ministry of Transport and Communications and Aalto University are carrying out a project that aims to create a common training package on cybersecurity civic skills for EU countries. The project will map the current situation across the EU and build on this work to create an open website with educational material in all EU languages. The project begins in 2022 and continues until the end of 2024. (See Liikenne- ja viestintäministeriö, 2022.)

Digital Compass

The Digital Agenda of the European Union aims to harness digitalisation to serve people and businesses and to support the goal of making Europe climate neutral by 2050. To support this, the European Commission proposed an EU digital compass in March 2021. In September 2021, the Commission presented an action plan to implement the objectives and to oblige the Member States to draw up their own roadmaps. The digital compass is divided into four areas: competence, secure and sustainable digital infrastructures, digital transformation of businesses, and digitalisation of public services.

Finland's digital compass is based on that of the EU and the corresponding proposal for a policy programme, which sets out the requirements for national roadmaps. A decision on the programme is expected in autumn 2022. The Finnish digital compass contains national targets to support the achievement of the objectives of the EU's digital compass. In addition, the digital compass gathers national goals and themes complementary to the EU compass, which are necessary to accelerate Finland's digitalisation development and for which Finland wants to be known.

7.9 Conclusions and development proposals

7.9.1 Current state

Non-degree studies in cybersecurity are available in Finland, but currently those most in need of education will not find it, nor will they seek it. For example, there is very little training aimed at senior citizens.

Children and young people currently receive training in cybersecurity as part of their educational pathways, in both primary and lower secondary education as well as in later studies. However, those who completed their studies at a time when cybersecurity was not part of basic education or further studies may currently be completely excluded from cybersecurity training if they do not receive it at their workplace.

There are quite a few providers of training to companies and other organisations in Finland. Employees in large companies and public organisations generally receive training in connection with their work, but employees in SMEs and the self-employed may not. Another problem may be that the management of SMEs or entrepreneurs do not recognise the need for training, or the price of training creates problems.

There are various forms of support for SMEs as well as very low-cost training, but the needs may not be recognised, and the lack of training may not be noticed. The representative of the organisation Suomen Yrittäjät stated that some attempts have been made to organise training, but it has been cancelled due to the low number of participants.

The supply of training is scattered, and not everyone understands what kind of training they would need. Adult education centres train different age groups, but even training organisations themselves do not necessarily have an idea of what kind of education should be organised.

It is also noteworthy that the IoT is hardly addressed in the training courses reviewed here. Given the risks associated with IoT devices that may not be understood by the average consumer, such training would be clearly needed.

For large companies and public organisations, the situation is good. Large companies have the capacity to purchase cybersecurity training for their employees, and training companies are happy to provide training solutions tailored to their needs. In the public sector, HAUS offers a wide range of cybersecurity-related training, which ensures basic competence for companies' employees.

There is a need to increase softer, or non-technical, training aimed at different target groups in Finland. Currently, there is not much training available for older age groups. It would also be important to remember accessibility and enable learning in different languages. For example, the Finnish Broadcasting Company Yle, the Finnish Digital Agency, the MPK, and many other organisations have useful material on offer. It would be helpful to collect all training for citizens under one umbrella in order to make it easier to find. Responsibility for marketing these resources should be allocated to a specific organisation, and it would also require financial resources.

7.9.2 Developing Finland's model

The Finnish Cybersecurity Strategy states that the national system for training and exercising digital security will be strengthened as part of digital security training in the public administration, in order to develop the skills of personnel in public administration, businesses, and other stakeholders as well as of citizens (Turvallisuuskomitea, 2019). In practice, Finland currently differs from many of the countries presented in this chapter in that the supply of training is rather fragmented and does not necessarily reach the target groups most in need of information and education. Finland would benefit from a specifically appointed body that would be responsible for training citizens and coordinating cooperation in training and that would have sufficient resources for this task. For example, the Greek programme, which offers every citizen an educational path in one place, could be a good option in Finland as well.

The EU countries discussed above train their citizens through extensive cooperation, but it is coordinated, and roles are clearly defined. Identification of risk groups and customised training was carried out in many countries, and such targeted training, if well marketed, will certainly reach its target groups better than general training.

In Belgium, for example, training and information packages aiming to develop citizens' cybersecurity skills are gathered on a single website, which is updated by the local Cybersecurity Centre. The site is actively promoted to the public through various campaigns. A similar platform is planned in Estonia.

In several countries, employees of SMEs who have completed their education paths at a time when cybersecurity was not part of formal education have been identified as a group easily deprived of cybersecurity training. The research data suggests that this is also the case in Finland.

In Finland, cybersecurity training for senior citizens has been largely delegated to the third sector, and it would be important to consider how training could be better targeted and made accessible to senior citizens.

The groups that are potentially left without information and training identified in other EU countries, such as the self-employed, employees of SMEs, children, young people, immigrants, and older people, should also be taken into account through tailored training in Finland.

