Cybersecurity Education in Finnish Universities of Applied Sciences: Workforce Alignment

Jani Ekqvist[1], Pasi Kämppi[2] and Jyri Rajamäki[2]
[1]Turku University of Applied Sciences, Turku, Finland
[2]Laurea University of Applied Sciences, Espoo, Finland

jani.ekqvist@turkuamk.fi
pasi.kamppi@laurea.fi
jyri.rajamaki@laurea.fi

Abstract: Performing effectively in cybersecurity work roles demands a diverse professional skill set. Fresh graduates often struggle to meet the high expectations of employers. This study assesses how 12 Finnish universities of applied sciences equip students with the most relevant professional skills for graduates' early careers. The question is topical because the cybersecurity profession suffers from a worldwide workforce shortage, with Finland requiring between 6000 and 13000 additional experts. This study compares the bachelor's and master's level study offerings in information and communications technology (ICT) of 12 universities of applied sciences in Finland with the professional skill requirements set by local companies and organizations for cybersecurity roles. The study offerings of participating universities are profiled and categorized based on the EU Joint Research Centre (JRC) Cybersecurity and Bloom's taxonomies. As an outcome, this study represents visually how study offerings in the participating universities of applied sciences align with industry needs and employer expectations. Previous studies in Finland on university-level cybersecurity education have been based on the U.S.-originated National Initiative for Cybersecurity Education (NICE) Framework. This study extends the current understanding and leverages the latest interview and survey-based research results and the European Joint Research Centre Cybersecurity Taxonomy. Among the bachelor's degree programs, five universities provide cybersecurity-focused programs, four universities offer complementary mid-level cybersecurity studies integrated within the non-cyber-focused education, and three universities have remarkably low-level cybersecurity study offerings in their curricula. The master's degree programs are well-aligned with each other and complement the bachelor's degree programs according to the Finnish dual model educational system.

Keywords: Cybersecurity competencies, Workforce alignment, Cybersecurity education

1. Introduction

Workforce shortage in cybersecurity has been widely reported globally and locally in Finland. In Development Needs in Cybersecurity Education, it is estimated that Finland alone will require between 6000 and 13000 cybersecurity professionals over the next few years (Lehto, 2022). OECD states that in Europe, there is a shortage of over 300 000 professionals, and the World Economic Forum estimates a global shortage of nearly 4 million professionals in cybersecurity (OECD, 2024; World Economic Forum, 2024). Solving this shortage requires increasing the number of cybersecurity graduates and ensuring that their education meets the industrial competency requirements. Thus, according to The Finnish Universities of Applied Sciences Act, "Ammattikorkeakoululaki" (L 14.11.2014/932), addressing the shortage is at the core of the mission of the universities of applied sciences (UAS) in Finland.

There have been several studies about the professional cybersecurity skills requirements for the workforce in Finland, and a few have been on designing a cybersecurity curriculum. However, a systematic review of the UAS cybersecurity curriculums is missing. Moreover, thus far, studies have been based on the National Initiative for Cybersecurity Education Framework from the United States (Petersen et al., 2020). This study utilizes the European Union's Joint Research Centre Cybersecurity Taxonomy (Nai, Hernandez and Neisse, 2021) and Bloom's taxonomy. This provides a better understanding of the required professional skills and knowledge in the European context compared to the US-centric NICE framework. Specifically, the competence domains of the taxonomy are used to categorize the requirements.

The study is a case study of 12 universities of applied sciences participating in a national cybersecurity education development project. Its purpose is to determine how the study offerings in bachelor's and master's ICT degree programs meet workforce professional skills requirements.

This article is structured as follows: section two reviews existing research. Section three represents the research methodology utilized in this study. Section four analyses the previous research into professional skills requirements for the cybersecurity workforce in Finland from recent years and aggregates a list of the industry's most sought-after categories of competence. Section five presents the research results of analyzing the

cybersecurity offerings of Finnish UASes and compares them to the identified requirements, and section six discusses the research findings.

2. Literature Review

Few previous studies exist on aligning cybersecurity curriculums in Finland with workforce requirements. Saharinen, Viinikanoja, and Huotari (2022) surveyed 19 graduates after one to three years of employment in a bachelor's degree program with a cybersecurity focus and compared their current work roles to the NICE framework with seven categories. In Development Needs in Cybersecurity Education (Lehto, 2022), industry needs were also categorized following the NICE framework. Both studies found that the employment possibilities are more promising in Protect and Defend, Operate and Maintain, and Securely Provision according to NICE categorization.

