Educating Cybersecurity Experts: Analysis of Cybersecurity Education in Finnish Universities

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

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

Abstract: Cybersecurity is no longer just a technical discipline but a strategic concept. Nowadays, cybersecurity has become an essential part of national security strategies. The European Union and European countries have established cybersecurity strategies to strengthen European and national resilience against cyber threats and ensure that citizens and businesses can take full advantage of reliable services and digital tools. A wide range of actors in society, from both government and non-government sectors, are already involved in cybersecurity work. However, there is a constant need to increase the workforce of cybersecurity specialists to manage cybersecurity risks. Finland's cybersecurity strategy emphasizes the importance of developing cybersecurity education to address the cybersecurity risks the country faces. For the nation to achieve cyber self-sufficiency, the pool of cybersecurity specialists should include experts in every knowledge area relevant to various aspects of cybersecurity. Universities have a role in training cybersecurity specialists through their education programs. Consequently, universities should offer comprehensive education encompassing all cybersecurity knowledge areas. This paper aims to overview the state of cybersecurity education in Finland's universities by focusing on cybersecurity education content. By analysing the content of the universities' cybersecurity education, the aim was to understand how current education in Finland meets the cybersecurity knowledge areas of the European Cybersecurity Taxonomy. In spring 2023, data on cybersecurity degree programs and courses were collected through surveys from nine Finnish universities providing cybersecurity education. As a result, we gained an understanding of the capability of Finnish university-level cybersecurity education to offer specialists in different domain areas of cybersecurity.

Keywords: Cyber Education, Cyber Strategy, Security, Cyber Competence, Cybersecurity Taxonomy

1. Introduction

Over time, cybersecurity has evolved from a technical discipline to a strategic concept, leading to a situation in which cybersecurity has become an essential part of national security strategies. Countries have established cybersecurity strategies to protect national security against attacks and threats targeted at the cyber environment. The European Union and European countries are implementing their cybersecurity strategies to strengthen resilience against cyber threats and ensure that citizens and businesses can take full advantage of reliable services and digital tools (EU, 2020). Already, cybersecurity work employs many people in government and non-government sectors, but still, countries have a constant and rapidly increasing need for a workforce of cybersecurity specialists. In 2022, the need for a workforce in cybersecurity increased by 26%, and it has been estimated that the current need for employment is 3.4. million cybersecurity workers globally (McCann, 2023). In Finland, there is an anticipated demand for 5,000-8,000 new cybersecurity specialists in the coming years, along with an additional need for 1,000-5,000 professionals who can incorporate cybersecurity responsibilities into their current roles (Lehto, 2023). In addition, Finland needs to increase the number of highly educated people. According to the Finnish Government's Education Policy Report (*Education Policy Report of the Finnish Government*, 2021), "One of the objectives is that by 2030, at least one-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 must be completed by 2030 compared to what can be achieved with the current intake numbers." This need to increase the number of highly educated people is also reflected in the need for more highly educated cybersecurity experts. However, it is important not to forget the civil skills related to cybersecurity, as these skills play an increasingly important role as our societies become more digitised.

Finnish cybersecurity strategy (The Security Committee, 2019) emphasizes that developing cybersecurity education is the key to managing cybersecurity risks targeted to Finland. Developing cybersecurity education for specialists allows nations to pursue cyber self-sufficiency. Implementing a robust cybersecurity strategy requires competent employees at every level of the cyber environment to identify, build, and staff the cybersecurity infrastructure defences and responses (Evans and Reeder, 2010). However, the skills associated with cybersecurity specialists consist of a wide range of knowledge domains. For example, The European Cybersecurity Skills Framework (ECSF) developed by ENISA (The European Union Agency for Cybersecurity) summarizes the cybersecurity-related roles into 12 profiles that include over 60 different essential knowledge areas that are required to perform the work functions and duties in the profiled roles (ENISA, 2022). A vast

number of knowledge areas of cybersecurity specialists challenge cybersecurity education, as educational institutions should pursue organizing education in every cybersecurity knowledge area.

To ensure comprehensive cybersecurity education, various standards, guidelines, frameworks, and concepts can be utilized to improve cybersecurity curricula (AlDaajeh *et al.*, 2022). For example, the National Initiative for Cybersecurity Education (NICE) Framework (Petersen *et al.*, 2020) is widely used when developing, building, and assessing cybersecurity education (see, e.g. Conklin, Cline and Roosa, 2014; AlDaajeh *et al.*, 2022; Varbanov, 2022).