7.9.3 Consideration of SMEs and the self-employed

State and municipal employees, as well as employees of large companies, often receive some basic training in cybersecurity through their workplace. Although this training often focuses on work-related safety issues, the lessons learned in the training can also be used outside of work. In addition, more and more employers are interested in training their employees in cybersecurity issues that are not directly related to work, due to reasons such as increased remote work, which makes the digital security of the home environment relevant for the employer.

The staff of SMEs, the self-employed, and entrepreneurs are easily left without training related to cybersecurity. It would therefore be useful to support these groups in understanding the importance of cybersecurity training and in obtaining it from either free or paid sources. One example of support measures is vouchers for purchasing training services. These groups would benefit from having all cybersecurity training on offer under a single website. The expert interviews we carried out highlighted the need to make existing training services better known and available to different groups.

In spring 2022, issues such as those related to cybersecurity have featured prominently in the media, which has likely increased the public understanding of its importance. However, there is still a need for targeted communication to SMEs, the self-employed, and entrepreneurs about the importance of cybersecurity training in reducing business risks. These groups could be informed through larger-scale campaigns and in cooperation with organisations such as Suomen Yrittäjät, the Finland Chamber of Commerce, and other organisations.

7.9.4 Attention to risk groups

The risk groups or critical target groups identified in this survey include senior citizens, children, parents of young children, and immigrants who do not have access to education in their own language, as well as people facing cyber risks in their work. Persons facing risks in their work currently receive training usually through their employers, but especially senior citizens, children and their parents, and immigrants with low Finnish proficiency, are excluded from training.

Training should be organised for these risk groups in cooperation with organisations already working with them, for example, in the case of children, with the Central Union for Child Welfare. In addition, the importance of cybersecurity issues should be communicated especially to senior citizens and those working with them, as well as to those working with young children and their parents. Again, it would help if freely open training was easily gathered in one place and clearly differentiated by target groups.

Adult education centres are a major provider of training for senior citizens, but not all of them have sufficient knowledge of cybersecurity training. Teachers of adult education centres (as well as other teachers) would benefit from further training in cybersecurity. The price has also seen as a problem for course attendance, which makes it worthwhile to consider whether adult education centres could be supported in organising courses, which would make them more affordable or free of charge.

Immigrants should also be considered as one risk group because training should be available in the participants' language. Here, cooperation in both communication and education could be carried out with those working with immigrants.

7.9.5 Clear coordination

The survey and interviews highlighted the need for coordination in cybersecurity training offered to citizens. Finland would benefit from a specifically appointed body that would be responsible for training citizens and coordinating the related cooperation and that would have sufficient financial and human resources for this task. The findability of training currently on offer has been seen as a problem, so efforts should also be made to market the training courses or the website functioning as a hub for all training.

It would be useful to have cybersecurity training targeted at different groups on a single website, maintained and updated by a designated body responsible for the cyber training of citizens and the coordination of the related cooperation. The present report on the education and training provided by different providers could be used in building the site although its maintenance requires a continuous update of information.

The website should differentiate the training by target groups and aim to communicate the importance of cybersecurity in everyday life from the perspective of each group.

7.9.6 Targeted education and training

In other EU countries, organisations corresponding to the Finnish Cybersecurity Centre have targeted both communications and training especially at those who are otherwise at risk to be excluded from cybersecurity training. In building targeted training, it is important to take into account the needs and abilities of the group. What may be called general cybersecurity training is not suitable for all target groups.

These training initiatives should be planned together with organisations working with the target groups, such as senior citizens, children, or immigrants, and the marketing and dissemination of the training should also be carried out in cooperation with those who already know the groups.

When carrying out the training and communicating about its importance, it is necessary to consider the channels used by the target groups, their general digital skills, and accessibility.

7.9.7 Increased cooperation

Effective cooperation networks have been established in other EU countries, connecting companies, government bodies coordinating cybersecurity training, and the third sector. Finland would also benefit from a cooperation network for developing citizens' cybersecurity skills, under the leadership of the body responsible for citizens' training and coordinating training cooperation. The network could also be used in the design of the website that gathers all cyber training and in the further development of the concept of cybersecurity for citizens.

The network should involve at least the largest education and training providers from all sectors, as presented in this report, as well as representatives of those working with risk groups, SMEs, and entrepreneurs. In addition, the network's competence could be used in both the creation and marketing of training.

References

2NS (2022). Tietoturvakoulutus. 2NS – Second Nature Security Oy. https://www.2ns.fi/palvelut/koulutus/. Retrieved 20.03.2022

Alma Talent (2021). Alma Talent koulutus. https://koulutus.almatalent.fi/ Retrieved 16.10.2021

Arrow ECS. (2021). Arrow ECS Edu. https://edu.arrow.com/fi Retrieved 16.10.2021

Arter Oy. (2021). Koulutukset. https://www.arter.fi/koulutukset/ Retrieved 16.10.2021

BMI (2021). Cyber Security Strategy for Germany 2021. Bundesministerium des Innern, für Bau und Heimat.

CCB (2021.) Cybersecurity Strategy Belgium 2.0 2021–2025. Centre for Cyber Security Belgium.

