Advancing Cybersecurity Education: Developing a Cybersecurity Higher Education Network in Finnish Universities

Piia Perälä and Martti Lehto
Faculty of Information Technology, University of Jyväskylä, Finland

piia.m.h.perala@jyu.fi
martti.j.lehto@jyu.fi

Abstract: Cybersecurity is a critical element of national security strategies. European countries have established cybersecurity strategies to enhance their resilience against cyber threats. In Finland, the cybersecurity strategy emphasizes the importance of cybersecurity education and its development as essential components in preparing the nation to address cybersecurity threats. Achieving national cyber self-sufficiency will require a diverse range of skilled cybersecurity experts. However, the global shortage of cybersecurity specialists poses a significant challenge to developing and maintaining cyber sufficiency and resiliency. This shortage is also recognized in Finland. Universities play a crucial role in training cybersecurity experts through their education programs. In Finland, initiatives have been launched to develop cybersecurity higher education to address skills shortages. A key measure identified is developing an educational network for cybersecurity higher education. In early 2023, a three-year national project was launched to develop university-level cybersecurity education in Finland. The project involves nine Finnish universities and aims to strengthen cooperation between universities, industry, and the public sector in cybersecurity education. This collaboration enables the development of cybersecurity education for both degree students and working professionals. This paper describes the process and measures for developing national university-level cybersecurity education in Finland. It also aims to provide an understanding of the opportunities and challenges in developing an educational network in higher education. A key finding is that the educational network provides a solid basis for developing cybersecurity skills and efficiently using resources. Additionally, it enables the coordination of cybersecurity education at the national level, thus supporting the promotion of Finnish cybersecurity strategy objectives.

Keywords: Cyber education, Security, Cybersecurity, Education network, Higher education

1. Introduction

Cybersecurity has been integrated as a fundamental component of national cybersecurity strategies. The Security Strategy for Society underlines the vitality of assuring and maintaining cybersecurity for national security (Security Committee, 2025). Finland's cybersecurity strategy emphasizes that cybersecurity education and training must be strong at all levels of society (Prime Minister's Office, 2024). Higher education institutions have been identified as the primary source of education and development of a skilled workforce (e.g., Chhinzer and Russo, 2017; Baird and Parayitam, 2019). Therefore, the Finnish higher education system, encompassing universities and universities of applied sciences, is crucial in educating cybersecurity specialists through educational programs.

Cybersecurity higher education programs in Finland cover a wide range of skills across various cybersecurity domains (Perälä and Lehto, 2024). Despite the broad range of programs, Finnish higher education institutions face challenges in educating enough workforce to meet the rapidly growing demand for cybersecurity specialists in the labour market. Similar to many other nations, Finland has a severe shortage of cybersecurity professionals (Ministry of Transport and Communications, 2021; Lehto, 2023; Ramezan, 2023). On a global scale, the demand for a cybersecurity workforce in 2024 was approximately 4.76 million (ISC2, 2024). In Finland, the projection from 2023 indicated a need for 5,000 to 8,000 new cybersecurity experts in the forthcoming years, in addition to 1,000 to 5,000 professionals capable of integrating cybersecurity responsibilities into their existing roles (Lehto, 2023).

In 2021, the Finnish Cybersecurity Development Program highlighted the necessity of enhancing cybersecurity education (Ministry of Transport and Communications, 2021). In 2022, the need for reform in cybersecurity higher education was acknowledged (Lehto, 2022). Finland's cybersecurity strategies have also highlighted the importance of cooperation between national cybersecurity actors. In 2023, a three-year nationwide project funded by the Ministry of Education and Culture was launched to develop a cybersecurity higher education network and advance cybersecurity education in higher education institutions (Ministry of Education and Culture, 2022). The project brought together nine Finnish universities offering cybersecurity education and forming the cybersecurity higher education network of Finnish universities. This network is a collaborative group of higher education institutions working together to enhance cybersecurity education and research. The network aims at developing Finnish cybersecurity higher education at the national level, creating joint cybersecurity education, establishing effective communication channels between higher education institutions

in cybersecurity education, and acting as a link to connect business actors and national cybersecurity authorities with Finnish universities' cybersecurity education.