This paper presents an overview of cybersecurity education in Finland's universities by analysing and assessing the contents of cybersecurity courses provided by the universities. Even though the NICE as the US framework is widely accepted for assigning cybersecurity education, this paper utilized the European Cybersecurity Taxonomy. The paper aims to elucidate the extent to which the education aligns with European cybersecurity development work when assessed with the European Cybersecurity Taxonomy. Furthermore, the paper provides an understanding of the capacity of Finnish university-level cybersecurity education to provide expertise across various domains within the field of cybersecurity.

2. Assessing Cybersecurity University-Level Education

Numerous studies have assessed the state of national cybersecurity education in higher education to understand essential needs for developing educational programs. For example, Cabaj et al. (2018) analysed the cybersecurity master programs offered by 21 universities. Their analysis focused on identifying the specific cybersecurity topics covered and the distribution of these topics across various courses. Lehto (2020) provided insights into the principles and implementation models utilized in Finnish university-level cybersecurity education. Furthermore, Conklin et al. (2014) delved into the critical factors contributing to discrepancies between industry requirements and cybersecurity education content in the US. Their objective was to formulate recommendations for developing cybersecurity study programs that better align with the evolving needs of the industry.

While assessing cybersecurity education, studies commonly lie in analysing education by frameworks, taxonomies, or guidelines. One of the most applied frameworks is the NICE framework (e.g., Cabaj *et al.*, 2018; AlDaajeh *et al.*, 2022). The NICE (Petersen *et al.*, 2020) is a workforce framework for cybersecurity that was initially developed to meet the US government's needs concerning the workforce. Nowadays, the NICE framework is applied across public, private, and academic sectors. The NICE framework provides the cybersecurity audience with a common language to define cybersecurity work and the set of tasks and skills it requires.

In Europe, ENISA is providing the ECSF to support the identification and articulation of tasks, competencies, skills, and knowledge associated with the roles of European cybersecurity professionals (ENISA, 2022). In addition, the European Commission's Joint Research Centre published the European Cybersecurity Taxonomy (Nai *et al.*, 2019) to align the cybersecurity terminologies, definitions, and domains to capture all the aspects of building the cybersecurity realm of knowledge (The taxonomy is discussed in more detail in the next chapter). Other tools utilized in the assessment of cybersecurity education include:

- The Association for Computing Machinery has introduced the Computing Classification System (CCS). The CCS designates security and privacy as a prominent generic area (*Computing Classification System*, 2012).
- The Institute of Electrical and Electronics Engineers (IEEE) proposes a taxonomy to categorize the publications of events made available through the IEEE Xplore Digital Library (*IEEE Thesaurus and IEEE Taxonomy Access*, 2024).
- The Cybersecurity Curricula 2017 provides guidance in cybersecurity education to facilitate program development and other educational initiatives (Joint Task Force On Cybersecurity, 2017).

3. European Cybersecurity Taxonomy

In 2019, the Joint Research Centre, the science and knowledge service of the European Commission, introduced a proposal for a European Cybersecurity Taxonomy. The taxonomy aims to "align the cybersecurity terminologies, definitions, and domains into a coherent and comprehensive taxonomy to facilitate the categorization of EU cybersecurity competencies" (Nai *et al.*, 2019, p.5). The definitions and domain categorizations within the taxonomy are grounded in widely accepted standards, international classification systems from working groups, regulations, best practices, and recommendations within the cybersecurity

domain. (Nai *et al.*, 2019). The taxonomy aims to facilitate the alignment of European cybersecurity competencies.

The taxonomy includes three dimensions: "*research domains*", "*sectors*", and "*technologies and use cases*". *Research domains (*i.e., *cybersecurity knowledge domains)* represent cybersecurity knowledge areas, such as human, legal, ethical, and technological aspects. *Sectors* emphasize the need to consider different cybersecurity requirements and challenges from a human, legal, and ethical perspective in scenarios in different sectors. *Technologies and use cases* represent the technological enablers that enhance the development of the different sectors interrelated to cybersecurity domains covering technological aspects.