CGI (2021). Tietoturva- ja kyberturvallisuus. CGI. https://www.cgi.com/fi/fi/tietoturva Retrieved 16.10.2021

Cyberwatch (2021). Palvelut. Cyberwatch Finland. https://www.cyberwatchfinland.fi/fi/palvelut/ Retrieved 17.10.2021

Cyberwiser (2022). Greece (GR). Cyberwiser.eu. https://www.cyberwiser.eu/greece-gr Retrieved 01.04.2022

Digivisio (2022). Digivisio 2030 -hanke. https://digivisio2030.fi/ Retrieved 30.03.2022

DVV (1.10.2021). Digiturvapalvelut. Digi- ja väestötietovirasto. https://dvv.fi/digiturva Retrieved 01.10.2021

Elisa (2021). Elisa Santa Monican kurssit. https://yrityksille.elisa.fi/kurssit Retrieved 17.10.2021

FINCSC (2022). FINCSC - Finnish Cyber Security Certificate. https://www.fincsc.fi Retrieved 12.04.2022

F-secure (2021). Consulting and training. https://www.f-secure.com/en/consulting/training. Retrieved 17.10.2021

Gobierno De Espana. (2019.) National Cybersecurity Strategy. Prime Minister's Office, Government of Spain.

Granite (2022). Tietoturvan perusteet -verkkokoulutukset. Granite. https://granite.fi/tietoturvan-perusteet/ Retrieved 15.03.2022

Greek Republic Ministry of Digital Governance. (2020) National Cybersecurity Strategy. (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Greece

HAUS (2021). eOppiva. HAUS kehittämiskeskus Oy. https://www.eoppiva.fi/ Retrieved 20.10.2021

Helsingin työväenopisto (2021). Tietotekniikka. https://www.hel.fi/sto/fi/opiskelu/tietotekniikka Retrieved 16.11.2021

Huoltovarmuuskeskus (2021). Tieto20. https://www.huoltovarmuuskeskus.fi/a/tieto20-harjoitus-testaa-yhteistoimintaa-laajassa-kyberhairiotilanteessa Retrieved 13.10.2021

Insta (2021). Kyberturvallisuus. https://www.insta.fi/palvelut/kyberturvallisuus/ Retrieved 18.10.2021

JYVSECTEC (2022). JYVSECTEC by Jamk. https://www.jyvsectec.fi Retrieved 12.04.2022

Kauppakamari (2021). Verkkokoulutukset. https://koulutusonline.fi/course/index.php?categoryid=12 Retrieved 15.11.2021

Keskuskauppakamari (2015). Tietoturvaopas yrityksille 2016 (ICC Cyber security guide for business). Keskuskauppakamari. https://kauppakamari.fi/wp-content/uploads/2020/06/tietoturvaopas-yrityksille.pdf

KPMG (2021). Tietoturvakurssit ja räätälöidyt koulutukset. KPMG. https://home.kpmg/fi/fi/home/palvelut/neuvontapalvelut/teknologia-konsultointi/tietoturva/tietoturvakoulutus.html Retrieved 18.11.2021

Lehto M. & Niemelä, J. (2019). Kyberalan tutkimus ja koulutus Suomessa 2019. Informaatioteknologian tiedekunnan julkaisuja 83/2019, Jyväskylän yliopisto. https://www.jyu.fi/it/fi/tutkimus/julkaisut/it-julkaisut/kyberalan_koulutus_suomessa_verkkoversio.pdf

Liikenne ja viestintäministeriö (2022). Suomi kehittää kyberturvallisuuden kansalaistaitoja koko Euroopan unionin alueelle. https://valtioneuvosto.fi/-/suomi-kehittaa-kyberturvallisuuden-kansalaistaitoja-koko-euroopan-unionin-alueelle Retrieved 20.03.2022

Maanpuolustuskoulutusyhdistys (2021). Kyber- ja informaatioturvallisuus. https://mpk.fi/koulutukset/kyber-ja-informaatioturvallisuus/ Retrieved 01.10.2021

Ministry of Digital Affairs Poland (2019.) Cybersecurity Strategy of the Republic of Poland.

Ministry of National Defence Republic of Lithuania (2018). National Cyber Security Strategy.

MOOC.fi (2021). Cyber Security Base with F-Secure. Course series. https://moocfi.github.io/courses/2017/cybersecurity/ Retrieved 17.10.2021

Naisten valmiusliitto (2022). Koulutukset. https://naistenvalmiusliitto.fi/koulutukset/tapahtumakalenteri/ Retrieved 20.02.2022

National Cyber and Information Security Agency Czech (2021). National Cyber Security Strategy of the Czech Republic.

NCSI (2022). National Cyber Security Index (NCSI) ranking. e-Governance Academy (eGA). https://ncsi.ega.ee/ncsi-index/?order=rank Retrieved 25.03.2022

Nixu (2021a). Kyberharjoittelu ja koulutus. Nixu Oyj. https://www.nixu.com/fi/palvelut/kyberharjoittelu-ja-koulutus Retrieved 14.11.2021

Nixu (2021b). Nixu Challenge. Nixu Oyj. https://thenixuchallenge.com/entry/ Retrieved 14.11.2021

Portugal Resolution of the Council of Ministers (2019.) National Strategy for Cyberspace Security 2019-2023. *Portuguese Official Journal*, Series 1 — No. 108 — 5 June, 2019.