This paper describes the process and measures for developing the cybersecurity education network among Finnish universities. It outlines the network's activities to enhance university-level cybersecurity education in Finland. Additionally, the paper highlights the opportunities and challenges in developing an educational network in higher education.

2. Overview of Cybersecurity Education in Finnish Universities

In Finland, higher education follows a dual model (Ministry of Education and Culture, 2025b). Both universities and universities of applied sciences offer degrees classified under the European Qualifications Framework (EQF) at levels 6 and 7 (Finnish National Agency for Education, 2018, 2025). Finnish universities' cybersecurity degree education focuses on master's level education (level 7 in EQF), while universities of applied sciences provide more bachelor's degree programs in cybersecurity. The main distinction between these institutions is that universities of applied sciences are more work-life-oriented, whereas universities emphasize advancing scientific knowledge (Finlex, 2025b, 2025a).

Universities' cybersecurity-related study programs aim to educate specialists in the cybersecurity field. According to the report from Perälä and Lehto (2023), six Finnish universities offered degree education in cybersecurity in 2023. All these universities offered only master's level degree programs in cybersecurity. In these master's programs, cybersecurity can be a field, major, or specialization. Some degree programs were international, and others were only for Finnish-speaking students. It was estimated that in 2022, approximately 100 students graduated from these programs, and more than 500 students are annually enrolled in cybersecurity degree programs at universities.

Finnish universities offer a broad range of educational content. According to Perälä and Lehto (2024), universities provided 96 cybersecurity courses in 2023. These courses covered various themes, including technical and technological cybersecurity, cybersecurity management, the societal and human aspects of cybersecurity, and general cybersecurity knowledge. These themes focused on developing specific skills in cybersecurity, such as technical skills and competence, understanding cybersecurity management and its impact on diverse organizations, understanding cybersecurity's role in the information society, and understanding the psychology of cybersecurity. However, the main focus of Finnish universities' educational content is developing technical and technological competence in cybersecurity (Figure 1). Additionally, cybersecurity education in Finnish universities has been found to be comprehensive when assessed against the European Cybersecurity Taxonomy. Universities' educational content broadly covers knowledge domains defined in the European Cybersecurity Taxonomy (Perälä and Lehto, 2024).

In addition to degree programs, universities provide cybersecurity-related modules and courses available to degree students from fields other than cybersecurity to deepen their knowledge and orient their studies. In addition, Finnish universities are part of different continuous learning programs in cybersecurity for non-degree students, accessible through open universities and online platforms, catering to various educational backgrounds and skill levels (Ministry of Education and Culture, 2025a).

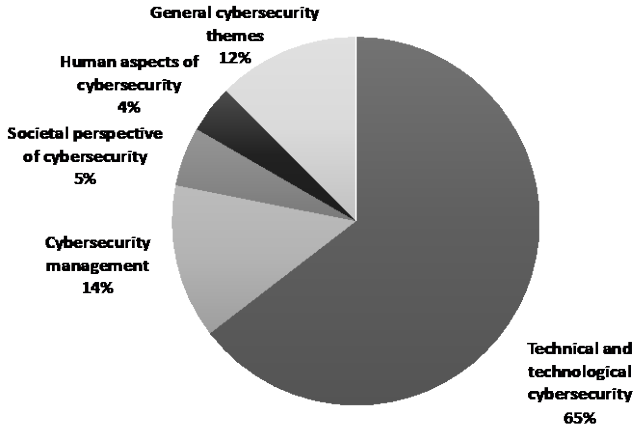

Figure 1: An illustration of the distribution of Finnish universities' cybersecurity educational content across themes (Perälä & Lehto, 2024)

3. Developing Cybersecurity Education and Education Network in Finnish Universities

This chapter describes the development of cybersecurity education and education network in Finnish universities. The chapter discusses the premises, the process, and the key measures to advance the development. The results and achievements presented in this paper reflect the progress made by early 2025.