Following the enhanced European Union Joint Research Center's Cybersecurity Taxonomy, professional skills were divided into 16 categories. Kämppi, Ekqvist and Rajamäki (2025) interviewed eight cybersecurity services and consulting business professionals in Finland. The Finnish service and consulting business seeks graduates with networking, programming and incident management skills. In the report by Majanoja et al. (2024), 61 Finnish organizations answered a questionnaire about the current and future cybersecurity competency complemented by interviewing 14 respondents. Their findings support the earlier studies and show that technical competency is essential, especially in operative cybersecurity.

The NICE Framework Components have been updated in 2024 with terminology refinement and updated category names (NIST, 2024). There are discrepancies in the naming between Saharinen, Viinikanoja, and Huotari (2022) and Lehto (2022), which is possibly explained by the ongoing development of the framework. The changes in the new scheme put more focus on national cybersecurity operations. This may explain why they are not prominent in either Finnish study that follows the NICE framework, as they are less relevant for the private sector. Unfortunately, this effectively reduces the decision space, making it harder to map the identified categories between the studies. On the other hand, the category descriptions from the earlier version of the NICE Framework do not yet make this distinction as explicitly (Petersen et al., 2020). The JRC taxonomy is more granular, focused on industrial needs, and fits better in Europe.

3. Research Methodology

The study was made as a single case study among 12 Finnish ICT-focused universities of applied sciences with an embedded multiple-case approach where a single university represents a subcase. Yin (2013) states that the subunits allow for more extensive analysis and enhance the insights of the selected case. According to Gerring (2006), the within-case results will be better with a limited number of carefully selected homogeneous subunits than with numerous heterogeneous samples.

The set research question was:

- How does the study offering of the 12 Finnish ICT-focused universities of applied sciences match the professional skill set requirements of the Finnish cybersecurity industry?

In practice, each university of applied science was instructed to assess the study offering with Bloom's and JRC taxonomy. After analyzing 12 educational institutes, the results of assessments were compared to professional skill set requirements, and conclusions were drawn. The research process is illustrated in Figure 1.

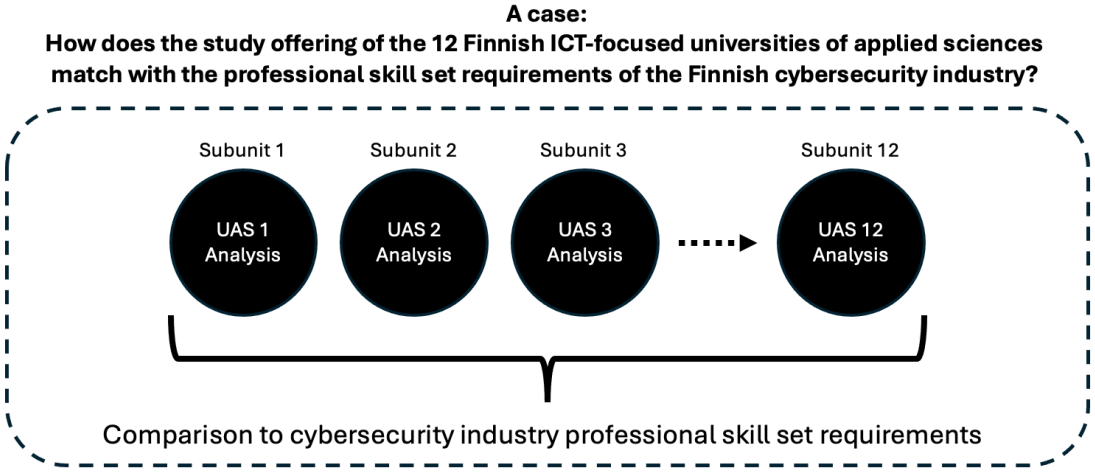

Figure 1: The research process for matching university offerings with professional skill set requirements

3.1 Analysis Framework

The rationale behind the analysis framework is to give clear instructions for researchers on how to proceed with the analysis in every university of applied sciences being analyzed. Van Niekerk and Von Solms (2013) remind us that curriculums can be created by professionals who are unaware of the learning theories. Thus, it is necessary to ensure that the analysis is academically precise and correct.

There are already examples of how the revised Bloom's taxonomy can be applied to information security and cybersecurity (Van Niekerk and Von Solms, 2013; Harris and Patten, 2015; Ramsoonder et al., 2020). Common for all papers, as mentioned earlier, is that the researchers aim to align all layers of the revised Bloom's taxonomy with information security and cybersecurity-specific learning objectives and verbs. Harris and Patten (2015) present an example of how the revised Bloom's taxonomy can be integrated with ACM IT2008 Curriculum Model and Ramsoonder et al. (2020) rely on the NICE) framework. Harris and Patten (2015) conclude that the model can be used to design and assess an existing curriculum.

