JYU DISSERTATIONS 617

Karo Saharinen

Research into the Aspects of Cybersecurity Education in Higher Education

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY

JYU DISSERTATIONS 617

Karo Saharinen

Research into the Aspects of Cybersecurity Education in Higher Education

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi yliopiston Agora-rakennuksen auditoriossa 2
huhtikuun 18. päivänä 2023 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, auditorium 2, on April 18, 2023 at 12 o'clock noon.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2023

Editors
Marja-Leena Rantalainen
Faculty of Information Technology, University of Jyväskylä
Ville Korkiakangas
Open Science Centre, University of Jyväskylä

ISBN 978-951-39-9511-9 (PDF)
URN:ISBN:978-951-39-9511-9
ISSN 2489-9003

Permanent link to this publication: http://urn.fi/URN:ISBN:978-951-39-9511-9

ABSTRACT

Saharinen, Karo
Research into the Aspects of Cybersecurity Education in Higher Education
Jyväskylä: University of Jyväskylä, 2023, 77 p. (+included articles)
(JYU Dissertations
ISSN 2489-9003; **617**)
ISBN 978-951-39-9511-9 (PDF)

The importance of cybersecurity has increased due to the digitalization of society. In the last 10 years, the Finnish Cybersecurity Strategy has been released twice - in 2013 and 2019. The newest cybersecurity strategy states as its third chapter the development of cybersecurity competence within society. To amend the strategy, an implementation plan was released for the years 2017–2019, and a development program was released in 2021. The first theme of the development program is to ensure top class knowledge and development of cyber security education in Finland.

During this time period, several degree programmes concentrating on cybersecurity have been established in Finland. In vocational education, the basic degree in Information and Communication Technology has been updated to contain the maintenance of cybersecurity as an elective module. In addition, several other steps have been taken to increase the knowledge around cybersecurity nationally.

This study concentrates on researching cybersecurity education from different perspectives. The study was scoped into cybersecurity education within the higher education institutions. The goal was to find and establish solid fundamentals on which the competences, knowledge, and skills, could be based. Viewpoints on national cybersecurity education were also researched internationally by comparing cybersecurity degrees abroad through a unified analysis framework. The research also included theses done within these degree programmes as well as graduate employment. When vocational education was updated to include cybersecurity, the decision was made to research how the industry needed the competences developed there.

As a conclusion, the framework chosen within this research was deemed valid for curriculum development and as an analysis tool for several aspects of cybersecurity education. This research also verified what kind of education would be most beneficial for a student focusing on cybersecurity. The dissertation also provides data and researched viewpoints to curriculum developers on how and what to establish their competence structure in degree programmes focusing on cybersecurity.

Keywords: cybersecurity, cybersecurity education, pedagogy

TIIVISTELMÄ

Saharinen, Karo
Tutkimus kyberturvallisuuden koulutuksesta korkeakouluissa
Jyväskylä: University of Jyväskylä, 2023, 78 p. (+included articles)
(JYU Dissertations
ISSN 2489-9003; **617**)
ISBN 978-951-39-9511-9 (PDF)

Yhteiskunnan digitalisoituessa on kyberturvallisuuden tärkeys yhteiskunnassa noussut merkittävästi. Viimeisessä kymmenessä vuodessa Suomen kyberturvallisuusstrategia on julkaistu kahdesti; vuosina 2013 ja 2019. Uusimman kyberturvallisuusstrategian kolmantena kohtana on kyberturvallisuuden osaamisen kehittäminen yhteiskunnassa. Strategian täydennykseksi on julkaistu toimeenpano-ohjelma vuosille 2017–2019 ja viimeisimpänä kehittämisohjelma 2021. Kehittämisohjelmassa puolestaan ensimmäisenä kohtana on huippuluokan osaaminen ja toisena kohtana kyberturvallisuuden koulutuksen kehittäminen.

Tänä aikana on Suomen korkeakouluihin perustettu tutkinto-ohjelmia, jotka keskittyvät kyberturvallisuuteen. Ammatilliseen tieto ja- viestintätekniikan perustutkintoon on tullut kyberturvallisuuden ylläpitäminen valinnaiseksi tutkinnon osaksi. Näiden lisäksi on useita muita avauksia tehty kansakunnan kyberturvallisuuden tietotason nostamiseksi.

Tässä väitöksessä tutkitaan kyberturvallisuuden koulutusta eri näkökulmista. Tutkimuksen rajauksena oli korkeakouluissa toteutettava kyberturvallisuuden koulutus. Tutkimuksen tavoitteena oli löytää soveltuvat perusteet, johon kyberturvallisuuden tutkintokoulutuksen kompetenssit sekä kehitettävät tiedot ja taidot pohjataan. Vertailukohtia kansalliseen kyberturvallisuuskoulutukseen haettiin myös ulkomaalaisten tutkintokoulutusten sisällöistä vertailemalla niitä yhtenevällä viitekehyksellä Suomessa toteutettavaan koulutukseen. Tutkimuksessa läpikäytiin myös tutkinto-ohjelmista tehtäviä opinnäytetöitä, sekä valmistuneiden sijoittumista työelämään. Ammatillisen tason tutkinnonperusteiden päivityttyä sisältämään kyberturvallisuutta, päätettiin myös tutkia sen osaamiskuvauksien tarvetta teollisuudessa.

Johtopäätöksenä todettiin, että käytetty viitekehys osoittautui päteväksi tutkinto-ohjelman kehityksessä, ja analysoinnin työkaluna eri osa-alueisiin kyberturvallisuuden opetuksessa. Tutkimuksen perusteella voitiin vahvistaa mitkä osa-alueet kyberturvallisuuden opetuksesta olisivat opiskelijalle hyödyllisimpiä. Tämän tutkimuksen perusteella kyberturvallisuuden tutkinto-ohjelmia suunnittelevat henkilöt voivat paremmin pohjustaa miten ja kuinka perustaa tutkinto-ohjelmansa kompetenssirakenteen.

Avainsanat: kyberturvallisuus, kyberturvallisuuskoulutus, pedagogiikka

Author

Karo Saharinen
Faculty of Information Technology
University of Jyväskylä
Finland

Supervisor

Professor Timo Hämäläinen
Faculty of Information Technology
University of Jyväskylä
Finland

Reviewers

Professor Kirsi Helkala
Norwegian Defence Cyber Academy
Norwegian Defence University College
Norway

Reviewers

Docent Ijaz Ahmad
VTT Technical Research Centre of Finland Ltd
Finland

Opponent

Associate Professor Mikko-Jussi Laakso
Department of Computing
University of Turku
Finland

ACKNOWLEDGEMENTS

I would like to thank my supervisor Dr. Timo Hämäläinen. This dissertation and my postgraduate studies would not have been possible without his patience for over half a decade. I was not the easiest or most predictable to guide.

I would also like to thank my colleagues Dr. Mika Karjalainen and Dr. Tuomo Sipola, for the discussions we had in the finalization of this dissertation. I am also grateful to Ms. Tuula Kotikoski, as almost every research paper in this dissertation underwent an English language proofread by her. Most probably she will find multiple places to improve this text even after as this gets published.

As an addition to this, my professional development has also been heavily influenced by my colleagues at several different work places through out my career. Too numerous to write all of their names; however, I thank all of you for interesting conversations around the intricacies of worklife.

My gratitute goes to my fellow authors. I thank them for their collaboration with me during this endeavour. In the order of their appearance in the included articles: Mika Karjalainen, Tero Kokkonen, Jaakko Backlund, Jarmo Nevala, Simone Fischer-Hübner, Matthias Beckerle, Alberto Lluch Lafuente, Antonio Ruiz Martïnez, Antonio Skarmeta, Pierantonia Sterlini, Janne Jaurimaa, Sampo Kotikoski, Jani Päijänen, Jarno Salonen, Tuomo Sipola, Jan Vykopal, Anni Karinsalo, Jarmo Viinikanoja, Juoni Huotari, Joonatan Ovaska, Vesa Leino and Timo Hämäläinen.

Most of the included articles were formed either completely or partially through some kind of funding by my employer; Jamk University of Applied Sciences. This research would not have been possible without the projects and their goals occasionally aligning with my goals in this dissertation. Thus, I would like to recognize the financial support from the Research and Development programs; *Cyber Security Network of Competence Centres for Europe (CyberSec4Europe or CS4E) -project of the Horizon 2020 program* and *LIPPA - Quality to ICT Education from Industry and Education Collaboration from the European Social Fund*.

One of the greatest aspects in life is friends. I would like to thank all of them for their more than encouraging words to keep one's feet on the ground. It has been an excellent way to get realistic feedback in life.

This road would not be possible without the Finnish society built by the generations before me. Within the protection of my sister, parents and grandparents I have had the possibility to prosper in life. I am grateful to all of them and all other relatives of our whole family, cousins, uncles, aunts, stepmother, father-in-law, mother-in-law and so forth.

Finally, as I conclude my way through the Finnish Education System, I would like to express my deepest gratitute towards my wife Elina and our sweet daughters. Time spent on this research has been away from my family the most. Now that this project nears its conclusion, I hope to make it up to all of you.