3.1 Background

In Finland, a national shortage of skilled workforce in the cybersecurity field has increased the need to educate more cybersecurity professionals (Lehto, 2023). Although universities have recruited teachers and researchers in the field, individual universities have insufficient resources to increase cybersecurity education significantly. It has been noted that cybersecurity education is limited in terms of the number of students and the education volume to meet the cybersecurity workforce shortage. Imbalances between the demand for a cybersecurity workforce and educational offerings have been identified (Ministry of Education and Culture, 2022; Lehto, 2023). Consequently, reports have highlighted the need for cybersecurity education development (Lehto, 2022).

In 2021, the Finnish Cybersecurity Development Program highlighted the need to enhance cyber education in Finland (Ministry of Transport and Communications, 2021). Developing cybersecurity skills is also a key objective of Finland's cybersecurity strategies (The Security Committee, 2013, 2019; Prime Minister's Office, 2024). In early 2023, a three-year national-wide project funded by the Finnish Ministry of Education and Culture was launched to boost cybersecurity in higher education and the workforce in Finland (Ministry of Education and Culture, 2022). This project aims to develop, strengthen, and expand cybersecurity education in Finland and foster greater cooperation among Finnish higher education institutions.

3.2 Project Overview

The project has brought together a network of nine Finnish universities, each offering cybersecurity education. It involves more than 40 people who are working on university-level cybersecurity education. The project aims to develop, coordinate, and strengthen higher education in cybersecurity to strengthen and expand cybersecurity education across Finnish universities. (JYU, 2023)

Cybersecurity education developed during the project is embedded in the everyday activities of universities' cybersecurity education and students. The project creates a model to establish a sustainable cybersecurity education network and maintain educational cooperation. The primary objective is to ensure broad and continuous training in cybersecurity expertise on a shared understanding of the core competencies, knowledge, and skills to be developed by education.

3.3 Process

The work for developing cybersecurity education and education network is structured into four distinct work packages, each with a specific main objective and essential tasks.

- Assessing the current state of cybersecurity education in Finnish universities.
- Developing cybersecurity education.
- Fostering educational collaboration between universities.
- Establishing methods for monitoring the universities' education network.

These work packages are designed so that understanding the current state of cybersecurity education forms a solid foundation for later work done in the other work packages, which are carried out in parallel. Upon completing the work packages, the project results in an operational cybersecurity education cooperation network.

3.3.1 The current state of cybersecurity education in Finland

The work package provided a comprehensive analysis of the current state of cybersecurity education in Finnish universities. It described the universities' cybersecurity education offerings and detailed the distribution of educational responsibilities according to universities' educational and academic competence profiles.

Data on degree programs, study modules, courses, and research areas in cybersecurity was collected from Finnish universities during the work package. The analysis provided a comprehensive overview of the volume and content of cybersecurity education. Specifically, it revealed how teaching volume was distributed among universities and highlighted universities' focus areas in educational content. Additionally, the initial analysis

examined how the Finnish university-level cybersecurity education content aligns with the cybersecurity knowledge areas of the European Cybersecurity Taxonomy (Perälä and Lehto, 2024).

3.3.2 Developing cybersecurity education

As part of the work package focusing on developing cybersecurity education, an analysis was conducted to identify the future needs for cybersecurity education. The results from the analysis were utilized to create an implementation plan for new cybersecurity courses and study modules.

The analysis of the future needs for cybersecurity education consisted of three phases. The first phase identified gaps in education, skills profiles, and content focus areas in Finnish universities' cybersecurity education. It examined how well Finnish university-level cybersecurity education aligns with the European Cybersecurity Skills Framework (ECSF) role profiles, key competencies, and the content areas covered. A tool was designed and implemented for this evaluation to assess educational content. This tool linked course content with the role profiles of the ECSF (European Union Agency for Cybersecurity, 2022) and the European Cybersecurity Taxonomy (Nai *et al.*, 2019).

The results from Majanoja et al. (2024) provide a comprehensive overview of cybersecurity education coverage in Finnish universities. The analysis examined how well these programs deliver cybersecurity skills concerning the role profiles of the ECSF and how different universities prioritize these roles. It also identified gaps in educational content, specifically the competencies least covered according to the European Cybersecurity Taxonomy. Based on these findings, several recommendations have been proposed to enhance cybersecurity education at Finnish universities. These include developing educational cooperation in areas where overlapping teaching is identified, increasing the number of practical exercises, and creating continuous learning programs to support workforce needs. Additionally, it is suggested that more time- and place-independent courses be offered and collaboration with companies enhanced to ensure that educational content aligns with current and future industry demands.