The analysis of the study offerings in this paper is based on the combination of JRC Taxonomy (Nai, Hernandez and Neisse, 2022), Bloom's for Computing (ACM Committee for Computing Education in Community Colleges (CCECC), 2023) and Revised Bloom's Taxonomy (Van Niekerk and Von Solms, 2013; Harris and Patten, 2015). The analysis framework has been adapted and developed further from Van Niekerk and Von Solms (2013) and Harris and Patten (2025). The improved analysis framework aims to ensure that the results of the analysis follow equal measures. In the first place, each course of the curriculum is looked through the JRC taxonomy matrix and then looked at which categories of the JRC taxonomy are covered. After mapping the categories, each covered category's learning level (1-3) is evaluated based on Bloom's for Computing verbs and revised Bloom's taxonomy. As a result, each course in the curriculum has an individual profile that indicates what categories are covered and associated with the desired learning levels (1-3). The analysis framework is presented in Figure 2.

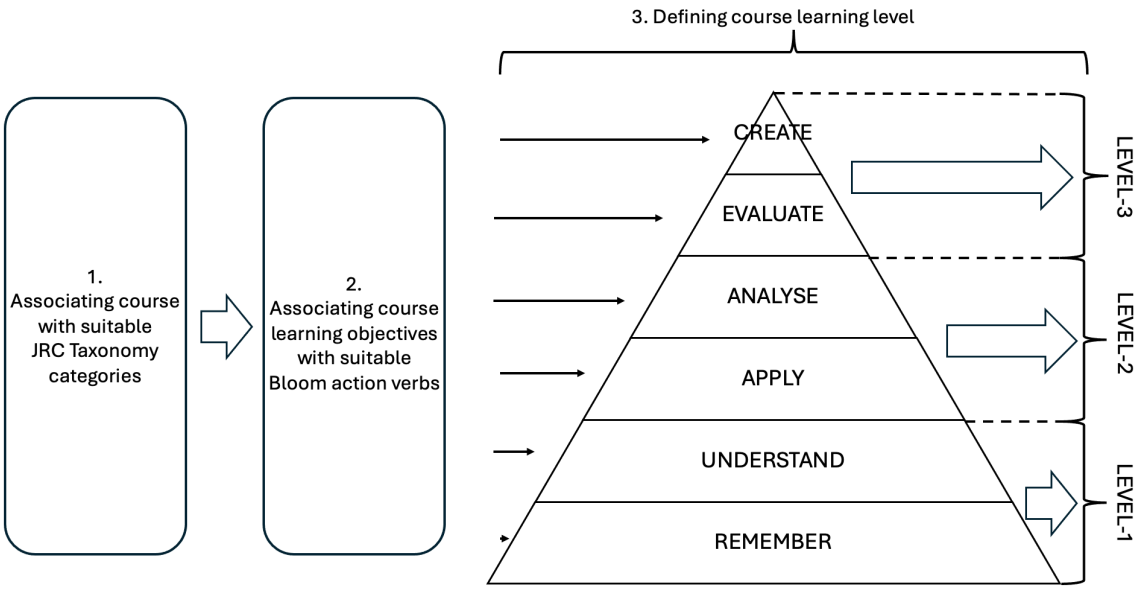

Figure 2: The analysis framework (adapted from Van Niekerk and Von Solms (2013) and Harris and Patten (2025)

3.2 Quantification and Profiling

The presented model enables quantifying the desired competency levels and profiling for an individual course, a whole curriculum, or a university. This paper uses the applied quantification and profiling framework to find a university-based profile that indicates the highest competency level associated with the JRC taxonomy. Table 1 presents an example of two universities profiled according to the presented model. The competency index for UAS1 is 22, averaging 1,69 when shared among all JRC categories. Equivalent indexes for UAS2 are SUM=22 and AVG=2,14. Vertical column summaries and averages indicate the competency indexes per JRC categories among the analyzed universities. In the presented example, JRC categories 5, 8, 10, and 11 have the highest indexes, and category 13 has the lowest index.