Cybersecurity knowledge is organized into fifteen distinct domains, each comprising specific sub-domains. A comprehensive list of sub-domains can be found in the "Proposal for a European Cybersecurity Taxonomy" (2019). According to the European Cybersecurity Taxonomy, definitions and examples of sub-domains of each cybersecurity knowledge domain are provided as follows:

- *Assurance, Audit, and Certification:* The methodologies, frameworks, and tools that provide the ground for confidence that a system, software, service, process, or network is working or has been designed to operate at the desired security target or according to a defined security policy. Examples of sub-domains are assurance, audit, assessment, and certification.
- *Cryptology (Cryptography and Cryptanalysis):* Cryptological aspects encompass mathematical, algorithmic, and technical facets, including the implementation of cryptanalytic methods, tools, and digital steganography techniques for concealing information. Examples of sub-domains include asymmetric cryptography, symmetric cryptography, mathematical foundations of cryptography, post-quantum cryptography, and homomorphic encryption.
- *Data Security and Privacy:* Security and privacy issues related to data that minimize or prevent privacy, confidentiality, and integrity risks during data processing. This should be achieved without inappropriately impairing data processing or by preventing data misuse after authorized entities access it. Specific sub-domains within this context include privacy requirements for data management systems, Digital Rights Management (DRM), risk analysis and attacks concerning de-anonymization or data re-identification (e.g., inference attack), and data usage control.
- *Education and Training:* The learning process that involves acquiring the knowledge, know-how, skills, and competencies necessary to protect network and information systems, their users, and affected individuals from cyber threats. Subdomains within this context include cybersecurity-aware culture (e.g., children's education), cyber ranges, Capture the Flag exercises, simulation platforms, educational/training tools, and cybersecurity awareness.
- *Human Aspects:* Within the cybersecurity domain, the interplay between ethics, relevant laws, regulations, policies, standards, psychology, and the human being. Subdomains include, for example, accessibility, usability, human-related risks/threats (social engineering, insider misuse, etc.), socio-technical security, user acceptance of security policies and technologies, psychological models and cognitive processes, human aspects of trust, and human perception of cybersecurity.
- *Identity Management:* Processes and policies that govern the lifecycle, value, type, and optional metadata of identity attributes within a specific domain, encompassing access management aspects such as authentication, authorization, and access control for individuals and smart objects when interacting with resources. This involves considerations of both physical and digital elements in authentication systems and legal aspects related to compliance and law enforcement. Sub-domains within this context may include identity and attribute management models, frameworks, applications, technologies, and tools (e.g., PKI, RFID, SSO, attribute-based credentials, federated IdM, etc.), along with protocols and frameworks for authentication, authorization, and rights management.
- *Incident Handling and Digital Forensics:* The theories, techniques, tools, and processes used to identify, collect, acquire, and preserve digital evidence. Sub-domains encompass incident analysis, communication, documentation, intelligence-based forecasting, response and reporting, vulnerability analysis and response, digital forensic processes and workflow models, as well as anti-forensics and malware analytics.
- *Legal Aspects:* The legal and ethical aspects related to the misuse of technology, illicit distribution, and reproduction of material covered by intellectual property rights (IPR), as well as the enforcement of laws about cybercrime and digital rights. Examples of sub-domains include

cybercrime prosecution and law enforcement, intellectual property rights, and legal and societal issues in information security (e.g., identity management, digital forensics, cybersecurity litigation).