The second phase focused on understanding the cybersecurity skills needs of companies. The aim was to identify the cybersecurity skills needs of companies in different areas of cybersecurity to develop cybersecurity education. The skills mapping was carried out according to the European cybersecurity taxonomy. Data was collected through questionnaires from 61 Finnish companies and public administration representatives. Interviews also complemented the questionnaires to provide in-depth information on the respondents' views and needs.

The results facilitated the identification of future cybersecurity skills anticipated by companies, the skill expectations for new employees in both competencies and soft skills and the role of higher education institutions in enhancing these cybersecurity skills. The report by Majanoja et al. (2024) provides a comprehensive analysis and detailed findings concerning the cybersecurity skill needs of companies.

In the third phase, the design and implementation of new courses and study modules began, leveraging the analysis of cybersecurity education coverage and the cybersecurity skills needs of companies. Various cooperative activities, including workshops and discussions, were organized among university representatives to promote the development of cybersecurity education. This collaborative effort generated ideas and outlined measures to expand education into new cybersecurity competence areas, enhance cooperation in teaching, and develop innovative methods for delivering education to a broader audience.

3.3.3 Fostering educational cooperation in the education network

The work package enhancing cooperation in the cybersecurity education network focuses on creating an operational model for cross-teaching and coordinating collaboration in the cybersecurity education network. Developing inter-university cooperation is closely linked to cybersecurity education development. Therefore, the measures undertaken to enhance cooperation in education were carried out in parallel and through close interaction with the development of cybersecurity education.

The work for fostering educational cooperation has identified multiple collaboration methods for cybersecurity education. These new opportunities for educational cooperation are being planned and implemented, including inter-university study modules in secure programming and cryptography fields, as well as a collaborative course in information security management. Additionally, universities have created a cybersecurity summer school concept, offering cybersecurity courses in cooperation with universities as part of international summer schools in Finland.

The work has also provided insights into the requirements and challenges that must be addressed to facilitate effective educational and training collaboration. The objective is to comprehensively understand the characteristics, motivation, managerial issues, opportunities, and challenges associated with universities' cooperation in educational offerings. It is expected that at the end of the project, the roadmap for ensuring the sustainability of cooperation within the cybersecurity education network will be finalized.

3.3.4 Establishing methods for monitoring the universities' education network

The work package aims to develop a methodology to monitor the effectiveness of the universities' education network and educational cooperation. The aim is to develop indicators for monitoring the quality and quantity of education the cybersecurity education network provides. Data and feedback are collected from teachers, students, and stakeholders on the activities of the network and the education it provides. The developed monitoring methods should support the network's development and ongoing maintenance.

4. Insights on the Relevance and Identified Challenges of the Cybersecurity Education Network

The cybersecurity education network, which has brought together nine Finnish universities offering cybersecurity education, has advanced the development of cybersecurity education across universities. However, while building a functional network and advancing educational initiatives, several challenges have been identified that must be addressed to sustain and further develop the cybersecurity education network of Finnish universities. The following sub-chapters outline the opportunities and challenges identified.

4.1 Relevance of the Education Network

Strengthened communication and consensus about Finnish universities' cybersecurity education: The cybersecurity education network has brought together Finnish universities, which play a key role and are responsible for providing an academically educated workforce in the cybersecurity field. The network has enabled regular communication between the universities and facilitated the building of a shared understanding of how Finnish universities' cybersecurity education should be developed in the future.

Strengthened communication and cooperation between cybersecurity higher education institutions and stakeholders: The cybersecurity education network has become a central point of contact for national cybersecurity actors and companies to collaborate and communicate with universities offering cybersecurity education. Previously, communication was fragmented and conducted separately with individual universities. Through the network, stakeholders can engage consistently with the cybersecurity education sector, facilitating collaboration and enhancing information sharing between universities and stakeholders. For example, stakeholders can readily discuss their needs with the education sector and provide insights on the directions and priorities for developing cybersecurity education. Furthermore, the collaboration between the universities' cybersecurity education network and national cybersecurity authorities supports the objectives of Finland's cybersecurity strategy. The Finnish cybersecurity strategy emphasizes cooperation among various national cybersecurity actors to enhance national cyber resilience.