Table 1: An example of profiling UAS offerings in each JRC Category

	JRC Categories														
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**SUM**	**AVG**
UAS1	*1*	*2*	*2*	*1*	*1*	*2*	*3*	*1*	*3*	*1*	*1*	*3*	*1*	*22*	*1,69*
UAS2	*1*	*0*	*0*	*2*	*3*	*0*	*0*	*3*	*0*	*3*	*3*	*0*	*0*	*15*	*2,14*
SUM	*2*	*2*	*2*	*3*	*4*	*2*	*3*	*4*	*3*	*4*	*4*	*3*	*1*		
AVG	*1*	*1*	*1*	*1,5*	*2*	*1*	*1,5*	*2*	*1,5*	*2*	*2*	*1,5*	*0,5*		

4. Professional Skills Requirements

In Saharinen, Viinikanoja and Huotari (2022) the most prominent NICE Framework categories of work roles were Protect and Defend, and Operate and Maintain, followed by Securely Provision. The most common work roles were Cyber Defense Analyst and Cyber Defense Incident Responder. In Development Needs in Cybersecurity Education (Lehto, 2022), the category with the highest need of professionals was Secure Production, followed by Protection and Defense, Oversight and Governance, and Operation and Maintenance. Other categories are Analysis, Collection of Data and Operation, and Investigation.

In the report by Majanoja et al. (2024), the five most important JRC categories of skills currently for organizations are Data Security and Privacy, Education and Training, Identity Management, Security Management and Governance, and Legal Aspects. In contrast, in Kämppi, Ekqvist and Rajamäki (2025) the categories were Software and Hardware Security Engineering, Network and Distributed Systems, Incident Handling and Digital Forensics, Security Management and Governance, and Assurance, Audit and Certification.

Table 22: Five most important professional skill categories in each study and mapping them between the frameworks

	Saharinen et al. (2022)	**Lehto (2022)**	**Majanoja et al. (2024)**	**Kämppi et al. (2025)**	**Saharinen et al. mapped to JRC**	**Lehto mapped to JRC**	**Majanoja et al. mapped to NICE**	**Kämppi et al. mapped to NICE**
1.	Protection and Defense	Secure Production	Data Security and Privacy	Software and Hardware Security Engineering	Incident Handling and Digital Forensics	Software and Hardware Security Engineering	Implementation and Operation	Design and Development
2.	Operation and Maintenance	Protection and Defense	Education and Training	Network and Distributed Systems	Network and Distributed Systems	Incident Handling and Digital Forensics	Oversight and Governance	Implementation and Operation
3.	Securely Provision	Oversight and Governance	Identity Management	Incident Handling and Digital Forensics	Software and Hardware Security Engineering	Security Management and Governance	Design and Development	Protection and Defense
4.	Analyze	Operation and Maintenance	Security Management and Governance	Security Management and Governance	Software and Hardware Security Engineering	Network and Distributed Systems	Oversight and Governance	Oversight and Governance
5.	Investigate	Analysis	Legal Aspects	Assurance, Audit and Certification	Incident Handling and Digital Forensics	Software and Hardware Security Engineering	Oversight and Governance	Protection and Defense

As seen in Table 2 , there is no clear-cut ordering between the categories. Using the NICE Framework mappings, the small number of relevant categories does not allow for distinguishing the priorities well. Some important categories can be identified when studies are compared using the JRC taxonomy mapping. Software and Hardware Security Engineering, Incident Handling and Digital Forensics, Network and Distributed Systems, and Security Management and Governance are all present in three studies out of four. The criteria for choosing the fifth most important category is not clear. Based on the identified and mapped categories, it could be argued that either Data Security and Privacy, or Assurance, Audit and Certification should be chosen.

The most differing results from other studies are obtained by Majanoja et al. (2024). The reason is not immediately evident from any differences in methodology in the studies. All four studies have Finnish cybersecurity professionals as their main demography. Kämppi, Ekqvist and Rajamäki (2025) is based on interviews, Saharinen, Viinikanoja and Huotari (2022) and Majanoja et al. (2024) are surveys, and Lehto (2022) is a meta-analysis of several mostly survey and job advertisement-based sources. Kämppi, Ekqvist and Rajamäki (2025) do note that the results of the study are in line with the ISC2 Cybersecurity Workforce Study by the International Information Systems Security Certification Consortium (ISC2, 2023) and the State of Cybersecurity 2023 by Information Systems Audit and Control Association (ISACA, 2023). Likewise, Lehto (2022) noted that the distribution identified in the study aligns with the 2022 version of the ISC2 study and in cybersecurity job advertisements in the United States collected by CyberSeek.

Selection of the fifth most important category is left to the analysis phase and both options, Data Security and Privacy, and Assurance, Audit and Certification are examined. As the methodologies, scales and results of the studies differ, the list of categories should not be regarded as a definite priority order. They have been ordered based on their occurrence and position in each study's top five category list (Table 3).