Professio (2022). IT-koulutukset. Professio Finland Oy. https://professio.fi/it/ Retrieved 20.02.2022

Puolustusvoimat (2021). Puolustusvoimiin perustetaan johtamisjärjestelmäkoulu. https://puolustusvoimat.fi/-/puolustusvoimiin-perustetaan-johtamisjarjestelma-koulu

Puolustusvoimat (2022). Kybervarusmiehet. https://intti.fi/kybervarusmiehet Retrieved 22.12.2022

Republic of Estonia Information System Authority (2021). Cybersecurity in Estonia 2021.

Republic of Estonia Ministry of Economic Affairs and Communications (2019). Cybersecurity Strategy. Republic of Estonia.

Salus (2021). Sotetraining-verkkokoulutukset. Salus Qualitas Consulting Oy. https://www.sotetraining.fi/ Retrieved 18.11.2021

Saranen (2021). Cyber Security Academy. Saranen Consulting Oy. https://www.saranen.fi/rekrytointikoulutus/cybersecurityacademy Retrieved 18.11.2021

Silverskin (2021). Academy. Silverskin Information Security Oy. https://www.silverskin.com/fi/academy.html Retrieved 20.11.2021

Sovelto (2021). Tietoturva – koulutukset. Sovelto Oyj. https://www.sovelto.fi/koulutukset/tietoturva/ Retrieved 21.11.2021

Sulava (2021). Tietoturvakoulutukset. Sulava Oy. https://sulava.com/kauppa/?category=tietoturva Retrieved 23.11.2021

Teknologiateollisuus (2021). Kyberturvallisuus. https://mytechohjelma.fi/kyberturvallisuus/ Retrieved 16.10.2021

TIVIA (2021). Koulutukset ja tapahtumat. Tieto- ja viestintätekniikan ammattilaiset TIVIA ry. https://tivia.fi/koulutukset/ Retrieved 12.11.2021

Turvallisuuskomitea (2019.) Suomen kyberturvallisuusstrategia 2019. Valtioneuvoston periaatepäätös 3.10.2019. Retrieved from: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf

Vanhustyön keskusliitto (2021). SeniorSurf. https://www.seniorsurf.fi/ Retrieved 15.10.2021

8 Identified skills needs

Interviews, various surveys, and more extensive studies indicate a significant shortage of cyber experts in Finland. Competition for talent is hampered by the global nature of the problem. This chapter assesses the scope of the shortage by numbers of persons and allocation between areas of expertise. The results are based on previous studies and statistical data. In particular, the data of a preliminary investigation (VN, 2020) on cyber competence needs commissioned by the Ministry of Transport and Communications was used to determine the scope of the national competence needs. This chapter is limited to discussing specific professional and educational titles, which is only the most visible part of the needs. Cybersecurity cuts across society, which is why skills gaps and education challenges are more extensive and complex than described here. (See ENISA, 2019; ENISA, 2021; CPO, 2020; CBR, 2020; NIST, 2017; UK Government, 2021; AustCyber, 2020.)

8.1 Skills shortage

The business sector, public administration, and the third sector all need new cyber professionals. In the survey on cyber competence needs by the Ministry of Transport and Communications (VN 2020), 73% of respondents identified a significant shortage of experts in their organisation. Almost all respondents would recruit new professionals if they were available. The survey indicates that the needs vary widely. The respondents represented five different groups and gave an estimate of their recruitment needs. The total number of responses to the survey was 273. Approximately half of the respondents were from the business sector, while just under one-half were from the public sector, and 5% were from the third sector. Based on the respondent groups, the survey results have been generalised to provide an assessment of the needs of society as a whole. A small group (16%) of respondents considered the skills gap to compromise the safety or profitability of their operations. The question is no longer about decreased growth, but viability.

There is also a strong demand within the cybersecurity industry. According to a survey by the Finnish Information Security Cluster (FISC, 2021), a technology industry association of companies and organisations that provide information and cybersecurity products and services, 87% of companies in the sector intended to hire cybersecurity personnel. The FISC survey reveals that around 35% of respondents reported that skill shortages are the most important factor constraining the growth of the sector. In British cybersecurity companies, the corresponding figure was 13% (UK Government, 2021).