Jyväskylä, 27th of March, 2023. Karo Saharinen.

LIST OF INCLUDED ARTICLES

PI Karo Saharinen, Mika Karjalainen and Tero Kokkonen. A Design Model for a Degree Programme in Cyber Security. *ICETC 2019: Proceedings of the 2019 11th International Conference on Education Technology and Computers (pp. 3-7)*, New York, NY, USA. DOI:https://doi.org/10.1145/3369255.3369266. URN: https://urn.fi/URN:NBN:fi-fe202002216171, 2019.

PII Karo Saharinen, Jaakko Backlund and Jarmo Nevala. Assessing Cyber Security Education through NICE Cybersecurity Workforce Framework. *ICETC 2020: Proceedings of the 12th International Conference on Education Technology and Computers (pp. 172-176)*, New York, NY, USA, 172–176. DOI:https://doi.org/10.1145/3436756.3437041. URN: https://urn.fi/URN:NBN:fi-fe2022030121335, 2020.

PIII Simone Fischer-Hübner, Matthias Beckerle, Alberto Lluch Lafuente, Antonio Ruiz Martínez, Karo Saharinen, Antonio Skarmeta and Pierantonia Sterlini. Quality Criteria for Cyber Security MOOCs. *13th IFIP WG 11.8 World Conference, WISE 13, Proceedings*, DOI:https://doi.org/10.1007/978-3-030-59291-2_4. URN: https://urn.fi/URN:NBN:fi-fe2022022420768, 2020.

PIV Janne Jaurimaa, Karo Saharinen and Sampo Kotikoski. Critical infrastructure protection - Employer expectations for cyber security education in Finland. *20th European Conference on Cyber Warfare and Security, 24th - 25th June 2021, Chester, UK.*, DOI:https://doi.org/10.34190/EWS.21.015 URN: https://urn.fi/URN:NBN:fi-fe2022022420763, 2020.

PV Jani Päijänen, Karo Saharinen, Jarno Salonen, Tuomo Sipola, Jan Vykopal and Tero Kokkonen. Cyber Range - Preparing for Crisis or Something Just for Technical People?. *20th European Conference on Cyber Warfare and Security, 24th - 25th June 2021, Chester, UK.*, DOI: 10.34190/EWS.21.012 URN: https://urn.fi/URN:NBN:fi-fe2021111956073, 2021.

PVI Anni Karinsalo, Karo Saharinen, Jani Päijänen and Jarno Salonen. Pedagogical and self-reflecting approach to improving the learning within a cyber exercise. *21th European Conference on Cyber Warfare and Security, 16th - 17th June 2022, Chester, UK.*, DOI:https://doi.org/10.34190/eccws.21.1.221, 2022.

PVII Karo Saharinen, Jarmo Viinikanoja and Jouni Huotari. Researching Graduated Cyber Security Students – Reflecting Employment and Job Responsibilities through NICE framework. *21th European Conference on Cyber Warfare and Security, 16th - 17th June 2022, Chester, UK.*, DOI:https://doi.org/10.34190/eccws.21.1.201, 2022.

PVIII Joonatan Ovaska, Karo Saharinen and Tuomo Sipola. Analysing Finnish Cybersecurity Thesis Topics Using Taxonomic Frameworks. *2022 IEEE International Conference on Cyber Science and Technology Congress (CyberSciTech)*, DOI: https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927808, 2022.

PIX Karo Saharinen, Vesa Leino, Tero Kokkonen, Tuomo Sipola and Timo Hämäläinen. Analysing Cybersecurity Education in Degree Programmes of Finnish Universities. *Journal of Information and Computer Security*, Submitted and Under Review URL: https://www.emeraldgrouppublishing.com/journal/ics, 2022.

PX Karo Saharinen, Tuomo Sipola and Tero Kokkonen. Development Needs in Cybersecurity Education - Final report of the project, Chapter 5. Cybersecurity Education In Universities of Applied Sciences. pp. 59-75.. *Informaatioteknologian tiedekunnan julkaisuja, 96/2022. University of Jyväskylä*, URN: http://urn.fi/URN:ISBN:978-951-39-9469-3, 2022.

LIST OF FIGURES

LIST OF TABLES

CONTENTS

1 INTRODUCTION

This research delves into the aspects of cybersecurity education: design principles of cybersecurity education through different competence and skill frameworks, course and platform improvement suggestions and requirements, examination of established degree programmes and investigations of students who have graduated from such degrees as well as employer expectations for graduates. The research mostly concentrates on higher education.

1.1 Research motivation

Cybersecurity education has been researched on a course- or assignment- specific level within a semester (Svábenský et al., 2020), from a technical learning environment perspective (Karjalainen, 2020) and from interviewing education personnel in universities on the state of cybersecurity education (Catota et al., 2019). Much time has also been devoted to researching the competences (e.g. knowledge areas or skills) required to work in cybersecurity (Rashid et al., 2018; Parekh et al., 2018). However, a multifaceted, in-depth research on current curricula situation, stakeholder expectations and results of such education have room for additional research.

The motivation for this research topic came in 2014 when the author of this dissertation was given the responsibility to design a cybersecurity specialization as part of the bachelor's degree programme of Information and Communications Technology at the Jamk University of Applied Sciences. The degree programme, and its associated course structure, was formed through collaboration with specialists in the field and began in 2015. The author was the acting degree proramme coordinator of the forementioned degree between 2015 and 2017. At the end of 2017–2018 semester, through reorganization of education at the university, the author received the responsibility of degree programme coordinator for the master of engineering programme in cybersecurity.

From these responsibilities, enthusiasm was sparked in the author to re-

search the development of curricula on cybersecurity. Much to the surprise of the author, the topic was rather fresh in the research field and guidelining frameworks were quite recently published. This was made more apparent by different funded projects, in the European Union (EU), with education-oriented work packages, which were running concurrently with the research conducted for this dissertation. Projects such as Cyber Security Network of Competence Centres for Europe (CyberSec4Europe)[1], Strategic Programs for Advanced Research and Technology in Europe (SPARTA)[2] and Cyber Security Competence for Research and Innovation (CONCORDIA)[3]. Moreover, similar undertakings were running in the United Kingdom under its National Cyber Security Programme and in the United States of America under its National Initiative for Cybersecurity Education -program[4].

1.2 Research questions

At the heart of this study was the need for a researched basis for the competences and learning objectives of an entire curriculum in cybersecurity at higher education institutions. A well-developed curriculum would serve all the stakeholders of such education: students, teachers and the industry. The student's perspective remained at the forefront of the research – to have a logical learning path from a bachelor's degree to a master's degree in cybersecurity. This objective ties in with the goal of the Ministry of Education and Culture (2017) to have the education provided by *Universities* and *Universities of Applied Sciences* be based on scientific knowledge.

Different established frameworks were evaluated and considered in laying the foundations of the competence structure of a degree. These frameworks would enable the establishment of goals in the form of skill and knowledge levels required to learn in order to pass the degree. These developed competences were also researched through the perspective of graduated students – which topics they were working on and what kind of responsibilities they were taking on after obtaining the degree.

Against this background, the following research questions were formulated:

RQ1. How should degree programmes utilize established frameworks and governmental guidance?

RQ1a. What competence foundations should cybersecurity education base on?

RQ1b. Which different categories of knowledge and skills should be emphasised on the degree?

[1] https://cybersec4europe.eu/
[2] https://www.sparta.eu/
[3] https://www.concordia-h2020.eu/
[4] https://www.nist.gov/itl/applied-cybersecurity/nice

RQ2. How does the industry need and graduates align with given education?

RQ3. How can the overall quality of courses that are part of a degree be enhanced?

To approach this phenomenon, different data acquisition perspectives were thought of and carefully selected to respect the data privacy of students under the data protection guidelines of university organizations. Ethical consideration was taken into account throughout the research as General Data Protection Regulation (GDPR) made data requests from universities a much more bureaucratic process than before (at least in the experience of the author).

1.3 Structure of the dissertation

This dissertation is sectioned in the following manner. The motivation of the researcher and the guiding research questions are presented in Section 1. The literature background for this dissertation is discussed in Section 2. This background is gone through education and its regulation and guidelines, cybersecurity and its definitions, and finally how the two come together in different frameworks, taxonomies and bodies of knowledge that are currently under development. Section 3 presents the research methodology, and how each of the papers in the study utilized the methodology.

Section 4 presents the most important parts of the papers included in the dissertation. It also states clearly the contributions of the author of this dissertation to each of the research papers. The section delves into how cybersecurity education has formed internationally and within Finland by analysing them with a unified cybersecurity framework. Education of cybersecurity is also researched from the viewpoint of stakeholders of such education – the industry and graduated students. Improvement suggestions through cybersecurity MOOC quality criteria proposal, cyber range usage and course improvement. Finally, Section 5 draws up the conclusions of the research, its limitations and ideas on how the phenomenon could be researched in the future.