Table 33: Aggregation of top five professional skill categories from the reviewed studies

Software and Hardware Security Engineering
Incident Handling and Digital Forensics
Network and Distributed Systems
Security Management and Governance
Data Security and Privacy, and Assurance, Audit and Certification

5. Results

The curriculum evaluation was conducted for 12 Finnish universities of applied sciences that participated in the national cybersecurity education development project. Notably, there are 24 universities of applied sciences in Finland and not all of them are presented in the study. However, all applied sciences universities that focus on cybersecurity are presented, and collectively, the studied universities have over 70% of all UAS ICT students in Finland (Vipunen, 2025). Curriculums are evaluated separately for bachelor's and master's degrees.

5.1 Bachelor's Degrees

The table 4 presents the demography for the bachelor-level degree programs being studied. Ten universities of applied sciences offer only Bachelor of Engineering (BEng) education, one institute offers only Bachelor of Information Technology (BIT) education, and one institute offers both BEng and BIT education. Four faculties focus on cybersecurity, and they provide bachelor-level cybersecurity degree programs. Other faculties have cybersecurity study offerings but have not profiled themselves as cybersecurity-focused universities of applied sciences. The number of cybersecurity-related courses varies from 4 to 23, while the amount of offered credits, according to the European Credit Transfer and Accumulation System (ECTS) varies from 13 to 115.

Table 44: Demography of cybersecurity education of the studied universities

UAS	Education	Cybersecurity degree	Number of Courses	Number of ECTS
South-Eastern Finland (XAMK)	BEng	Yes	23	115
Jyväskylä (JAMK)	BEng	Yes	22	108
Laurea	BIT	Yes	13	62
Turku (TurkuAMK)	BEng/BIT	Yes	13	60
Tampere (TAMK)	BEng	No	7	33
Oulu (OAMK)	BEng	No	6	28
Vaasa (VAMK)	BEng	No	6	26
Lapin AMK	BEng	No	5	25
Metropolia	BEng	No	6	20
Karelia AMK	BEng	No	3	15
Savonia	BEng	No	3	15
Centria	BEng	No	4	13
Master TurkuAMK	MEng/MBA	Yes	6	30
Master XAMK	MEng	Yes	5	25
Master JAMK	MEng	Yes	4	20

Figure 3 shows the distinct separation between universities offering a cybersecurity degree and those that do not. Cybersecurity-focused universities are highlighted in the orange figure. The only exception is the Tampere University of Applied Sciences (TAMK), which does not have a cybersecurity-focused degree but offers a wide range of cybersecurity courses and a deeper understanding of selected categories for ICT engineering students. When comparing Table with Figure 3, they align with each other as universities that offer cybersecurity degrees have a higher number of courses and ECTS, and naturally have a higher level of offering in JRC categories. The offering levels do not match the number of courses and ECTS strictly, as some universities have incorporated cybersecurity as part of other ICT courses, whereas universities with cybersecurity degrees especially offer courses specializing in cybersecurity. The universities reported all courses that contain cybersecurity and reported the total ECTS granted for each course.

	JRC Categories														
	1	2	3	4	5	6	7	8	9	10	11	12	13	SUM	AVG
JAMK	2	3	2	3	2	2	3	2	3	3	3	3	2	33	2,54
TurkuAMK	3	2	3	1	2	1	3	2	2	3	3	3	1	29	2,23
Laurea	2	2	2	2	3	1	1	2	3	3	3	3	1	28	2,15
TAMK	2	3	1	2	2	2	3	1	3	2	2	2	2	27	2,08
XAMK	2	2	2	2	2	3	3	2	3	2	2	2	0	27	2,08
VAMK	2	2	2	2	1	2	1	1	3	2	2	2	0	22	1,69
Karelia AMK	1	2	2	2	2	2	2	1	1	1	1	3	1	21	1,62
Metropolia	1	1	1	1	2	1	2	1	2	1	2	3	1	19	1,46
Lapin AMK	1	3	2	1	2	1	2	1	1	1	1	1	0	17	1,31
Centria	0	2	2	0	1	1	1	1	2	1	0	1	1	13	1,00
OAMK	0	0	2	1	1	0	0	1	0	0	0	0	0	5	0,38
Savonia														0	
SUM	16	22	21	17	20	16	21	15	23	19	19	23	9		
AVG	1,45	2,00	1,91	1,55	1,82	1,45	1,91	1,36	2,09	1,73	1,73	2,09	0,82		
SUM-Cyber	9	9	9	8	9	7	10	8	11	11	11	11	4		
AVG-Cyber	2,25	2,25	2,25	2	2,25	1,75	2,5	2	2,75	2,75	2,75	2,75	1		