Promote educational cooperation and expand education offerings: The cybersecurity education network has brought together cybersecurity educators from the university sector, establishing a framework for discussion and cooperation among universities and their lecturers to develop cybersecurity education. This network has facilitated different forms of educational collaboration, strengthening and expanding cybersecurity education offerings in Finnish universities. For example, typically, Finnish universities offer courses exclusively to students from their degree programs. However, the cybersecurity education network has developed courses available to students from multiple universities. Additionally, efforts are being made to create inter-university study modules in specific areas of cybersecurity. Universities contribute to organizing courses for these modules. Students from different universities can enrol in these modules due to agreements on cross-institutional studies. Upon completion, the credits are transferred to the student's transcript of records.

Enhanced use of resources: Universities have recognized the potential for more efficient use of teaching resources through educational cooperation. Universities have established collaborative teaching efforts via the education network in areas where overlapping educational content has been identified. These subject areas often serve as foundational knowledge for more advanced studies in cybersecurity. The objective is for universities to jointly deliver courses that provide essential knowledge in these areas. Such core competency courses can be widely offered to students from multiple universities. By minimizing overlapping teaching, universities can optimize teaching resources. For example, lecturers can allocate more time to deepening

students' knowledge in specific cybersecurity competence areas. Additionally, the aforementioned collaborative study modules expand educational offerings without excessively increasing resource requirements compared to a single university organizing study modules independently. Overall, collaborative education organized through the cybersecurity education network facilitates the spread of course offerings to a broader audience without excessively increasing individual lecturers' workload.

4.2 Identified Challenges to Consider

Resourcing the maintenance of the education network: The funded project has allocated resources to build the cybersecurity education network, start its activities, and develop cybersecurity education. However, for the network to become established, sustainable, and expanded, human and financial resources are needed to sustain its activities. Continuing the network's activities purely voluntarily could pose a risk to its sustainability. For example, the network's activities require maintenance, development, and coordination. In addition, the maintenance and development of cooperation in education requires that the universities involved in the cybersecurity education network provide lecturers with the opportunity to participate actively in the activities.

Issues in developing educational cooperation: While there is a willingness and potential to promote inter-university cooperation in cybersecurity education, effective development is hampered by the need to reconcile different university approaches and practices. For example, the diverse information systems used by universities can complicate organizing educational collaboration. Universities use different student information systems and learning platforms. When education is delivered across universities, these systems should be compatible with transferring data regarding students and the completion of studies (e.g., students' course enrolments, grades, and course completion data). Additionally, universities have varying policies and regulations regarding organizing education, which can pose challenges for cooperation. For instance, scheduling and teaching methods may vary significantly. One university might offer flexibility in scheduling and teaching methods, while another may adhere to a strict timetable and prescribed teaching methods, such as face-to-face lectures.

5. Discussion and Conclusion

Cybersecurity is a key element of national security strategies, as highlighted by the Security Strategy for Society (Security Committee, 2025). Finland's cybersecurity strategy emphasizes developing cybersecurity education to mitigate cyber risks (Prime Minister’s Office, 2024). Finnish higher education institutions play a vital role in educating a skilled workforce. The rapidly growing global and national demand for a cybersecurity workforce has compelled Finnish higher education institutions to consider how to increase their cybersecurity study offerings. However, Finnish higher education institutions struggle to meet the growing demand for educating cybersecurity professionals.

In response to the challenge, a nationwide project was launched in 2023 to develop cybersecurity in higher education and foster collaboration among higher education institutions. This initiative brought together nine Finnish universities to form a cybersecurity education network to enhance education and research, foster cooperation, and connect academia with industry and national cybersecurity authorities.

In this paper, we introduced the process and measures for developing the cybersecurity education network of Finnish universities. We also outlined the network's activities to enhance university-level cybersecurity education in Finland. This process was established to advance cybersecurity education and create a collaborative cybersecurity education network. The work involved assessing the current state of cybersecurity education in Finnish universities, developing cybersecurity education, fostering educational collaboration between universities, and establishing methods for monitoring the universities' education network. Eventually, practices for an operational cybersecurity education cooperation network were developed.