Several key estimates of the labour demand have been made. In 2020, FISC members employed an estimated 6,500–7,000 cybersecurity professionals in Finland. The growth in the recruitment rate of companies offering products and services related to cybersecurity was typically between 21% and 100% according to the survey by the Ministry of Transport and Communications. We can derive from these responses that Finnish companies focusing on cybersecurity need approximately 4,000 additional experts. The calculations are based on the distribution of responses and previous information on the current number of professionals and their distribution. In a previous study carried out by the Technical Research Centre of Finland VTT (Pelkonen et al., 2016), it was estimated that a similar number of cyber professionals work full-time in other companies and in the public sector. In addition to these equal groups, a slightly larger group of people do similar tasks alongside other work. This means that 60% of cyber professionals work in cybersecurity on a full-time basis and 40% on a part-time basis. The study *Cyber security skills in the UK labour market 2021* assessed the relationship between cyber tasks and cyber expertise in the labour market. Based on job advertisements (2,700 and 5,000 per month), the ratio would be 35% and 65% respectively.

For the other categories of respondents (other private companies, the public sector, and the third sector), the additional need is smaller, less than 20%, or between 1,000 and 4,000 people over the next few years. The total number of full-time recruits would therefore range between 5,000 and 8,000 additional experts. On the basis of the same calculation, the number of new recruits carrying out these tasks alongside other work is between 1,000 and 5,000. In total, between 6,000 and 13,000 cyber professionals will be needed over the next few years.

The estimated range is not very different from other Finnish calculations. Based on an internal survey of the cybersecurity industry and other material, the industry association estimated that in 2025 there would be a need for up to 15,000 experts in the field (FISC, 2020; ENISA, 2019; ISC2, 2021). According to an earlier estimate made by the Technology Industries in Finland in 2018, its member companies will need 11,400 new ICT professionals. This survey assessed the situation of IT specialists in relation to the interests of the technology industry as a whole (Teknologiateollisuus, 2018).

The projected growth rate of ICT jobs can be mirrored with the Labour Force Survey of Statistics Finland. According to their survey, the ICT sector is in a growth trend, but the increase is mainly dependent on software, consultancy, and related activities. Production, communications, and information service activities have not increased in recent years (FiCom, 2021). Based on the reports mentioned above, most of the ICT professionals who are needed would end up working in cybersecurity.

According to the International Labour Force Survey (ISC 2021), many countries have responded to increased demand. In the course of a year, 700,000 people have entered the field in these countries, and Germany in particular has greatly increased its skills base. Ireland, which is similar to Finland in terms of its economy and population size, has 15,000 cyber professionals. In Ireland, the yearly increase of employees in the sector was 800. (See ISC2, 2021.)

8.2 Placement of professionals in different fields of expertise

Companies have a wide range of skills needs. The survey by the Ministry of Transport and Communication (VN 2020) asked which specific areas of expertise respondents would place their new recruitments. The categories were based on the general NCWF[3] classification. The American framework has been extensively used in describing the main categories of expertise related to cybersecurity, as well as the specific areas of expertise

[3] The name of the reference framework used in the survey was NIST. This is the National Cybersecurity Workforce Framework (NCWF) under the US National Institute of Standards and Technology (NIST), related to the National Initiative for Cybersecurity Education (NICE).

under them. In what follows, the relative attractiveness of the different main categories and the relative attraction of some specific areas of expertise are examined from the point of view of the recruiting organisations. The results obtained in this way are then related to a previous estimation of the number of new recruits (Niemelä, 2019). The main categories of competence are:

1. Secure Production
2. Operation and Maintenance
3. Oversight and Governance
4. Protection and Defence
5. Analysis
6. Data Collection and Operation
7. Investigation

Each of these has a number of areas of specialist expertise. In the survey, the respondent was able to indicate both a main category and specialist areas. The most important specialisation areas of expertise in each main category are mentioned in the following paragraphs if more than one in four respondents identified it as suffering from a skills shortage.

The first main category, secure production, is almost equally important for all respondent groups. Companies that produce cybersecurity products and services for others emphasised this category somewhat more than others, while educational and research organisations gave somewhat less emphasis. The survey indicates that most important areas of specialisation in this main category were systems architecture, risk management, and software development.

In the second main category, operations and maintenance, the background of the organisation had a greater impact on the perceived needs. In particular, organisations at regional level indicated labour needs in this sector clearly more frequently (17%) than the relative size of this respondent group would lead to expect (13%). The areas of specialisation in this main category that were in highest demand are, in descending order, data administration, systems administration and network services.

The third main category, oversight and governance, emerged as an important skills need, especially for the state. The most significant specialist area was cybersecurity management. Executive cybersecurity leadership and strategic planning and policy were also in high demand.

Responses to the fourth main category, protection and defence, was almost identical to the relative sizes of the respondent categories. The most important subcategories here were vulnerability assessment and management, incident response, cybersecurity defence analysis and cybersecurity defence infrastructure support.

One in two respondents (47%) reported that they will have a skills shortage in two to three years' time in the various specialist areas of the fifth section, analysis. These were threat, exploitation, all-source, target, and language analysis. This emerged especially in responses by governmental organisations and the third sector. It should be noted that the survey was carried out when the hacking of therapy centre Vastaamo was widely covered in media. The temporal distribution of responses shows that the increased media visibility increased the responses in this category. Subdivision into specialist areas of analysis was not asked, as the level of detail of the American framework in this main category was considered too detailed for the Finnish context.