2 BACKGROUND OF THE RESEARCH

2.1 Education

Finland's high scores in the Programme for International Student Assessment (PISA) has deemed it a 'success'. It is researched even within Finland to understand the phenomena behind it and their implications going forward (Välijärvi et al., 2002; Simola et al., 2017; Ahonen, 2021). Reseachers from other countries are also attempting to understand and learn lessons from it (Üstün and Eryilmaz, 2018; Altaf et al., 2020). Critical research has been conducted to compare the scores of Finland to those of other countries and to better make sense of the results (Soh, 2014; Mikk, 2015; McIntosh, 2019). Nonetheless, Finland takes pride in its achievements in the field of education; calling it a national success story (Ministry of Education and Culture, 2017).

As with other countries, the Finnish education system has had to reform and align, as mandated by regulation from the EU, with the European Qualifications Framework (EQF). This alignment is done through the national qualification frameworks (NQF), which describe how national education systems align to the eight-level framework of the EQF (Council of the European Union, 2017; The Finnish National Agency for Education and Ministry of Education and Culture, 2018). These are depicted in Table 1. The main focus of this research is on EQF levels four, six, and seven.

Definitions of terminology in education within the EU can be acquired from, for example, the publishment of the European Council (2017). There is a strong interweaving of terms such as *learning outcomes*, *competence*, *knowledge* and *skills*. This used terminology can be found quite contradicting to read when comparing multiple different frameworks produced from different continents and countries. Even the definition of *competence* is debatable on its exact meaning (Schneider, 2019).

TABLE 1 Education levels within the European Qualifications Framework

EQF	**Degree**[1]
Level 1	Basic Education
Level 2	Basic Education
Level 3	Basic Education
Level 4	Matriculation and Vocational qualifications
Level 5	Specialist vocational qualifications
Level 6	Bachelor's Degree
Level 7	Master's Degree
Level 8	Licentiate and Doctoral Degrees

[1] Slight generalisation made by the author and not an all encompassing list

The European Credit Transfer System (ECTS) is built to have transparency in higher education and identical credits awarded for completion of courses in the European Higher Education Area (EHEA). This helps in creating student mobility in exchange programs. The ECTS not only bases itself on the workload and learning outcomes of the student, but also on the design, description and delivery of a degree programme. The ECTS Users' Guide (European Commission, 2017) recommends the publishing of a course catalogue of the degree programmes and this catalogue should at least provide the following sections: *general information*, *resources and services*, *information on programmes* and *information on individual educational components*. These sections form a data structure of which many of the data collecting of curricula within this dissertation bases on. However, the guide does not mandate the format of the data published on the webpages; it only recommends that they should be published.

The *Information of the Programmes* section of the guide mentions a *field(s) of study* that should be published by the programmes. It is recommended that these fields be based on the International Standard Classification of Education (UNESCO Institute for Statistics, 2015). The standardized fields are also the basis for Statistics of Finland to provide information to the Ministry of Education and Culture on how the education sector is performing. Within these fields, the field of *Information and Communications Technology* is relevant for this study as most of the Finnish cybersecurity education has been concentrated in that field.

Given this background on the education structure in EU and Finland, the resultant education structure and this research context are illustrated in Figure 1.

During the lifespan of this research, the Finnish government decided to extend the period of compulsory education in Finland through regulation (Finnish Government, 2020). This was combined with the renewal of qualification requirements for vocational education, particularly in the ICT field with a study unit on 'Maintaining Cybersecurity' (Finnish National Agency for Education, 2021). Through this renewed curriculum, the vocational school became also became of interest for this dissertation.

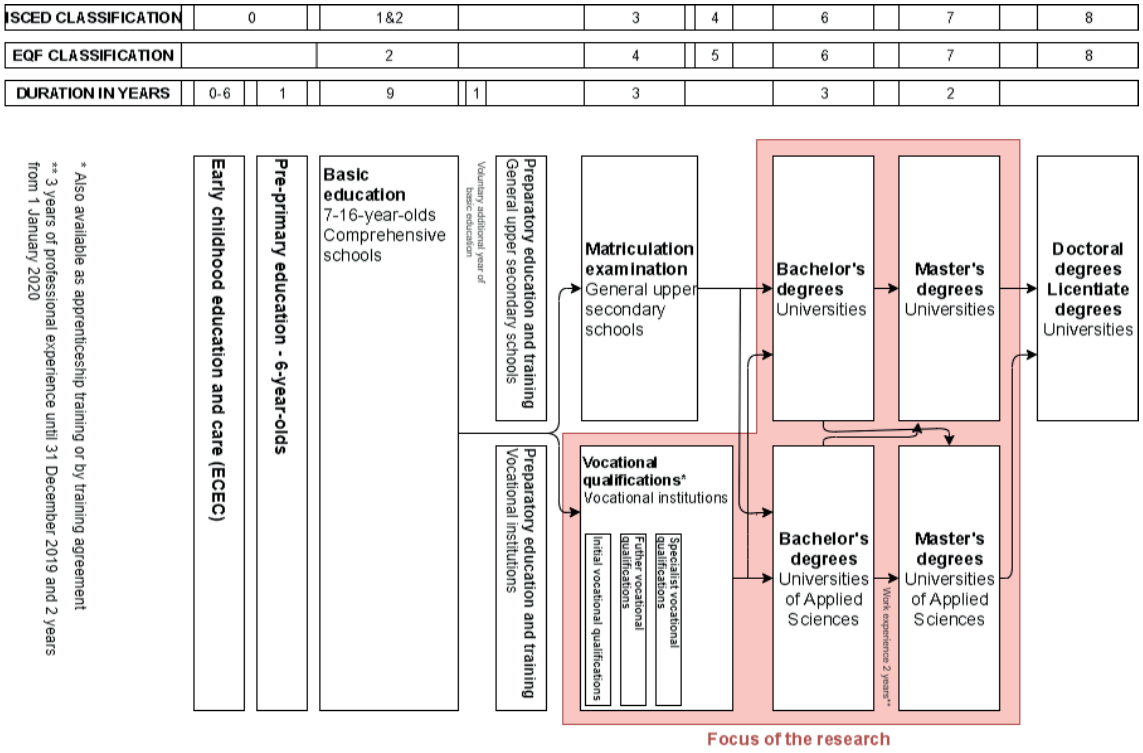


FIGURE 1 The Finnish education system and the present research context

As depicted in Figure 1, the Finnish higher education is divided into two organizations: *Universities of Applied Sciences* and *Universities*. Table 2 represents the complete list of universities that were researched as part of this dissertation. The following universities dedicated to social work, arts or business were excluded: *Diaconia University of Applied Sciences*, *Humak University of Applied Sciences*, *Hanken School of Economics* and *University of the Arts Helsinki*.

The Minister of Education and Culture declared the addition of 2300 study places within the higher education of Finland at the end of 2021 (Ministry of Education and Culture, 2021b). In both higher education institutions of Finland (Universities and Universities of Applied Sciences), these study places were distributed to different fields of education (Ministry of Education and Culture, 2021a,c). However, these study places were not directly added to cybersecurity education, but generally to the field of ICT. This addition follows the workgroup proposal for Higher Education and Research Vision 2030 (Ministry of Education and Culture, 2017) and the current Government Programme of Finland (Finnish Government, 2019) – to increase the education level of Finnish citizens to have at least 50 % of the population obtain a bachelor's degree level education.

Through governmental governance the Ministry of Education and Culture provides guidelines and goals to Finnish higher education institutions by establishing agreements between them on an individual per institution level[1]. These public agreements are generally available on the webpages of the ministry and are valid from 2021–2024.

[1] https://okm.fi/en/steering-financing-and-agreements

TABLE 2 Universities in Finland

Universities	Universities of Applied Sciences
Aalto University	Arcada University of Applied Sciences
University of Helsinki	Centria University of Applied Sciences
University of Eastern Finland	Diaconia University of Applied Sciences
University of Jyväskylä	Haaga-Helia University of Applied Sciences
University of Lapland	Humak University of Applied Sciences
LUT University	Häme University of Applied Sciences
University of Oulu	Jamk University of Applied Sciences
Hanken School of Economics	South-Eastern Finland University of Applied Sciences
University of the Arts Helsinki	Kajaani University of Applied Sciences
Tampere University	Karelia University of Applied Sciences
University of Turku	LAB University of Applied Sciences
University of Vaasa	Lapland University of Applied Sciences
Åbo Akademi University	Laurea University of Applied Sciences
National Defence University	Metropolia University of Applied Sciences
	Oulu University of Applied Sciences
	Satakunta University of Applied Sciences
	Savonia University of Applied Sciences
	Seinäjoki University of Applied Sciences
	Tampere University of Applied Sciences
	Turku University of Applied Sciences
	Vaasa University of Applied Sciences
	Novia University of Applied Sciences
	Åland University of Applied Sciences
	Police University College

The agreements have the following set structure:

- Strategic goals, choices and profiles
- Core areas and newly emerging scientific fields
- Degree objectives (or completed degree goals)
- Following of results and funding

While researching all the agreements, cybersecurity was found in only one agreement of the University of Applied Sciences, but none in the other agreements between the Ministry and Universities of Finland. However, this does not imply a neglect of cybersecurity education in the Universities. It merely implies that it has not risen as a major field of study next to other fields of education, research and development.