During the work, insights into the relevance and challenges of the cybersecurity education network were identified. The operating education network strengthened communication and consensus about cybersecurity education among Finnish universities. It also provides a solid point of contact for national cybersecurity actors and companies to collaborate and communicate with universities offering cybersecurity education. The education network has also promoted educational cooperation between universities, leading to expanded cybersecurity education offerings. The collaboration has also enabled more efficient use of recourses by developing courses and study modules taught jointly by multiple universities.

However, universities' diverse approaches and practices pose challenges to educational cooperation. To ensure smooth educational cooperation among universities, their approaches and practices need to be harmonized. In

addition to maintaining and developing the education network, human and financial resources are required to sustain its activities. Without the necessary resources, the network's continued operation is uncertain.

Studies have suggested that increasing the number of cybersecurity study programs increases the cybersecurity workforce (e.g., Harris, 2024) However, this paper presents an alternative approach to expanding cybersecurity study offerings to enhance education and educate future cybersecurity professionals. It demonstrates that forming an education network provides a solid foundation for building cooperation in cybersecurity education among universities, which can eventually expand cybersecurity education.

The utility of our findings is limited, as this paper discusses practices for developing university-level cybersecurity education only in Finland. Different countries have varying approaches and practices regarding cybersecurity education in higher education. Creating common practices requires extending the cybersecurity education network beyond Finland's higher education system. However, network cooperation between universities in jointly chosen subject areas will undoubtedly benefit all parties involved.

Acknowledgements

The work was supported by the Ministry of Education and Culture in Finland (OKM/60/522/2022).

Ethics declaration: An ethics declaration was not required for the research.

AI declaration: AI tools were not used in the creation of this paper.

References

Baird, A.M. and Parayitam, S. (2019) 'Employers' ratings of importance of skills and competencies college graduates need to get hired: Evidence from the New England region of USA', *Education + Training*, 61(5), pp. 622–634. Available at: https://doi.org/10.1108/ET-12-2018-0250.

Chhinzer, N. and Russo, A.M. (2017) 'An exploration of employer perceptions of graduate student employability', *Education + Training*, 60(1), pp. 104–120. Available at: https://doi.org/10.1108/ET-06-2016-0111.

European Union Agency for Cybersecurity (2022) *ECSF, European cybersecurity skills framework*. LU: Publications Office. Available at: https://data.europa.eu/doi/10.2824/859537 (Accessed: 1 February 2025).

Finlex (2025a) *FINLEX ® - Translations of Finnish acts and decrees: 558/2009 English*. Oikeusministeriö. Available at: https://www.finlex.fi/en/laki/kaannokset/2009/en20090558?search%5Btype%5D=pika&search%5Bkieli%5D%5B0%5D=en&search%5Bpika%5D=2009%2F558 (Accessed: 1 February 2025).

Finlex (2025b) *FINLEX ® - Translations of Finnish acts and decrees: 932/2014 English*. Oikeusministeriö. Available at: https://www.finlex.fi/en/laki/kaannokset/2014/en20140932 (Accessed: 1 February 2024).

Finnish National Agency for Education (2018) *Report on the referencing of the Finnish National Qualifications Framework to the European Qualifications Framework and the Framework for Qualifications of the European Higher Education Area*. The Finnish National Agency for Education, p. 60. Available at: https://www.oph.fi/sites/default/files/documents/190482_report_on_the_referencing_of_the_finnish_national_qualifications_framework.pdf (Accessed: 2 January 2025).

Finnish National Agency for Education (2025) *Qualifications frameworks | Finnish National Agency for Education*. Available at: https://www.oph.fi/en/education-and-qualifications/qualifications-frameworks (Accessed: 1 February 2025).

Harris, G. (2024) 'How State Universities are addressing the Shortage of Cybersecurity Professionals in the United States', *Journal of Cybersecurity Education, Research and Practice*, 2024(1). Available at: https://doi.org/10.62915/2472-2707.1194.

ISC2 (2024) *Global Cybersecurity Workforce Prepares for an AI-Driven World*. Available at: https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/research/2024-ISC2-WFS.pdf (Accessed: 1 February 2025).