LEGEND:

1 Assurance, Audit, and Certification
2 Cryptology
3 Data Security and Privacy
4 Education and Training
5 Human Aspects
6 Identity Management
7 Incident Handling and Dig. Forensics
8 Legal Aspects
9 Network and Distributed Systems
10 Security Management and Governance
11 Security Measurements
12 Software and Hardware Security Engineering
13 Steganography, Steganalysis and Watermarking

Highest Overall Offerings
Cyber-focused UAS values
Bloom Level 3
Bloom Level 2
Bloom Level 1
No Offering

Figure 3: Highest level of bachelor offering of each university for each JRC category

The focus of offering in different JRC categories (Figure 3) is also relatively consistent between the universities. The highest overall offering is in Network and Distributed Systems, and Software and Hardware Security Engineering. These are followed closely by Cryptology, Data Security and Privacy, and Incident Handling and Digital Forensics. Some specialization can still be seen between the cybersecurity-focused universities. TurkuAMK is the only one offering level 3 Assurance, Audit and Certification, and Data Security and Privacy courses, Laurea specializes in Human Aspects, and XAMK has the only level 3 Identity Management offering. Overall, JAMK has the highest average of the category levels at 2,54, with other cybersecurity-focused universities having an average level between 2,23 and 2,08. Other universities are well below this, averaging between 1,69 and 0. Karelia AMK and Metropolia have a level 3 offering in Software and Hardware Security Engineering, and Lapin AMK in Cryptology.

If only universities offering a cybersecurity degree are evaluated, the focus of categories somewhat changes. Network and Distributed Systems, and Software and Hardware Security Engineering are still in the most prominent categories, but Security Management and Governance, and Security Measurements share the same average level. Incident Handling and Digital Forensics is still the fifth most prominent category. There is little focus on Steganography, Steganalysis and Watermarking, but the level of offering in all other categories averages between 2,00 and 2,75.

Table 55: Comparison of bachelor's level offerings and workforce requirements by most prominent JRC categories

Overall UAS Offerings	Cyber-focused UAS Offerings	Workforce Requirements
Network and Distributed Systems	Network and Distributed Systems	Software and Hardware Security Engineering
Software and Hardware Security Engineering	Software and Hardware Security Engineering	Incident Handling and Digital Forensics
Cryptology	Security Management and Governance	Network and Distributed Systems
Data Security and Privacy	Security Measurements	Security Management and Governance
Incident Handling and Digital Forensics	Incident Handling and Digital Forensics	Data Security and Privacy, or Assurance, Audit and Certification

Table 5 compares the JRC categories of the five highest bachelor's level offerings of the universities with the five highest skills requirements in the workforce. The three most essential requirements in the workforce, namely Software and Hardware Security Engineering, Incident Handling and Digital Forensics, and Network and Distributed Systems, are also well presented in the offerings of the universities. Security Management and Governance offering is concentrated in cybersecurity-focused universities, which provide a high level of competence. Still, whether this is enough to satisfy the workforce demand is unclear. Data Security and Privacy, and Assurance, Audit and Certification are not in the focus of offering with only TurkuAMK having level 3 content, but Data Security and Privacy is still the fourth highest in overall UAS offerings. From the overall UAS offerings, Cryptology is not as highly valued by the workforce, and neither are Security Measurements from the cybersecurity-focused offerings. In conclusion, the offerings of the universities are well-matched to the top requirements of the workforce overall, but there is still room for improvement in the less prominent categories.

5.2 Master's Degrees

	JRC Categories														
	1	2	3	4	5	6	7	8	9	10	11	12	13	SUM	AVG
YAMK JAMK	3	2	2	2	2	2	3	1	3	3	3	3	1	30	2,31
YAMK XAMK	2	3	1	3	2	0	3	2	3	2	2	3	0	26	2,00
YAMK TurkuAMK	2	0	1	2	3	2	3	2	2	3	3	3	0	26	2,00
SUM	7	5	4	7	7	4	9	5	8	8	8	9	1		
AVG	2,33	1,67	1,33	2,33	2,33	1,33	3,00	1,67	2,67	2,67	2,67	3,00	0,33		

LEGEND:

1 Assurance, Audit, and Certification
2 Cryptology
3 Data Security and Privacy
4 Education and Training
5 Human Aspects
6 Identity Management
7 Incident Handling and Dig. Forensics
8 Legal Aspects
9 Network and Distributed Systems
10 Security Management and Governance
11 Security Measurements
12 Software and Hardware Security Engineering
13 Steganography, Steganalysis and Watermarking