2.2 Cybersecurity

Kavak et al. (2021) state that there is a challenge to find a consensus on the definition of cybersecurity because of its dynamic nature. There are multiple mod-

els, phrases and taxonomies that attempt to explain cybersecurity (ENISA, 2016; ACM and IEEE-CS, 2020).

The International Telecommunication Union (ITU) has a phrase that aims at the protection of the cyber environment through any collection of means, tools, policies and actions (ITU-T, 2008). One could understand the previously mentioned cyber environment to be the same as the one mentioned in the Finnish Cyber Security Strategy as 'cyber domain' (Secretariat of the Security Committee, 2013). The International Organization for Standardization (ISO) has published ISO 27000 which has the closest definition to cybersecurity in the term *information security* and it is explained through the usage of the *confidentiality, integrity and availability* triad (ISO, 2018). European Telecommunications Standards Institute (ETSI) formed a technical committee which covers a set of domains under the terms *horizontal cybersecurity*, *security technologies and systems* and *security tools and techniques*'[2].

Nevertheless, the common element within the definitions is that cybersecurity is considered to be a highly interdisciplinary field (Jacob et al., 2020). The digitalization of every aspect of humanity is increasingly bringing cybersecurity to the surface in any lifecycle stage of the human lifespan (Jones et al., 2019). Managing this interdisciplinary and widespread situation has become one of the top priorities of private and public organizations (Lehto and Limnéll, 2021).

With the current global political tensions, cybersecurity is said to be amidst a cyber arms race (Limnéll, 2016; Craig and Valeriano, 2016). The different actors within the cyber domain are actively developing; educated personnel, technical advantages and operational capabilities (Rantapelkonen and Salminen, 2013; Kuusisto, 2014). The laws and regulations are attempting to keep up to have control over this escalating situation. However, the situation is considered to be highly political and different 'like-minded states' are developing regional agreements (Henriksen, 2019).

In Finland, this has resulted in securing the cyber domain in every different sector of the government (Lehto et al., 2018). Finland's Cyber Security Developement Programme has, as its first chapter, the goal to develop world-class competence and directing enough resources for the education of cybersecurity (Paananen, 2021). This is not a new requirement as the Finnish Cyber Security Strategy has had similar demands since 2013; cybersecurity education should be established and implemented on all levels of education in Finland (Secretariat of the Security Committee, 2013). In the 2019 version of the cybersecurity strategy the statement is made more precise with the following quote:

> Training programmes related to cyber and information security, software and application development, information networks and telecommunications in vocational education, universities of applied sciences and universities will be strengthened. (Secretariat of the Security Committee, 2019)

There are efforts to establish key topic areas and curricular guidelines for cybersecurity similarly as mathematics, physics, chemistry and biology have (Rashid et

[2] https://www.etsi.org/committee/cyber

al., 2018). However, as revealed in the following chapter on various frameworks, one could conclude that there exists a rather fragmented vision of cybersecurity education. A phenomenon quite similar to the definition of cybersecurity.

2.3 Cybersecurity education and frameworks

In their book, Bloom et al. (1956) introduced a taxonomy of six categories which help, for example, curriculum designers to focus on their learning objectives, plan teaching and prepare evaluation methods to support the before mentioned. These six categories of the **Bloom's taxonomy** were as follows: *knowledge*, *comprehension*, *application*, *analysis*, *synthesis* and *evaluation*. These categories could be utilized in a different order than the one introduced by the book; however, the curricula designers often rely to it in one form or another. The taxonomy itself was revised by Anderson et al. (2001) to emphasise focus more on curriculum planning, instruction and assessment and all combinations of the before mentioned. Thus, they introduced the following revised categories (or cognetive processes): *remember*, *understand*, *apply*, *analyze*, *evaluate* and *create*. Different universities have taken these revised categories broadly into use (Rahman et al., 2018; Sobral, 2021).

European Network for Accreditation of Engineering Education (ENAEE) is a not-for-profit organization that promotes the accreditation of engineering education within Europe through the use of EUR-ACE® framework. The EUR-ACE® label is a certificate granted by an authorized agency to an accredited degree programme within a higher education institution. In Finland, such an authorized agency is the Finnish Education Evaluation Center (Finnish: Kansallinen koulutuksen arviointikeskus - KARVI)[3].

The **EUR-ACE Framework Standards and Guidelines** (ENAEE, 2021) list multiple aspects that an evaluated programme should abide by. For this dissertation the main section is learning area descriptors that should be in close alignment with the EUR-ACE® descriptors: *knowledge and understanding*, *engineering analysis*, *engineering design*, *investigations*, *engineering practice*, *making judgements*, *communication and team-working* and *lifelong learning*. The framework provides more specific details on each of the descriptors at both the bachelor's degree and the master's degree levels.

In the field of computers, the **ACM Computing Curricula** encompasses different paradigms for the global education of computing at the undergraduate level (ACM and IEEE-CS, 2020). These programs can be seen in the University offering in Finland with rough translations presented in Table 3.

[3] https://karvi.fi/en/

TABLE 3 ACM Paradigms and their estimated Finnish translation

ACM Paradigm	In Finnish
Computer Engineering	Tietokonetekniikka
Computer Science	Tietojenkäsittelytiede
Cybersecurity	Kyberturvallisuus
Information Systems	Tietojärjestelmätiede
Information Technology	Informaatioteknologia tai tietotekniikka
Software Engineering	Ohjelmistotuotanto
(Data Science)[1]	(Data-analytiikka)

[1] (Under development) as stated by the CC2020

These different paradigms can be seen in the Finnish University system as organizational units (e.g. departments), names of degree programmes, or specialization studies. Table 4 presents examples. The degree programmes are of varying levels, either bachelor's degrees or master's degrees and are often a mix of the paradigms. From the author's perspective, there is little researched or public knowledge on how ACM curricula guidelines are being taken into account in Finnish education.

TABLE 4 Different paradigms in use in Finnish higher education

ACM Paradigm	University of Applied Science	University
Computer Engineering	Degree Programme in Electronics, Metropolia[3]	Digitalization, Computing and Electronics, Oulun Yliopisto[4]
Computer Science	-	Department of Computer Science, HY[1]
Cybersecurity	Degree programme in Business Information Technology, Cyber Security[2]	Kyberturvallisuuden maisteriohjelma[9]
Information Systems	Tietojärjestelmäosaamisen ylempi tutkinto-ohjelma, TAMK[8]	Tietojärjestelmätieteen kandidaatti- ja maisteriopinnot, JYU[7]
Information Technology	Institute of Information Technology, Jamk[13]	Faculty of Information Technology, JYU[11]
Software Engineering	Bachelor's Degree Programme in Software Engineering, TAMK[10]	Software Engineering Research Area/Group, LUT University[12]
(Data Science)	Dataosaamisen ja tekoälyn ylempi tutkinto-ohjelma, TAMK[5]	Data-analytiikka päätöksenteossa, LUT[6]

[1] https://opas.peppi.utu.fi/fi/perustutkintokoulutus/teknillinen-tiedekunta/14002/33054
[2] https://ops.laurea.fi/212701/en/69076/230740/2521
[3] https://opinto-opas.metropolia.fi/en/88094/en/70329/TXD22S1/year/2022
[4] https://www.oulu.fi/fi/hae/kandidaattiohjelmat/elektroniikka-ja-tietoliikennetekniikka
[5] https://www.tuni.fi/fi/tule-opiskelemaan/dataosaamisen-ja-tekoalyn-ylempi-tutkinto-ohjelma-insinoori-ylempi-amk
[6] https://www.lut.fi/fi/opiskelu/tekniikka/data-analytiikka-paatoksenteossa-maisteriohjelma
[7] https://www.jyu.fi/it/fi/opiskelu/kandidaatti-ja-maisteriohjelmat/tietojarjestelmatiede
[8] https://www.tuni.fi/fi/tule-opiskelemaan/tietojarjestelmaosaamisen-ylempi-tutkinto-ohjelma
[9] https://www.jyu.fi/it/fi/opiskelu/maisteriohjelmat/kyberturvallisuus
[10] https://opinto-opas-ops.tamk.fi/index.php/fi/167/fi/169887
[11] https://www.jyu.fi/it/en/faculty
[12] https://www.lut.fi/fi/tutkimusryhmat/software-engineering
[13] https://www.jamk.fi/en/apply-to-jamk/ict

Cybersecurity was introduced as a paradigm of computing before the release of the ACM Curricula Guidelines 2020. The ACM Education Board noticed the urgent need for cybersecurity education to fill the sudden requirement

for a cybersecurity workforce, as recognized by both governmental and non-governmental sources. This introduction was earlier published as **Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity** known as JSEC2017 (ACM, IEEE-CS, AIS SIGSEC and IFIP, 2017).

Parallel to ACM's work the **Workforce Framework for Cybersecurity** (or **NICE Framework**) was released by Newhouse et al. (2017) in version 1.0. The update of the framework was released by Petersen et al. (2020). The background of the framework was done throughout a decade of development[4] and corresponding scientific publishments that supported its development such as Jones et al. (2018) and Armstrong et al. (2020).