- *Network and Distributed Systems:* Network security encompasses the hardware, software, fundamental communication protocols, network frame structure, and communication mechanisms within a network. In the network context, Information Security focuses on ensuring data integrity, confidentiality, availability, and non-repudiation during transmission across the network. Cybersecurity in a distributed system covers message authentication and all facets of computation, coordination, message integrity, availability, and (if required) confidentiality. Examples of sub-domains include principles, methods, protocols, algorithms, and technologies in network security, security considerations in distributed systems, such as managerial, procedural, and technical aspects, requirements for network security, protocols, and frameworks for secure distributed computing, as well as network layer attacks and mitigation techniques.
- *Security Management and Governance:* Security governance and management includes all those activities, methodologies, processes, and tools aimed at preserving confidentiality, integrity, and availability of information, as well as properties such as authenticity, accountability, and non-repudiation. Examples of sub-domains encompass risk management involving modelling, assessment, analysis, and mitigations, modelling of cross-sectoral interdependencies and cascading effects, threats and vulnerabilities modelling, attack modelling, techniques, and countermeasures (e.g., adversary machine learning).
- *Security Measurements:* Information security measures aim to facilitate decision-making and improve performance and accountability by collecting, analysing, and reporting relevant cybersecurity performance-related data. Measuring performance monitors the status of measured activities and facilitates improvement by applying corrective actions based on observed measurements. Examples of sub-domains include security analytics and visualization, security metrics, and key performance indicators and benchmarks.
- *Software and Hardware Security Engineering:* Security aspects in the software and hardware development lifecycle include risk and requirements analysis, architecture design, code implementation, validation, verification, testing, deployment, and runtime monitoring of operation. Examples of sub-domains comprise security requirements engineering emphasizing identity, privacy, accountability, and trust, security and risk analysis of components compositions, as well as secure software architectures and design (security by design).
- *Steganography, Steganalysis, and Watermarking:* Techniques for steganography, steganalysis, and watermarking. Steganography is a technique for hiding secret data within files or messages, while steganography deals with detecting hidden data using steganography. Digital watermarking is similar to steganography, where the embedded data typically is not secret, and the goal is also to ensure data integrity. Examples of sub-domains include steganography, steganalysis, and digital watermarking.
- *Theoretical Foundations:* Using analysis and verification techniques based on formal methods aims to provide theoretical proof of software, hardware, and algorithm design security properties. Examples of sub-domains include the formal specification of various security aspects (e.g., properties, threat models, etc.), formal specification, analysis, and verification of software and hardware, information flow modelling and its application to confidentiality policies, the composition of systems, and covert channel analysis.
- *Trust Management and Accountability:* Trust issues related to digital and physical entities such as applications, services, components, or systems. Trust management approaches can be employed to assess assurance and accountability guarantees. Examples of sub-domains encompass semantics and models for security, accountability, privacy, and trust, architectures, mechanisms, and policies for trust management, trust and privacy considerations, and identity and trust management.

4. Method

In the spring of 2023, data was collected from nine Finnish universities through online surveys concerning the universities' cybersecurity education (i.e., cybersecurity degree programs and courses). The survey included questions, for example, related to universities' cybersecurity degree education, as well as courses and course contents aimed at developing expertise in cybersecurity. The questionnaires were reviewed before data collection. Subsequently, the questionnaires were edited and refined in alignment with the suggestions provided

during the review. The questionnaires were distributed to the universities, where persons responsible for cybersecurity-related courses were expected to provide the needed information, considering the courses they were teaching. The responses received were checked for any gaps, and additions were requested from the universities if necessary.

Data was obtained from 96 courses that aim to develop skills in cybersecurity-related topic areas. The distribution of these courses across universities ranged from a minimum of one to a maximum of 28 courses offered by a single university. The levels of the courses were divided as follows: 64 advanced studies, 17 intermediate studies, 12 basic studies, and nine other studies. The sample did not include theses (Master's or Bachelor's).

During the analysis, we identified themes included in fifteen cybersecurity knowledge domains defined by the European Cybersecurity Taxonomy (2019) from course contents and learning outcomes. Content analysis (Weber, 1990) was used to identify the themes of courses and what cybersecurity knowledge domains were emphasized within and between courses. We followed the Joint Research Centre guidelines (Nai *et al.*, 2019, p.38) while applying the European Cybersecurity Taxonomy. We concentrated on identifying cybersecurity knowledge domains in each course but did not associate courses with an explicit sector, technology, or use case. This approach was chosen because, in many courses, the domain can be applied to different sectors, technologies, and use cases, causing a large number of combinations.

5. Results

The overview of Finnish universities' cybersecurity courses revealed identifiable themes based on the course contents, providing insights into the specific educational focus areas. These themes encompassed technical and technological cybersecurity, cybersecurity management, the societal perspective of cybersecurity, the human aspects of cybersecurity, and general cybersecurity themes. Education focused on technical and technological themes aims to develop technical skills and competence in cybersecurity. Typically, the goal is to gain specific technical knowledge in various domains within the field of cybersecurity. The cybersecurity management theme encompasses subject areas related to the management and the impact of cybersecurity within diverse organizations. The societal perspective of cybersecurity focuses on societal cybersecurity issues, such as cybersecurity's role in the information society, cybersecurity strategies, and operations. The educational content within the human perspective of cybersecurity address topics associated with individuals' cybersecurity, including individual security behaviour and the psychology of cybersecurity. The general cybersecurity theme concentrates on cybersecurity at a general level. These courses do not provide specific expertise in cybersecurity but aim to provide general knowledge and skills related to cybersecurity.