Highest Overall Offerings
Bloom Level 3
Bloom Level 2
Bloom Level 1
No Offering

Figure 4: Highest level of master offering of each university for each JRC category

Three universities of applied sciences offer master's degrees in cybersecurity in Finland: JAMK, TurkuAMK, and XAMK. To be eligible for a master's degree studies in a Finnish university of applied sciences, the student must complete a bachelor's degree in a relevant field and have at least two years of relevant work experience to emphasize the working life connection (L 14.11.2014/932, HE 21/2001 vp). Thus, master's level students do have at least general ICT experience but not necessarily specific expertise in cybersecurity. This is also reflected in the offering evaluation results, as the overall competence level reached is the same or even lower than in the bachelor's studies at all three universities. Master's degree requires 60 credit units (CU) if the student has previously completed an engineering degree. 30 CUs are reserved for the thesis and 5-10 focus on general research knowledge, so only 20-25 CUs of the studies are from the analyzed offerings. If a student has completed another bachelor's degree, typically in ICT business administration, the requirement is 90 CUs, but as can be seen from table 4, no university offers cybersecurity courses for the full amount.

The categories with the highest level of offering in all universities are Incident Handling and Digital Forensics, and Software and Hardware Security Engineering with every university having a level 3 offering. They are followed by Security Management and Governance, Security Measurements, and Network and Distributed Systems, where the average is 2,67. The least emphasis is given to Steganography, Steganalysis, and Watermarking, with only one university offering it at all, and only at level 1. At the level of this analysis, the differences between the universities are minor. TurkuAMK does not include cryptology in the studies and offers both Master of Business Administration (MBA) and Master of Engineering (MEng) degrees, XAMK has no identity management, and JAMK focuses less on legal aspects. XAMK and JAMK offer only Master of Engineering degree.

Table 66: Comparison of master's level offerings and workforce requirements by most prominent JRC categories

Universities Offerings	Workforce Requirements
Incident Handling and Digital Forensics	Software and Hardware Security Engineering
Software and Hardware Security Engineering	Incident Handling and Digital Forensics
Security Management and Governance	Network and Distributed Systems

Universities Offerings	**Workforce Requirements**
Security Measurements	Security Management and Governance
Network and Distributed Systems	Data Security and Privacy, or Assurance, Audit and Certification

Table 6 compares the JRC categories of the five highest master's level offerings of the universities with the five highest skill requirements in the workforce. The same categories are mainly represented on both lists, although there are some differences in priorities. The first two categories, Incident Handling and Digital Forensics, and Software and Hardware Security Engineering are the same. Still, workforce requirements emphasize Network and Distributed Systems, whereas universities offer more Security Management and Governance skills.

Security Measurements are included in the master's studies, but not as highly regarded in the workforce. Neither one of the fifth category of workforce requirements, Data Security and Privacy, or Assurance, Audit and Certification depending on which interpretation of the workforce studies is followed, is on the top offerings list. The offering of JAMK best covers both options, and JAMK also has all the other top workforce categories at the highest offering level. XAMK studies seem more technically focused, whereas TurkuAMK is more focused on the governance and human aspects.

6. Discussion

Among the 12 universities of applied sciences being studied, five bachelor-level degree programs focus on cybersecurity, including networking, programming, incident response, cryptology, and data security, which aligns well with professional skills requirements. Four universities have included cybersecurity-relevant topics in their curricula, but the achieved competency level is lower compared to the universities that focus on cybersecurity. Three universities have remarkably low levels of cybersecurity education, and the level of education is more on creating cybersecurity awareness than producing a professional cybersecurity skill set. However, it is not necessarily a burden if the cybersecurity awareness training is justified and planned accordingly.

The focus and coverage of master's studies differ from the bachelor level. The content overlaps with incident handling, networking, and programming, but more in-depth competency is gained for information security and governance. It is mentionable that master's studies in the Finnish universities of applied sciences are planned according to the Finnish dual-mode system where a student must have a suitable bachelor-level degree and two years of working experience at a minimum, making it possible to focus studies differently with lower study coverage. The model also makes it possible to get a cybersecurity degree without a previous one. In the big picture, the Finnish dual model produces graduates in the broad competency spectrum, and different focus areas are justified.

It should be noted that all studies in the bachelor's degree programs are not compulsory for students, and students typically have the freedom to select 15 to 30 CUs elective studies outside the curricula. However, despite the flexibility, five bachelor's degree programs offer a good professional skill set if a student plans studies accordingly. The master's studies have less flexibility, and the gained professional skill set reflects better curricula.