NICE framework approaches the field through *Work Roles* present in the field. These *Work Roles* are subjugated to *Specialty Areas* which reside under *Categories* of Cybersecurity. This hierarchy is represented in Figure 2.

FIGURE 2 One way of visualizing the hierarchy in the NICE framework

[4] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/history

One can use which level of the hierarchy as one pleases; however, some of them were deprecated in the first revision of the framework to improve the agility of the framework. This deprecation feels like a step backwards by the author of this dissertation. Thus, these levels of hierarchy were used before the updated framework revision and their usage was continued after the updated revision to facilitate a backwards comparability for the research. The same phenomenon is evident on different websites provided to enhance the usage of the NICE framework[5]. The most used hierarchy level within this dissertation are the workforce *categories*. These are described in Table 5.

TABLE 5 NICE framework categories as presented in the framework (Newhouse et al., 2017)

Workforce category	**Description**
Securely Provision (SP)	Conceptualizes, designs, procures and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyses, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information.

There is little discussion of how companies organize their business within the framework. Different companies might have multiple categories present in their organizational structure, or they might specialize in only one category section. There is little research in Finland on how organizations align from the aspects of this framework. Figure 3 shows how categories are dissected to speciality areas and work roles. The work roles are assigned tasks which require knowledge, skills and abilities.

[5] https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

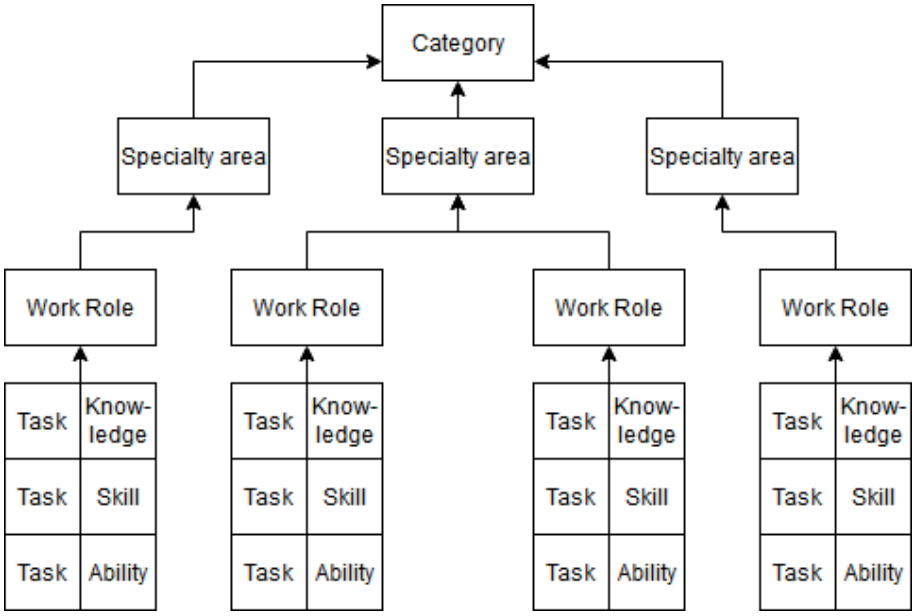


FIGURE 3 Work roles and categories build upon knowledge and skills

Moreover, an aspect to be aware of is that this framework is not exactly education-oriented. However, the *Knowledge* and *Skills* required within each *Work Role* could be usable from the viewpoint of an education facilitator. These acquired *Knowledge* and *Skills* are needed to perform *Tasks* that are assigned to each *Work Role* within the framework. One could draw a line between these to imply a *Competence* necessary for such work as described by the European Council (2017). Figure 4 presents one way of dissecting the NICE framework for teaching goals.

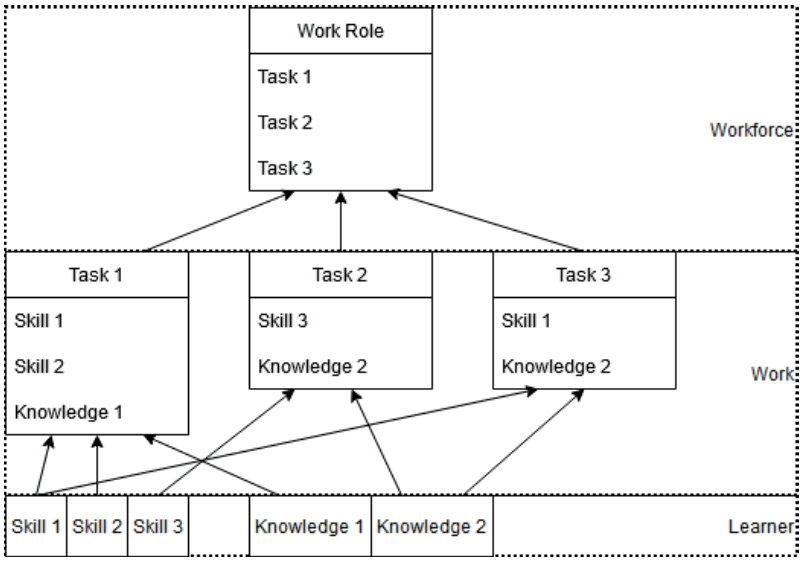


FIGURE 4 One way to dissect the NICE framework

From among the EU funded projects, SPARTA in particular published a deliverable of the project called **Cybersecurity Skills Framework** written by Hajný et al. (2020). Within the report was a section of preliminary work conducted to

establish skills needed in the cybersecurity field. One of the referenced works was the NICE framework (note: this was without revision 1 changes) and along side it was other approaches like Nai Fovino et al. (2018) which later was published as **A Proposal for an European Cybersecurity Taxonomy** (Nai Fovino et al., 2019). The work done within SPARTA's deliverable was to utilize the aforementioned frameworks to map out a preliminary European Cybersecurity Skills Framework. However, in their conclusion chapter, they mention, *'an exhaustive list is still left to be completed'* (see Hajný et al., 2020, 61). This preliminary work resulted in an ad-hoc workgroup being established in 2020 under The European Union Agency for Cybersecurity (ENISA), which began work in 2021[6].

Furthermore, the publication also discusses the varied definition of cybersecurity by examining multiple different literature sources and attempting to combine a set and clear taxonomy definition to be used within the European Union. The conclusion of the paper emphasises the complexity of the discipline. Their solution was to implement a three-dimensional taxonomy based on *research domains*, *sectors* and *technologies and use cases* (see Nai Fovino et al., 2019, Figure 5). Within this research, the *sectors* which utilize cybersecurity are used as an analysis framework in the research papers. This dissertation would fall under the research domain of education and training of said framework.

To highlight the parallel production of cybersecurity frameworks, the **Cyber Security Body of Knowledge** (CyBOK) project had initiated in the United Kingdom 'to provide a foundation for the development of the cyber security profession' (National Cyber Security Centre, 2020). This project published their model in January 2020 with an aim to have CyBOK in use nationally for undergraduate and postgraduate degrees. The framework uses the term *knowledge areas* that are bound to five broad categories. These are not utilized in the research within this dissertation; however, the publishment of the new framework underlines the undergoing development within the field of cybersecurity education.

6 https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls

3 RESEARCH METHODS AND DATA

3.1 Research approach

Given the number of articles, each of the research cases had their own steps of usage of scientific methods: identification of a problem and research topic, conceptual background study, research design and methodology, data collection, data analysis to finally research results in interpretation of results and possible conclusions based on researched results (Bilgin, 2017).

The personal preference of the author, maybe because of an engineering background, was to use quantitative research methods as much as possible to obtain more comparable data of education. However, throughout the process it became evident to the author that one should not have such a rigid stance on research methodology. Rather, one should have the two complement one another and think of them as the opposite ends of a wide spectrum of research (Creswell, 2013).

Thus, as the research progressed, it was evident that to produce quantitative data sets, the decisions made in quantifying the data were qualitative in nature. This indicates that with the same data sets, different researchers can have slightly different outcomes. However, the main results would most probably be the same even if small changes of categorization might occur.

3.1.1 Quantitative analysis

Within this dissertation articles, quantitative methods were used to collect statistics on education to obtain comparable data through the measurement of numbers, percentages and average values. These measurements were used to visualize the different levels of emphasis on different research topics. Often, to reach this viewpoint of the results, the usage of a unified analysis framework needed to be in place. If the results had been analysed with several frameworks, the amount of work for each article would have grown out of proportion. However, the author would like to emphasise that other frameworks can be used for the analysis

of the same data sets.

Articles II, IV, V, VII, VIII, IX, and X used quantitative methods to research and compare teaching subjects of the curricula from multiple different perspectives. The inclusion of a chosen framework for analysis made the results possible for comparison within this dissertation.

3.1.2 Qualitative aspects

To categorize words into numbers, the subjectivity of the categorization needs to be in place. Efficient ways of categorization through attributes such as word names and spelling needed to be developed and used to have an efficient means of understanding the data. For example, this implied, that words like programming (Finnish: ohjelmointi) or coding (Finnish: ohjelmoida) in course names needed to be categorized under the same topic, and the ECTS used for the course would count towards its framework category (such as Securely Provision). Several listed articles in this disseratation had such cases at hand, and these are discussed in the data analysis section of each article.