Data collection and operations, or the sixth main category, were somewhat important for companies selling cybersecurity products or services to other companies. However, no specialist area emerged in the survey responses.

The final main category, investigation, was raised especially by respondents representing governmental organisations. Among the areas of specialisation in this category, respondents mentioned cyber investigation. Approximately 11% of the respondents wrote about other skills needs in addition to the fixed alternatives. The open responses included topics such as cryptology, communication, teaching, and various references to overall perception.

8.3 Recruitment needs by main category and area of specialisation

Additional recruitment needs take a concrete form as individuals. The total need is first divided according to the main categories of competence. The calculations are based on both full-time recruitment needs (5,000–8,000) and overall recruitment needs (6,000–13,000). In the latter, people working in cybersecurity alongside other work have been added to full-time jobs.

Full-time new employees would be divided into main categories of competence as follows:

1. Secure production 900–1,500 persons
2. Operations and maintenance 700–1,100 persons
3. Oversight and governance 800–1,300 persons
4. Protection and defence 900–1,400 persons
5. Analysis 600–1,700 persons
6. Data collection and operation 500–800 persons
7. Investigation of 500–800 persons

The larger number of recruits, between 6,000 and 13,000, would accordingly be divided as follows:

1. Secure production 1,100–2,400 persons
2. Operation and maintenance 900–1,900 persons
3. Oversight and governance 1,000–2,200 persons
4. Protection and defence 1,000–2,300 persons
5. Analysis 800–1,700 persons
6. Data collection and operation 600–1,300 persons
7. Investigation 600–1,300 persons

The accuracy of the relative proportions mentioned here can be assessed by comparing the figures with international sources and data derived through other methods. The same NCWF framework has been used in other studies, for example, in the investigation of vacancies in cybersecurity in the US and in the international ISC survey of existing jobs.

Different data sets can be compared by dividing the total need (100%) into different skill categories. The percentages in this competence survey, American job advertisements and the international ISC survey are similar (CyberSeek, 2022; ISC2, 2021). The distribution is presented in Table 9.

TABLE 9. Total skills needs per category of competence

Competence category	Survey	US job advertisements	ISC2 survey
Secure production	19%	22%	18%
Operation and maintenance	14%	26%	14%
Oversight and governance	17%	18%	28%
Protection and defence	17%	16%	16%
Analysis	13%	10%	8%
Data collection and operation	10%	4%	6%
Investigation	10%	3%	4%

The above-mentioned Finnish survey material anticipates the next few years, and the two international data sets assess the current situation. The observed differences likely reflect national differences between sectors and their levels of maturity. The only distinctly Finnish deviation is the perceived importance of the last two sections: data collection and operation, and investigation. Data collection and operations are important for companies producing cybersecurity products and services, while investigation is important for government organisations.

Niemelä (2019) classified Finnish job vacancies accordingly. The main categories were distributed in his study as follows: 1.35%, 2.30%, 3.23%, 4.4%, 5.3%, 6.0% and 7.6%. Based on Niemelä's data (168 job advertisements), the attention of Finnish employers was concentrated in only a few main categories. Job advertisements were also analysed in the survey Digibarometer 2020: Cybersecurity in Finland (Mattila et al., 2020). At that time, job advertisements in the cyber sector were focused on professionals in systems architecture, cyber business, software, maintenance, and oversight.

The preliminary investigation also shows the order of importance of the specialist areas in each main category, which may also be used in deriving quantitative estimates. Table 10 shows estimates of the needs in the specialist areas. After each main category the columns show the share of the specialist area, followed by person-level estimates in four cases. First, a range of full-time cyber experts is given; the second figure also includes professionals who do cyber work alongside other jobs.

When examined per category, the data show a concentration of the skills need in the smaller main categories. In the larger main categories, the needs and the attention of respondents are more dispersed, potentially making any single area of expertise less important. Based on the calculation, the specialist area of cyber investigation, under the main category of investigation, faces a need of up to 760 persons. Following it, in descending order, are, under the main category of protection and defence, vulnerability assessment and management with a need for 260–660 persons, incident response with a need for 230–590 persons, and cybersecurity defence analysis with a need for 230–590 persons. The specialist areas of the most important main category, secure production, were evenly distributed. The most common specialist areas in the first main category were systems architecture with a need for 180–470 persons, risk management with a need for 150–390 persons, and software development with a need for 140–370 persons.