JYU (2023) *National cybersecurity education cooperation network | University of Jyväskylä*. Available at: https://www.jyu.fi/en/projects/national-cybersecurity-education-cooperation-network (Accessed: 30 January 2025).

Lehto, M. (2022) *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimus – hankkeen loppuraportti*. 93. University of Jyväskylä. Available at: https://urn.fi/URN:ISBN:978-951-39-9336-8.

Lehto, M. (2023) 'Kyberturvallisuuden ammattilaisten koulutus', *Cyberwatch Finland Magazine*, pp. 19–23.

Majanoja, A.-M., Ekqvist, J., Hakkala, A. and Virtanen, S. (2024) 'Kyberturvallisuuskoulutuksen kehittäminen Suomessa: yritysten osaamistarvekartoitus'. Available at: https://urn.fi/URN:ISBN:978-951-29-9920-0 (Accessed: 1 February 2025).

Majanoja, A.-M., Hakkala, A., Lehto, J. and Virtanen, S. (2024) 'Suomen kyberturvallisuuskoulutusta tarjoavien yliopistojen koulutuksen osaajaprofiilit ja kurssien painotusalat'. Available at: https://urn.fi/URN:ISBN:978-951-29-9916-3 (Accessed: 1 February 2025).

Ministry of Education and Culture (2022) *Kyberturvallisuusalan koulutusta kehitetään korkeakoulujen yhteistyönä – myös informaatiopsykologista tutkimusta vahvistetaan - OKM*, *Opetus- ja kulttuuriministeriö*. Available at: https://okm.fi/-

/kyberturvallisuusalan-koulutusta-kehitetaan-korkeakoulujen-yhteistyona-myos-informaatiopsykologista-tutkimusta-vahvistetaan?languageId=en_US (Accessed: 11 October 2024).

Ministry of Education and Culture (2025a) *Continuous learning reform - OKM - Ministry of Education and Culture, Finland*, *Opetus- ja kulttuuriministeriö*. Available at: https://okm.fi/en/continuous-learning-reform (Accessed: 2 February 2025).

Ministry of Education and Culture (2025b) *Finnish education system - OKM - Ministry of Education and Culture, Finland*, *Opetus- ja kulttuuriministeriö*. Available at: https://okm.fi/en/education-system (Accessed: 1 February 2025).

Ministry of Transport and Communications (2021) *Kyberturvallisuuden kehittämisohjelmatrans*. Sarjajulkaisu. Liikenne- ja viestintäministeriö. Available at: http://urn.fi/URN:ISBN:978-952-243-599-6 (Accessed: 11 October 2024).

Nai, F.I., Neisse, R., Hernandez, R.J.L., Polemi, N., Ruzzante, G.-L., Figwer, M. and Lazari, A. (2019) *A Proposal for a European Cybersecurity Taxonomy*. Available at: https://doi.org/10.2760/106002.

Perälä, P. and Lehto, M. (2023) *Selvitys yliopistojen kyberturvallisuusalan koulutuksen nykytilasta*. Internal report. Finland: University of Jyväskylä. Available at: Unpublished.

Perälä, P. and Lehto, M. (2024) 'Educating Cybersecurity Experts: Analysis of Cybersecurity Education in Finnish Universities', *European Conference on Cyber Warfare and Security*, 23(1), pp. 371–378. Available at: https://doi.org/10.34190/eccws.23.1.2256.

Prime Minister's Office (2024) *Finland's Cyber Security Strategy 2024–2035*. Available at: http://urn.fi/URN:ISBN:978-952-383-462-0.

Ramezan, C.A. (2023) 'Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field', *Journal of Information Systems Education*, 34(1), pp. 94–115.

Security Committee (2025) *Security Strategy for Society : Government resolution*. Finnish Government. Available at: http://urn.fi/URN:ISBN:978-952-383-817-8.

The Security Committee (2013) 'Finland's Cyber Security Strategy'. Available at: https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf (Accessed: 2 January 2025).

The Security Committee (2019) *Finland´s Cyber Security Strategy 2019*. Available at: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf (Accessed: 2 January 2025).