The dissertation and the included articles still are missing an interview based study, be it narrative research or phenomenological research or any other kind of sociological study on the stakeholders of cybersecurity education (Creswell, 2013). Thus, one would not say that this dissertation builds upon a mixed method research.

3.1.3 Constructive research approach

A constructive research approach was utilized to solve certain problems within cybersecurity education – for example, course, curriculum or education environment. This methodology bases the proposed solution on theory through literature reviews and possibly expert opinions to establish an understanding of the researched topic. After this phase, the constructs are designed and tested to evaluate their applicability to solve the stated problem (Koskinen et al., 2011; Lehtiranta et al., 2015). In this dissertation, Articles I, III, and VI utilized the methodology of constructive research approach. These articles cover and propose improvements on different aspects of cybersecurity education.

3.2 Data Collection

Given the article background of this research, an understanding of necessary cybersecurity education and ways to improve it was obtained. Table 6 presents the articles and the research methods employed for each individual article.

TABLE 6 Methodology for data collection and article contributions to this dissertation

Article	Methods	Research aim
I	Constructive research	Curricula requirements structure from regulation, accreditation and cybersecurity framework viewpoints
II	Quantitative methods	Collected quantitative data set on cybersecurity curricula structures taught outside of Finland and their analysis
III	Constructive research	A model of requirements for cybersecurity education MOOCs collected and proposed from theoretical background research
IV	Quantitative methods	Quantitative methodology to understand the need for cybersecurity education in the regional industry. Main focus on vocational education and bachelor's degree education.
V	Quantitative methods	Survey research on the usage of cyber ranges in organizations.
VI	Constructive research	Proposal for a pre-emptive questionnaire to prepare participants for learning in a cyber range.
VII	Quantitative methods	Survey for cybersecurity bachelor's degree graduates on employment sectors and responsibilities.
VIII	Quantitative methods	Analysis of cybersecurity theses conducted regionally in Central-Finland.
IX	Quantitative methods	Framework based analysis of curricula in Finnish universities. Cybersecurity education alignment and emphasis through framework categories.
X	Quantitative methods	Research on Universities of Applied Sciences in Finland. Amount of cybersecurity specific curricula, number of students and possible workforce estimates.

4 RESEARCH CONTRIBUTION

4.1 Overview of the articles

Articles gathered in this dissertation were written through collaborations with multiple different researchers in several projects and work packages of such projects. Scientific publishing is a task that one could call a tedious and time-consuming process (Derntl, 2014); however, through the articles, the insight of the author also grew into the art of scientific research and publishing. Thus, research settings in the latter articles, in the subjective opinion of the author, have a more clear scope and focus.

Article I was written around an idea which was generated by the author. Fellow colleagues encouraged, further developed the idea, and supported the writing of the article. The idea had a background in a recent accreditation by the National Education Evaluation Centre[1] towards the bachelor's degree programme in Information and Communications Technology at Jamk University of Applied Sciences. Through discussions within the accreditation process, it became evident that some backgrounds were lacking in the course descriptions related to courses focused on cybersecurity. Thus, the work behind the article was done to fuse different frameworks within the curricula to clarify the subjects being taught within the curriculum. The author was the first writer of the article.

Article II gained momentum during the writing of the previous article. Where the first article focused on the work done within the curricula, the author became interested in how cybersecurity education was taught internationally. The research idea and analysis methods were predetermined by the author of this dissertation who acted as the second writer of the article. Data collection and processing was done by the first author of the article.

Article III was a collaboration within Cyber Security for Europe project to

[1] https://karvi.fi/

which the author of this dissertation got invited. An aim of the project was the requirement specification for cybersecurity education given in massive open online courses (MOOCs). The proposed quality criteria presented in Article III was conceived by reviewing existing structures and having a reseaerch background on the subject. The author of this dissertation acted as a contributor to the written text on cybersecurity MOOCs utilizing cyber ranges. The author also commented and acted as a reviewer of the proposed quality criteria and the paper as a whole and was accredited as the fifth author.

Article IV emerged from an idea of the author to obtain insight into the regional demand for cybersecurity education. Simultaneously, there was also a the reform underway in ICT education within the vocational education of Finland. Thus, it was interesting to see if this newly created competence module within vocational education had any attraction within the industry of Finland. Moreover, the necessity (or demand) of cybersecurity modules offered as part of the bachelor's degree of Jamk University of Applied Sciences was also included in the scope of the research. The author of this dissertation had predetermined the frameworks utilized for data analysis and actively collaborated with the first author in conceiving the results of the research. This author acted as the second author of the publication.

Article V emerged during the ongoing research on cybersecurity education utilizing cyber ranges. The use cases and target groups active within the field were of interest. The research was conducted during the Cyber Security for Europe project to collect information on how cyber ranges are utilized within the European Union. The author contributed in the research theory and verification of data analysis and results. The author was the second author of the publication.

Article VI continued along the same path with the fifth article. However, in the sixth article, the perspective of incoming participants was in focus. A questionnaire was created for the upcoming flagship cyber exercise to understand the participants and their background better and to obtain their input on the practicalities within the exercise. This questionnaire could help the educators in the exercise to understand their learners better. The author contributed in writing the educational framework theory to support the questionnaire on which much of the questions relied upon. The author acted as the second writer of the publication.

Article VII adopted a hindsight approach to the stakeholders of the curriculum – the alumni students. The research focused on their job responsibilities and placement within the industry after their graduation. This was relevant when focusing on serving the employment rate of the students through curriculum offerings. The author had the main idea and acted as the first author establishing the research scope, research methodology, and delving into the results. The author wrote the publication on the research as the main writer.

Article VIII was focused on collecting cyber security theses conducted in bachelor's and master's degree regionally in Central Finland. Quantitative analysis was performed to understand where and what kind of theses were written on a larger scale. Moreover, industry and subject analyses were performed through a cybersecurity framework to obtain a statistical understanding of the phenomenon. The author acted as the second author of the publication.

Article IX was based on the curricula of Finnish higher education published between 2018 and 2021. Quantitative analysis was performed on the degree course offerings to understand the cybersecurity category emphasis of the degree education in Finland. The author came up with the research idea, data analysis methodology, and acted as the first author of the article.

Article X involved the author collaborating with a group of people under the order of the Finnish Transport and Communications Agency to obtain a view of the entire cybersecurity education in Finland – from private organizations to public organizations. The author had the responsibility of investigating the current curricula of the Universities of Applied Sciences and was the main author of that section of the report. The report was published during the summer of 2022.

4.2 Cybersecurity Curricula Research (Articles II, IX, and X)

4.2.1 International Curricula Research

Given the increase in the offering of cybersecurity education globally (Parrish et al., 2018), one of the first research papers within this dissertation was aimed at obtaining an idea of what is currently being taught as part of cybersecurity curricula. The research included degrees associated with cybersecurity (or similar) in the degree title and the curricula available in English. Through this setting, 69 degree programmes were investigated with over 2000 different courses; 36 degrees from the United States out of which 21 were graduate programs (master's degrees) and 15 were undergraduate programs (bachelor's degrees). From the European Union, 33 degree programmes were investigated, with 19 master's degrees and 14 bachelor's degrees.

The NICE framework was selected as the analysis method for curricula content as it was the most viable framework at the time when the research was conducted. This analysis method provided a standardized method to compare the different degree programmes on what topics they were focusing on educating. As further analysed in Article II, global education is rather difficult to compare, as different nations have different durations for completion of degrees and degree titles awarded. However, a consensus was derived from the data to visualize the education between different ranges of ECTS scopes. Figure 5 presents an average ECTS distribution within the NICE framework categories in singular bachelor's degrees.

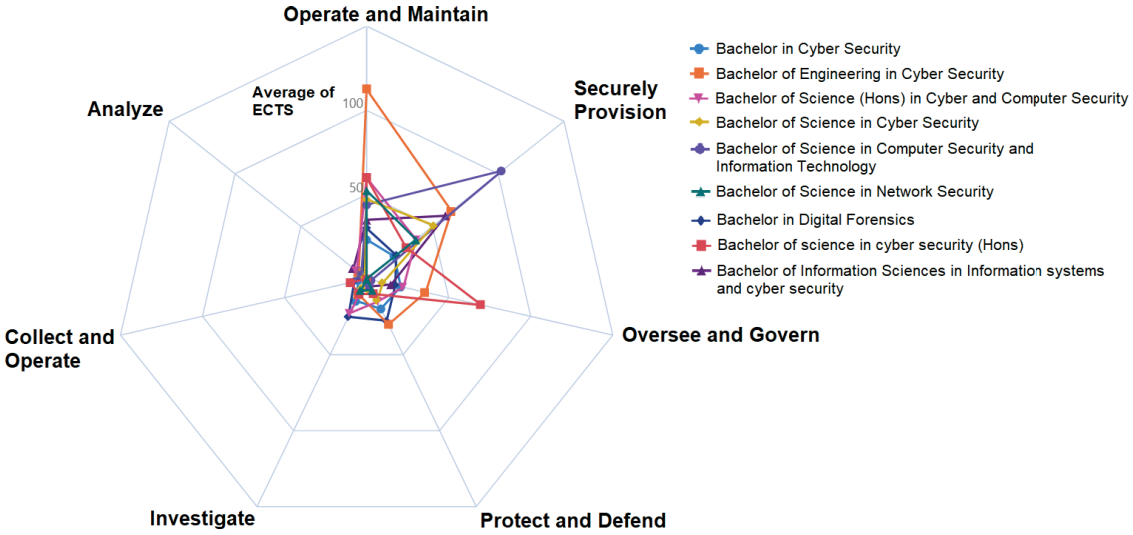


FIGURE 5 NICE framework category weights in singular bachelor's degrees

The differences between degree focuses are rather apparent. The figure above provides an erratic view of how those categories are generally weighted. Thus, from the data, a combined view of the average weights of different curricula within the ECTS duration of 168–210 was collected. This is depicted in Figure 6.