TABLE 10. Estimated skills needed in specialised areas

Specialist area	Share of the main class	Full-time min	Full-time max	Full-time and IATOD min	Full-time and IATOD max
1. Secure production		900	1500	1100	2400
1.1. Secure production – Risk management	16 %	147	244	179	391
1.2. Secure production - Software development	15 %	137	229	168	367
1.3. Secure production - System architecture	20 %	176	293	215	469
1.4. Secure production - Research and development of technologies	9 %	82	137	101	220
1.5. Secure production - Definition of requirements	13 %	114	189	139	303
1.6. Secure production - Assessment and testing	14 %	126	211	155	337
1.7. Secure production - System development	13 %	117	196	143	313
2. Operation and maintenance		700	1100	900	1900
2.1. Operation and maintenance - Data management	23 %	161	253	207	436
2.2. Operation and maintenance - Knowledge management	14 %	100	157	128	271
2.3. Operation and maintenance - Customer service and technical support	7 %	49	77	63	133
2.4. Operation and maintenance - Network environment management	20 %	138	217	178	376
2.5. Operation and maintenance - Management of the system environment	21 %	144	227	186	392
2.6. Operation and maintenance - System analysis	15 %	108	169	139	293
3. Oversight and governance		800	1300	1000	2200
3.1. Oversight and governance - Legal services	14 %	114	185	142	313
3.2. Oversight and governance - Training, education and raising awareness	13 %	106	172	133	292
3.3. Oversight and governance - Cybersecurity management	25 %	202	329	253	557
3.4. Oversight and governance - Strategic planning and policies	16 %	129	210	161	355
3.5. Oversight and governance - Project management and procurement expertise	14 %	114	185	142	313
3.6. Oversight and governance – Cybersecurity and information security management	17 %	135	219	169	371

(Table 10 continues)

Specialist area	Share of the main class	Full-time min	Full-time max	Full-time and IATOD min	Full-time and IATOD max
4. Protection and Defence		900	1400	1000	2300
4.1. Protection and Defence - Analysis of systems and data protection needs	25 %	229	357	255	586
4.2. Protection and Defence - Defence infrastructure for cyber security	20 %	180	280	200	460
4.3. Protection and Defence - Responding to incidents	26 %	232	361	258	592
4.4. Protection and Defence - Vulnerability assessment and management	29 %	259	403	288	662
5. Analysis		600	1000	800	1700
5.1. Analysis – everything, e.g., threat and intrusion analysis	100 %	600	1000	800	1700
6. Data collection and operation		500	800	600	1300
6.1. Data collection and operation - Event data collection	29 %	145	233	174	378
6.2. Data collection and operation - Cyber operations planning	38 %	188	301	226	489
6.3. Data collection and operation - Cyber operations	33 %	167	267	200	433
7. Investigation		500	800	600	1300
7.1. Investigation - Cyber investigation	59 %	294	470	352	764
7.2. Investigation - Digital criminal investigation	41 %	206	330	248	536

The framework clearly delineates the areas of specialisation, but the number of small groups can make it difficult to perceive the overall picture. To improve clarity, the responses may be aggregated into larger units. The responses reveal that particular demands were in (a) oversight and governance (with specialist areas such as systems architecture, cybersecurity management, strategies, and cybersecurity or information security managers working with strategies) and (b) more operative competence with an emphasis on systems protection and related analysis. The public sector has a relatively greater need for leadership and risk management experts with a very broad perspective, while the business sector seeks experts in management and architecture.

The municipal sector had a greater need for cyber experts in customer service and technical support, as well as in project management and leadership. The latter sectors were not as common in the responses of other sectors. Only few respondents represented the third sector, but for them data management and analysis were particularly important areas of specialised expertise.

Based on the member survey by FISC (2020), the respondents offering cybersecurity products and services needed experts in the following areas: software competence, business competence, strategic cybersecurity competence, cryptography/cryptology, technical cybersecurity, maintenance and governance competence, and systems architecture competence. In the survey by the Ministry of Transport and Communications (VN 2020), the findings were the same: companies that produce cybersecurity services or products need more professionals in software development and systems architecture.

Other studies on competence needs have similar results. A report by the national emergency supply organisation examined the maturity level of cybersecurity in sectors that are key to security of supply. It found that the main convergent areas for development from a business perspective were, first, the company's cybersecurity strategy; second, its cybersecurity architecture; and third, technical traceability, or log tracking.

A 2018 survey by the Technology Industries of Finland examined the needs in different areas of ICT more extensively. In particular, respondent companies highlighted the following areas: robotics and automation, development of the intelligence of products and services, enterprise resource planning and product information systems, cloud services and data analytics.

An extensive British study (2021) broadens the skills shortage to very different job titles in cyber companies. There, the job titles facing greatest needs included security engineers (37%), security analysts (18%), security managers (14%), and security architects (11%). According to the same study but a different data set, 37% of cyber positions have been difficult to fill. Most of these positions have been general cybersecurity and manager-level jobs, but they have also included penetration testers, security architects, and sales staff. Not all positions were for full-time cyber professionals, but they were still expected to have expertise in the field. In half of the cases, filling the positions had been hampered by the candidates' lack of technical competence. One in three lacked work experience (35%) or their attitude was not suitable for the position (30%). (See UK Government, 2021.)

According to a study by the Enterprise Strategy Group – Information Systems Security Association (2021), the greatest shortage of cyber skills was in cloud computing security (39%), security analysis and investigations (30%), and application security (30%). The data was concentrated in North America (ESG-ISSA, 2021).

According to the Global ISC Survey (2021), skills shortages will remain critical at a global level. One in two respondents mentioned secure provision (48%), analysis (47%), and protection and defence. Other main categories were close behind. (See ISC2, 2021.)