When looking at the priorities of the subject areas of cyber security education, it was found that universities' educational content focuses on developing technical and technological competence in cyber security. More than 60 percent of courses contained technical topics in the field of cyber security. In addition to technical and technological education, another focus theme of education was found to be cyber security management. Themes addressing cybersecurity from a societal or human perspective received less coverage in education. Figure 1 illustrates the distribution of Finnish universities' cybersecurity educational content across the different themes.

The analysis of cybersecurity education content in Finnish universities, in alignment with the European Cybersecurity Taxonomy, revealed that the contents of courses covered 14 out of the 15 cybersecurity knowledge domains specified by the taxonomy. Only content related to the knowledge domain concerning "*Steganography, Steganalysis, and Watermarking*" was not covered in cybersecurity courses. In most cases, several knowledge domains were identified to be covered in one course. For example, the content of the course called "*Cryptography in Networking*" covered five knowledge domains such as "*Cryptology*", "*Data Security and Privacy*", "*Identity Management*", "*Network and Distributed Systems*", and "*Software and Hardware Security Engineering*". However, it was found that in twenty-nine courses, contents could be identified as covering only one knowledge domain.

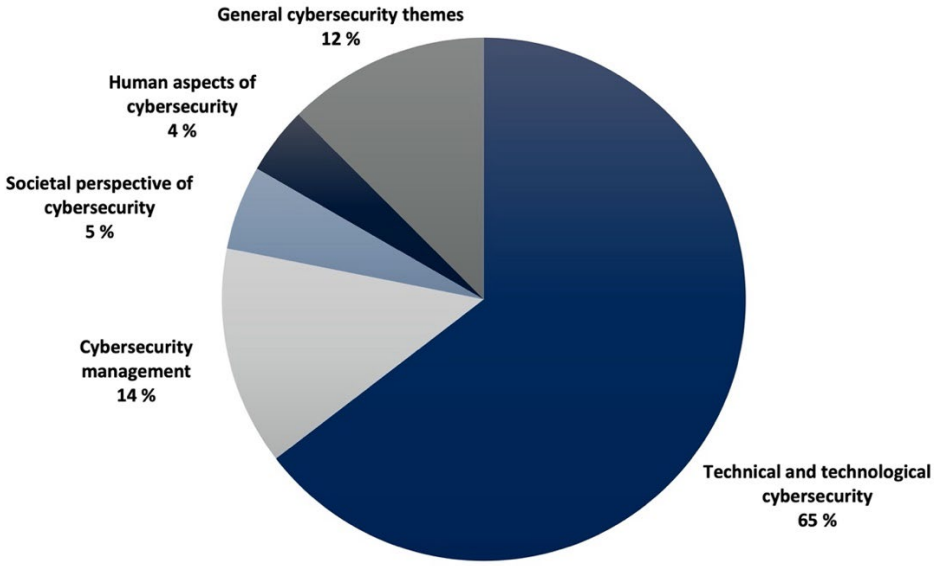

Figure 1: The distribution of Finnish universities' cybersecurity educational content across different themes.

More detailed analysis showed that the knowledge domain concerning "*Software and Hardware Security Engineering*" was the most represented in the course contents, as this area of expertise was part of the learning outcomes of 31 courses. Meanwhile, "*Cryptology*", "*Education and Training*", "*Network and Distributed Systems*", and "*Security Management and Governance*" knowledge domains were also strongly represented in the courses. These knowledge domains were part of the learning outcomes of over 20 courses. Whereas such knowledge domains as "*Legal Aspects*", "*Assurance, Audit, and Certification*", "*Theoretical Foundations*", and "*Trust Management and Accountability*" had the weakest representations in the courses. The "*Security Measurements*" domain was covered in 18 courses, "Identity Management" in 14 courses, "Data Security and Privacy" in 11 courses, "*Human Aspects*" in 9 courses, and "*Incident Handling and Digital Forensics*" in 6 courses.

In addition, we found it challenging to identify knowledge domains from the contents of several courses concentrating on AI, machine learning, and anomaly detection as part of different topics in cybersecurity. The taxonomy did not specify which knowledge domains these course contents covered. Table 1 illustrates the distribution of courses across different cybersecurity knowledge domains.