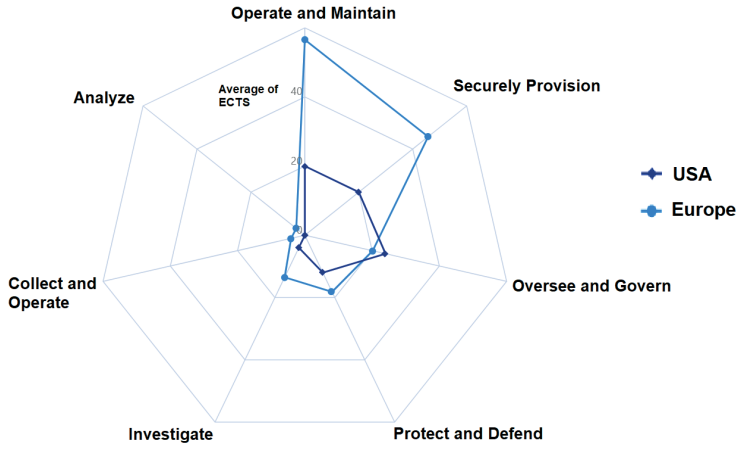


FIGURE 6 NICE framework category weights on average per continent

Through the data and the visualization, it is rather apparent that in the United States and in Europe, the duration of the bachelor's degree programmes are quite different. However, the alignment of the categories follows a similar path with most of the studies falling under the *Operate and Maintain* category. With regard to the second most weighted, the categories *Securely Provision* and *Oversee and Govern* switch places between the continents. The remainder of the categories align in a similar manner.

The other degree durations and their visualizations are made more apparent in Article II. All the visualizations are presented in a unified table for better analysis and diffusion of results regarding this dissertation. Table 7 shows how different categories were weighed in different curricula durations.

TABLE 7 Research results in Article II

Degree length (ECTS)	**1st**	**2nd**	**3rd**	**4th**	**5th**	**6th**	**7th**
USA							
Bachelor's degrees (168 to 210)	Operate and Maintain	Oversee and Govern	Securely Provision	Protect and Defend	Investigate	Collect and operate	Analyze
Bachelor's degrees (240 to 252)	Operate and Maintain	Securely Provision	Oversee and Govern	Investigate	Protect and Defend	Collect and Operate	Analyze
Master's degrees (60 to 90)	Operate and Maintain	Oversee and Govern	Securely Provision	Investigate	Protect and Defend	Analyze	Collect and Operate
Europe							
Bachelor's degrees (168 to 210)	Operate and Maintain	Securely Provision	Oversee and Govern	Protect and Defend	Investigate	Collect and Operate	Analyze
Bachelor's degrees (240 to 252)	Operate and Maintain	Securely Provision	Oversee and Govern	Protect and Defend	Investigate	Collect and Operate	Analyze
Master's degrees (60 to 90)	Operate and Maintain	Securely Provision	Oversee and Govern	Protect and Defend	Investigate	Collect and Operate	Analyze
Master's degrees (120 to 139)	Operate and Maintain	Securely Provision	Oversee and Govern	Protect and Defend	Investigate	Analyze	Collect and Operate

Considering the categories given above, one can give weights to each of the placements of the categories. Table 8 summarizes this with first place given the weight of seven and last place given the weight of one.

TABLE 8 Weighted summary of the research results in Article II

NICE category	**Total Weight**	**Master's weights**	**Bachelor's weights**
Operate and Maintain	49	21	28
Securely Provision	40	17	23
Oversee and Govern	37	16	21
Protect and Defend	26	11	15
Investigate	23	10	13
Collect and Operate	12	4	8
Analyze	9	5	4

It is evident from these weighted categories that most the education within the research scope is on *Operate and Maintain* category with *Securely Provision* and *Oversee and Govern* following close behind. However, this is a bit of a simplification when the ECTS average differences described in Article II are rather small or rather drastic. Nevertheless, it provides us with a quantitative statistic to understand the general phenomenon.

4.2.2 Finnish Curricula Research

Contents of the Curricula

To investigate the situation of cybersecurity in the Finnish Higher Education system, a similar research setting was utilized within one country. The investigated universities were listed in Table 2. However, the entire field of Information and Communications Technology was included into the research. The research also integrates education that is only available in Finnish language and with a published Finnish language curriculum. This broader research scope was deemed possible as the researchers had more in-depth understanding of the language of the published curricula. Given the universities and the scope, the resulting degrees are listed in Table 9.

TABLE 9 Different degrees/qualifications in data collection

University	Qualification, English	Qualification, Finnish	ECTS
Applied Sciences	Bachelor of Business Administration	Tradenomi (AMK)	210 cr
Applied Sciences	Master of Business Administration	Tradenomi (YAMK)	90 cr
Applied Sciences	Bachelor of Engineering	Insinööri (AMK)	240 cr
Applied Sciences	Master of Engineering	Insinööri (YAMK)	60 cr
Applied Sciences	Bachelor of Police Services	Poliisi (AMK)	180 cr
Applied Sciences	Master of Police Services	Poliisi (YAMK)	120 cr
University	Bachelor of Engineering	Tekniikan Kandidaatti	180 cr
University	Bachelor of Science	Luonnontieteiden Kandidaatti	180 cr
University	Master of Engineering	Diplomi-Insinööri	120 cr
University	Master of Science	Luonnontieteiden Maisteri	120 cr
University	Bachelor of Military Sciences	Sotatieteiden Kanditaatti	120 cr
Universtiy	Master of Military Sciences	Sotatieteiden Maisteri	180 cr

Even within one country the dual university systems and the previous background of different degree programmes provides a varied number of degree durations (in ECTS). Table 10 visualises the number of the degrees and their ECTS durations within the scope of the research.

TABLE 10 Number of sampled degree programmes

Degree programmes	60 cr	90 cr	120 cr	180 cr	210 cr	240 cr
University of Applied Sciences, bachelor's degree	-	-	-	1	19	27
University of Applied Sciences, master's degree	13	11	1	-	-	-
University, bachelor's degree	-	-	-	23	-	-
University, master's degree	-	-	37	-	-	-

From the specific curricula, a data pool of 8321 course names was collected through curricula published on the universities web pages. One way of analysing the course pool was to utilize a word list derived from all the collected course names. From this list, different grammatical spellings of course topics were recognized in their various grammatical forms – plural, singular, and inflected forms. These different forms were combined into generalised attributes that were also part of the NICE framework. Figure 7 illustrates the number of recognized attributes within this data set.

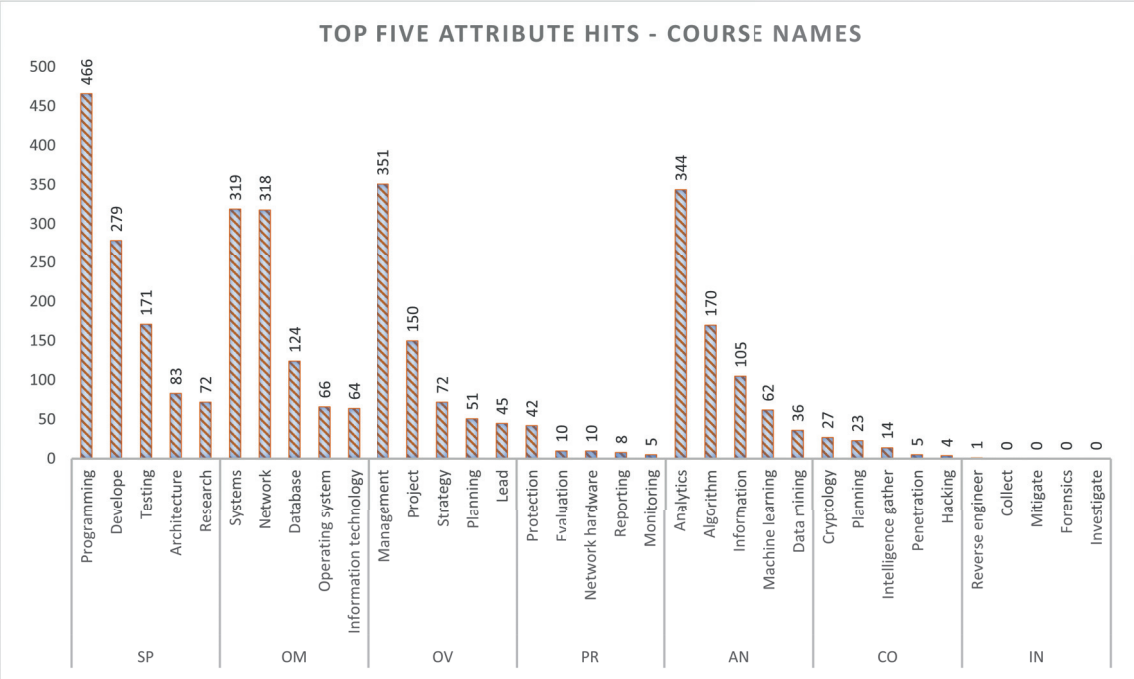


FIGURE 7 Course names through attribute hits within categories

Subsequently, it is important to note that Figure 7 does not take into account whether or not the courses are core, speciality, or elective courses; they are merely present in the course catalogue listings. The graph indicates that the trend is that the top five attribute hits amount to the following statistics presented in Table 11.