8.4 Conclusions and development needs

The figures derived from previous Finnish data have also been compared with international sources. The credibility of the results is enhanced by the fact that they are consistent with these international studies.

The skills shortage is a reality, although it is difficult to predict its level accurately. Based on the source data, it is estimated that we will need between 5,000 and 8,000 cybersecurity professionals in the coming years. In addition, between 1,000 and 5,000 new professionals will do cybersecurity-related work alongside other work. All of these people need to be trained in the field.

The greatest number of new experts is needed for secure production. More specifically, a group of 6,000 to 13,000 new cyber professionals can be divided according to their main field of training as follows:

1. Secure production 1,100–2,400 persons
2. Operation and maintenance 900–1,900 persons
3. Oversight and governance 1,000–2,200 persons
4. Protection and defence 1,000–2,300 persons
5. Analysis 800–1,700 persons
6. Collection of data and operation 600–1,300 persons
7. Investigation 600–1,300 persons

The competence profile is fairly evenly distributed across all cybersecurity competence areas. This means the need for comprehensive education and training. The degree studies of higher education institutions and conversion and continuing education must cover all these areas in order to meet the skills needs.

Increasing the intake of cybersecurity education and training requires resources for both education and research. The challenge is to recruit researchers and teachers to higher education institutions within a short timeframe. The Ministry of Education and Culture funds the increase in initial intakes in universities of applied sciences as follows:

- UAS bachelor's student EUR 6,000/year/student
- UAS master's student EUR 6,000/year/student
- Bachelor's students from outside the EEA are subject to an annual tuition fee of EUR 8,000.

In universities, the cost impact arises when the intake increases by dozens of students. At the bachelor's level, the need is about EUR 6,000/year/student and at the master's degree level EUR 9,000/year/student.

References

AustCyber (2020). Australia’s Cybers Security: Sector Competitiveness Plan 2020. Australian Cybersecurity Growth Network. https://www.austcyber.com/resources/sector-competitiveness-plan .

CBR (2020). Europe’s Cybersecurity Skills Gap Has Doubled: Report. By CBR Staff Writer. https://techmonitor.ai/technology/cybersecurity/cybersecurity-job-gap.

CPO (2020). Study Reveals That Cybersecurity Skills Gap Affects About Three-Quarters of Organizations and Still Worsening. CPO Magazine. https://www.cpomagazine.com/cyber-security/study-reveals-that-cybersecurity-skills-gap-affects-about-three-quarters-of-organizations-and-still-worsening/ .

CyberSeek (2022). Cybersecurity Supply/Demand Heat Map: Job openings by NICE Cybersecurity Workforce Framework Category. https://www.cyberseek.org/heatmap.html.

ENISA (2019). Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA’s Higher Education Database. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

ENISA (2021). Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

ESG-ISSA (2021). The Life and Times of Cybersecurity Professionals 2021, Vol. V. ESG-ISSA Research Report. https://2ll3s9303aos3ya6kr1rrsd7-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf

FiCom (2021). ICT-alan työlliset 19.11.2021. Lähde: Tilastokeskuksen työvoimatutkimus, FiCom ry.

FISC (2020). Jäsenkysely. Finnish Information Security Cluster (FISC).

FISC (2021). Kyberosaajatarvekysely. Finnish Information Security Cluster (FISC).

ISC2 (2021). Cybersecurity Workforce Study. International Information Systems Security Certification Consortium (ISC)^2. https://www.isc2.org/Research/Workforce-Study.

Mattila, J., Mäkäräinen, K., Pajarinen, M., Seppälä, T., Ali-Yrkkö, J. & Tervo, E. (2020). Digibarometri 2020: Kyberturvan tilannekuva Suomessa. Helsinki: Taloustieto Oy.

Niemelä, J. (2019). Kyberturvallisuusalan työvoiman kysyntä, saatavuus ja kehittäminen vastaamaan työvoiman tarvetta Suomessa. Pro gradu, Jyväskylän yliopisto.

NIST (2017). Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future. National Institute of Standards and Technology (NIST). https://www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf

Pelkonen, A., Ahlqvist, T., Leinonen, A., Nieminen, M., Salonen, J., Savola, R., Savolainen, P., Suominen, A., Toivanen, H., Remes, J. & Kyheröinen, J. (2016).

Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2016.

Teknologiateollisuus (2018). 9 ratkaisua Suomelle: Teknologiateollisuuden Koulutus ja osaaminen -linjaus 2018. https://teknologiateollisuus.fi/sites/default/files/file_attachments/teknologiateollisuus_koulutus_ja_osaaminen_linjaus_2018.pdf.

UK Government (2021). Cybersecurity skills in the UK labour market 2021: Findings report. https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2021;

VN (2020). Kyberosaamistarpeet – esiselvitys, VN/20895/2020, Valtioneuvosto.

Informaatioteknologian tiedekunnan julkaisuja
No. 96/2022

ISBN 978-951-39-9469-3 (e-publication)
ISSN 2323-5004

JYVÄSKYLÄN YLIOPISTO