Table 1: The distribution of courses across different cybersecurity knowledge domains.

Cybersecurity knowledge domain of the European Cybersecurity Taxonomy	The number of courses representing the knowledge domain
Assurance, Audit, and Certification	2
Cryptology (Cryptography and Cryptanalysis)	21
Data Security and Privacy	11
Education and Training	21
Human Aspects	9
Identity Management	14
Incident Handling and Digital Forensics	6
Legal Aspects	3
Network and Distributed Systems	22
Security Management and Governance	23
Security Measurements	18
Software and Hardware Security Engineering	31
Steganography, Steganalysis, and Watermarking	0

Cybersecurity knowledge domain of the European Cybersecurity Taxonomy	The number of courses representing the knowledge domain
Theoretical Foundations	2
Trust Management and Accountability	2

6. Discussion and Conclusion

Cybersecurity has become an essential part of national security strategies. National cybersecurity strategies have been established to protect nations' security against attacks and threats targeted at the cyber environment. Competent employees from different cybersecurity knowledge domains are needed if nations wish to implement cybersecurity strategies robustly (Evans and Reeder, 2010). 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 programs at the universities in the field. However, these measures require an increase in human resources. Additionally, increasing the number of cybersecurity experts involves developing education at the university level. It is also essential for universities to strengthen conversion and continuing education, as continuous learning plays an important role in these efforts. Furthermore, improving educational cooperation between universities would enable students to acquire more versatile specializations in different areas of cybersecurity (Lehto, 2022). This goal is promoted in an ongoing research project between universities in Finland (JYU, 2024).

In this paper, we presented a study that assessed the capacity of cybersecurity education in Finnish universities to train expertise and skills that cover the knowledge domains outlined in the European Cybersecurity Taxonomy. We analysed data from 96 cybersecurity courses from nine Finnish universities. Our findings indicated that Finnish universities provide relatively comprehensive cybersecurity education, as the contents of courses covered all other cybersecurity knowledge domains in the European Cybersecurity Taxonomy except for the domain called "*Steganography, Steganalysis, and Watermarking"*. The courses were commonly broad in scope, as one course could cover several cybersecurity knowledge areas. Course contents aiming to develop technical and technological expertise in cybersecurity were found to have the most extensive coverage in educational offerings. On the other hand, education on the less technical aspects of cybersecurity issues received comparatively less coverage in the courses. These findings align with the observation made by Cabaj et al. (2018) and Blažič (2022), as they noticed the scarcity of less technical educational content in cybersecurity education programs. Furthermore, the analysis revealed that the educational content at universities included topics that could not be categorized explicitly within any cybersecurity knowledge domains in the taxonomy.

Our findings increase the understanding of the coverage of cybersecurity education in Finnish universities by considering the content of cybersecurity courses through the European Cybersecurity Taxonomy. The results can be utilized as a base for the debate on how to direct and develop Finnish university-level cybersecurity education so that programs educate the workforce with a broad range of specialized expertise in cybersecurity. In addition, the results can be utilized as an initial step towards developing Finnish university-level cybersecurity education to align with European cybersecure educational work.

Based on the findings, some recommendations could be stated. As the university-level cybersecurity education intends to educate experts with a wide range of cybersecurity skills, the Finnish university-level education should be developed in a way that in the future it would cover all cybersecurity knowledge domains of the European Cybersecurity Taxonomy. Especially courses covering topics related to the knowledge domain of "Steganography, Steganalysis, and Watermarking" should be developed. Furthermore, educational content should be strengthened for those cybersecurity knowledge domains where courses are less available. (e.g., "*Trust Management and Accountability*", "*Theoretical Foundations, Assurance, Audit, and Certification*"). As the universities' cybersecurity education focuses on developing technical skills, the education aiming at less technical competence should be increased to enhance the competence of cybersecurity experts (Cabaj *et al.*, 2018; Blažič, 2022). Overall, universities' cybersecurity education should maintain a multidisciplinary approach that provides valuable skills to address national cybersecurity issues effectively and helps prepare for the complexities of critical fields (Lehto, 2020).