The future research topic could be to study all applied sciences universities in Finland with the presented study methodology. The presented method produces more granular results and more profound insights than previous studies. It could also be valuable to conduct such a study frequently, e.g., every five years, and follow how the universities are aligned with industry needs and current competency requirements.

Acknowledgements

This article has received funding partly from the Ministry of Education and Culture, Finland and partly from the European Union's Digital Europe Programme (DIGITAL) project "EAGLE -Digital Skills Training" under grant agreement No 101100660. Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

References

ACM Committee for Computing Education in Community Colleges (CCECC) (2023) *Bloom's for Computing: Enhancing Bloom's Revised Taxonomy with Verbs for Computing Disciplines.* New York, NY, USA: Association for Computing Machinery.

Gerring, J. (2006) *Case Study Research: Principles and Practices.* 1 edition. New York: Cambridge University Press.

Harris, M. and Patten, K. (2015) 'Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computing Curriculum'*, Journal of Information Systems Education*, 26(3), pp. 219–234.

HE 21/2001 vp. *Hallituksen esitys Eduskunnalle laiksi ammattikorkeakoulun jatkotutkinnon kokeilusta ja eräiksi siihen liittyviksi laeiksi*. Government of Finland.

ISACA (2023) *State of Cybersecurity 2023 Global Update on Workforce Efforts, Resources and Cyberoperations.* ISACA. Available at: https://www.isaca.org/resources/reports/state-of-cybersecurity-2023 (Accessed: 18.1.2025).

ISC2 (2023) *ISC2 CYBERSECURITY WORKFORCE STUDY How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce 2023.* ISC2. Available at: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e (Accessed: 18.1.2025).

Kämppi, P., Ekqvist, J. and Rajamäki, J. (2025) 'Competency Requirements for the Juniors in the Finnish Cybersecurity Service and Consultancy Business.' *Accepted to 20th International Conference on Cyber Warfare and Security 28th-29th March 2025, Williamsburg, Virginia, U.S.A.*

L 14.11.2014/932. *Ammattikorkeakoululaki*. Government of Finland.

Lehto, M. (ed.) (2022). 'Development Needs in Cybersecurity Education: Final report of the project.' *Informaatioteknologian tiedekunnan julkaisuja*.96. Jyväskylän yliopisto, Informaatioteknologian tiedekunta. URN:ISBN:978-951-39-9469-3.

Majanoja, A.-M., Ekqvist, J., Hakkala, A. and Virtanen, S. (2024) 'Kyberturvallisuuskoulutuksen kehittäminen Suomessa: yritysten osaamistarvekartoitus'. *Teknillisen tiedekunnan raportteja nro 2*. Turun yliopisto. URN:ISBN:978-951-29-9920-0.

Nai, F.I., Hernandez, R.J.L. and Neisse, R. (2021) *JRC Cybersecurity Taxonomy*. European Commission. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC125533 (Accessed: 19.1.2025).

NIST (2024) *NICE Framework: Current Versions*. NIST. Available at: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions (Accessed: 19.1.2025).

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

Ramsoonder, N.K., Kinnoo, S., Griffin, A.J., Valli, C. and Johnson, N.F. (2020) 'Optimizing Cyber Security Education: Implementation of Bloom's Taxonomy for future Cyber Security workforce', *in 2020 International Conference on Computational Science and Computational Intelligence (CSCI). 2020 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 93–98. DOI: 10.1109/CSCI51800.2020.00023.

Saharinen, K., Viinikanoja, J. and Huotari, J. (2022) 'Researching Graduated Cyber Security Students – Reflecting Employment and Job Responsibilities through NICE framework.' *21st European Conference on Cyber Warfare and Security, 16th - 17th June 2022, Chester, UK.* DOI: 10.34190/eccws.21.1.201.

Van Niekerk, J. and Von Solms, R. (2013) 'Using Bloom's Taxonomy for Information Security Education', in R.C. Dodge and L. Futcher (eds) *Information Assurance and Security Education and Training.* Berlin, Heidelberg: Springer, pp. 280–287. DOI: 10.1007/978-3-642-39377-8_33.

Vipunen. (2025). Education Statistics Finland. Ministry of Education and Culture. Available at: https://vipunen.fi/en-gb/polytechnic/Pages/Opiskelijat-ja-tutkinnot.aspx. (Accessed: 26.2.2025).

Yin, R.K. (2013) *Case Study Research: Design and Methods*. Fifth edition. Los Angeles: SAGE Publications, Inc.