Additionally, Finnish universities' cybersecurity education content should be regularly assessed against the European cybersecurity knowledge frameworks (e.g., ENISA and European Cybersecurity Taxonomy) to ensure extensive university-level cybersecurity education that aligns with European recommendations considering

cybersecurity competencies. This ongoing assessment contributes to achieving more coherent cybersecurity education in Europe and potentially reduces variation in educational content between European nations.

This study has several limitations. This paper discusses the coverage of Finnish university-level cybersecurity education only from one European taxonomy. A more comprehensive understanding requires that universities' education be reviewed through other cybersecurity frameworks, taxonomies, and classification systems. In addition, the education assessment is based on the description of course contents and learning outcomes. A deeper understanding of the course contents requires more detailed information, as the course potentially covers more topics than described in the course description and learning outcomes.

Acknowledgements

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

References

AlDaajeh, S. *et al.* (2022) 'The role of national cybersecurity strategies on the improvement of cybersecurity education', *Computers & Security*, 119, p. 102754. Available at: https://doi.org/10.1016/j.cose.2022.102754.

Blažič, B.J. (2022) 'Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?', *Education and Information Technologies*, 27(3), pp. 3011–3036. Available at: https://doi.org/10.1007/s10639-021-10704-y.

Cabaj, K. *et al.* (2018) 'Cybersecurity education: Evolution of the discipline and analysis of master programs', *Computers & Security*, 75, pp. 24–35. Available at: https://doi.org/10.1016/j.cose.2018.01.015.

Computing Classification System (2012) *ACM Digital Library*. Available at: https://dl.acm.org/ccs (Accessed: 27 January 2024).

Conklin, Wm.A., Cline, R.E. and Roosa, T. (2014) 'Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors', in *2014 47th Hawaii International Conference on System Sciences*. *2014 47th Hawaii International Conference on System Sciences*, pp. 2006–2014. Available at: https://doi.org/10.1109/HICSS.2014.254.

Education Policy Report of the Finnish Government (2021). Publications of the Finnish Government 2021:64. Finnish Government. Available at: https://julkaisut.valtioneuvosto.fi/handle/10024/163273 (Accessed: 30 January 2024).

ENISA (2022) *European Cybersecurity Skills Framework (ECSF)*. Available at: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework.

EU (2020) *The EU's Cybersecurity Strategy for the Digital Decade*. Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

Evans, K. and Reeder, F. (2010) *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters*. CSIS.

IEEE Thesaurus and IEEE Taxonomy Access (2024). Available at: https://www.ieee.org/publications/services/thesaurus-thank-you.html (Accessed: 27 January 2024).

Joint Task Force On Cybersecurity (2017) *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. New York, NY, USA: ACM. Available at: https://doi.org/10.1145/3422808.

JYU (2024) *National cybersecurity education cooperation network | University of Jyväskylä*. Available at: https://www.jyu.fi/en/projects/national-cybersecurity-education-cooperation-network (Accessed: 30 January 2024).

Lehto, M. (2020) 'Cyber security capacity building -cyber security education in Finnish universities Cyber security capacity building -cyber security education in Finnish universities', in *Proceedings of the 19th European Conference on Cyber Warfare and Security, ECCWS2020,* pp. 221–231. Available at: https://doi.org/10.34190/EWS.20.112.

Lehto, M. (2022) *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimus – hankkeen loppuraportti*. 93. University of Jyväskylä. Available at: https://jyx.jyu.fi/bitstream/handle/123456789/82709/Kyberturvallisuuden%20koulutusohjelman%20muutostarpeiden%20tutkimus%20v4.pdf.

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

McCann, M. (2023) *Council Post: The Quest To Close The Cybersecurity Talent Gap*, *Forbes*. Available at: https://www.forbes.com/sites/forbeshumanresourcescouncil/2023/10/16/the-quest-to-close-the-cybersecurity-talent-gap/ (Accessed: 27 January 2024).

Nai, F.I. *et al.* (2019) *A Proposal for a European Cybersecurity Taxonomy*. Available at: https://doi.org/10.2760/106002.

Petersen, R. *et al.* (2020) *Workforce Framework for Cybersecurity (NICE Framework)*. National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.800-181r1.

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

Varbanov, P. (2022) 'Perspectives in the Design of a Modern Cybersecurity Training Programme: The ECHO Approach', *Information & Security: An International Journal*, 53, pp. 177–190. Available at: https://doi.org/10.11610/isij.5312.

Weber, R.P. (1990) *Basic Content Analysis*. SAGE.