TABLE 11 Total attribute hits in course names per category

Category	Total hits	Percentage
Securely Provision (SP)	1071	30.63%
Operate and Maintain (OM)	891	25.48%
Analyze (AN)	717	20.50%
Oversee and Govern (OV)	669	19.13%
Protect and Defend (PR)	75	2.14%
Collect and Operate (CO)	73	2.09%
Investigate (IN)	1	0.03%

Another means of exploring the weights of educated subjects is to compare the courses categorically with the total amount of ECTS spent on the curriculum. This implies that one 3 ECTS course would account for 2,5% of the curriculum of a master's degree (with a duration of 120 ECTS). If all the course topics within a curricula are counted and the average usage of ECTS per category combined together, one can create a visualization such as Figure 8 illustrates.

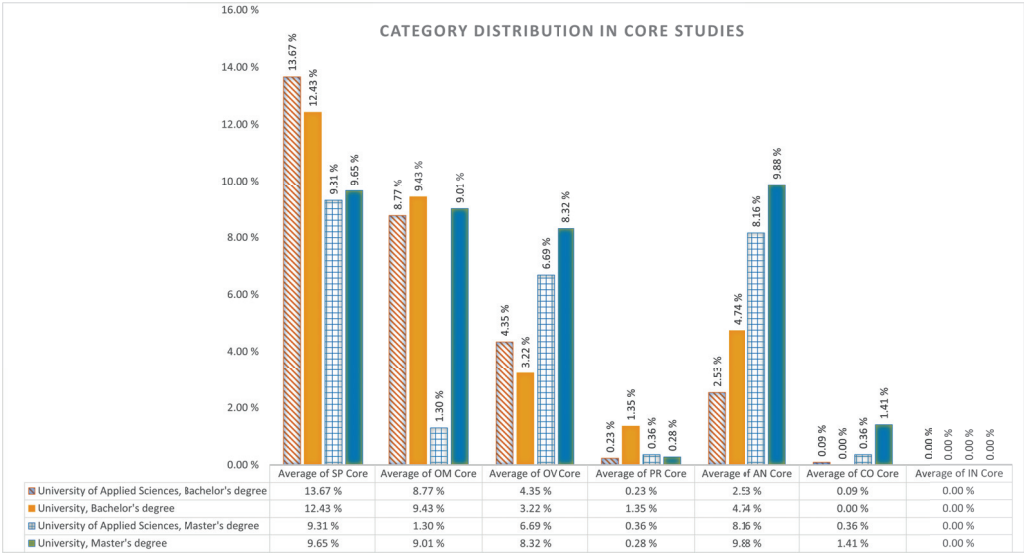


FIGURE 8 Category distribution in core studies

As demonstrated in Figure 8, the core studies are presented with varying emphasis between the universities and respective EQF levels. It is evident that master's degrees have more research-oriented analyze category as part of the curricula in general; this is also true with science-oriented universities in which the research orientation is mandatory in the bachelor's degree. Both bachelor's degrees offer quite a lot of *Securely Provision* compared to the global education emphasis, which was on *Operate and Maintain*.

Along with core studies, the students can select speciality studies to specialize themselves in a certain area. Figure 9 presents the research analysis in speciality studies.

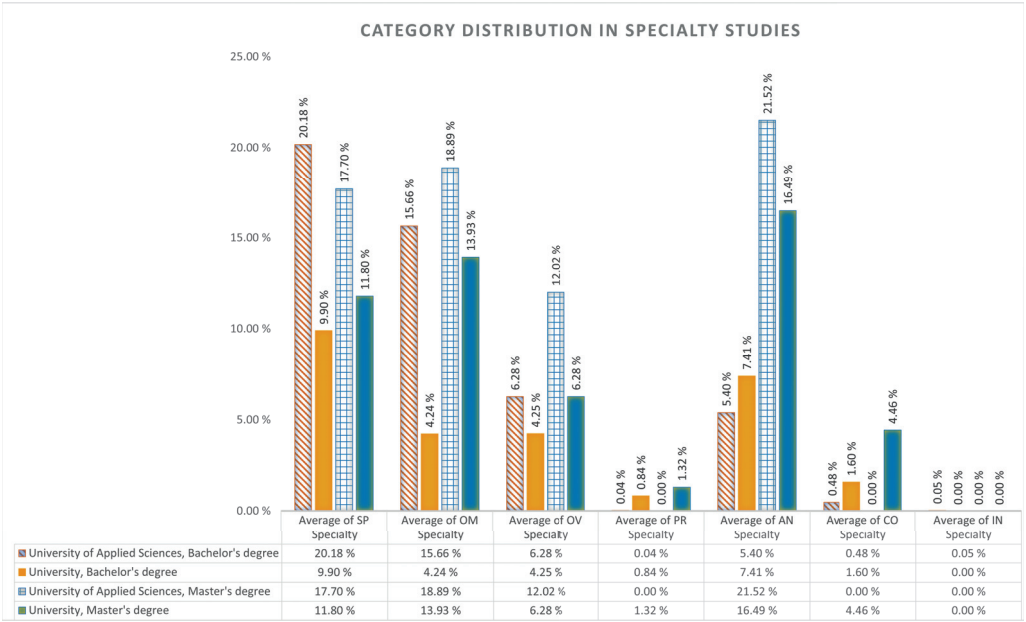


FIGURE 9 Category distribution in specialty studies

As expected, the published curricula offer a varied number of different categories for specialization. However, it is apparent that the *Protect and Defend* and *Collect and Operate* categories are rather miniscule in their course offerings. However, *Investigate* is completely neglegted.

Article IX has a section on elective studies, but it was deemed unnecessary for this dissertation as the courses listed are rather broad and, as mentioned earlier, completely elective. To conclude the Finnish curricula analysis, a chart of category distribution in all studies is presented in Figure 10.

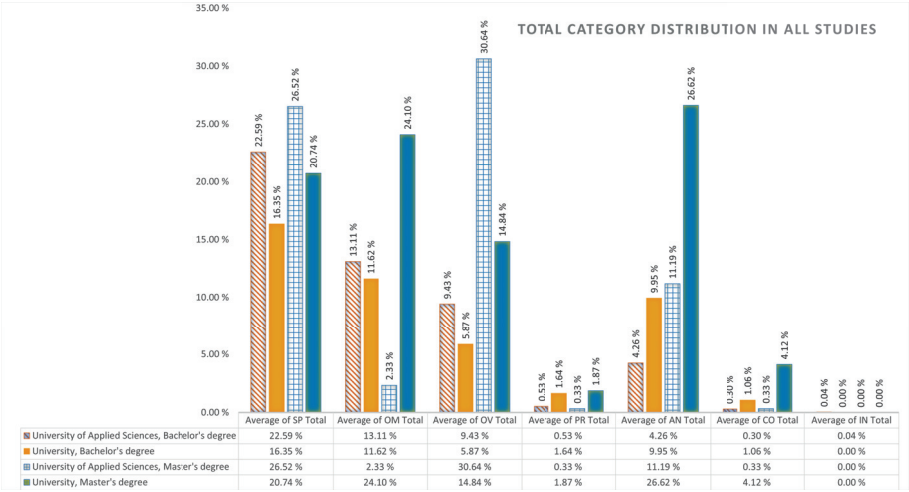


FIGURE 10 Total category distribution in all studies

Figure 10 provides an view of the entire field of higher education of Finland in regards of cybersecurity and with the usage of the NICE framework as an analysis method. The weighing of each category and respective education level and institute is represented. To summarize the weights of each category, Table 12 was created similarly as Table 8.

TABLE 12 Research results in Article IX

Degree (University)	**1st**	**2nd**	**3rd**	**4th**	**5th**	**6th**	**7th**
Finland							
Bachelor's degrees (Applied Sciences)	Securely Provision	Operate and Maintain	Oversee and Govern	Analyze	Protect and Defend	Collect and Operate	Investigate
Bachelor's degrees (University)	Securely Provision	Operate and Maintain	Analyze	Oversee and Govern	Protect and Defend	Collect and Operate	Investigate
Master's degrees (Applied Sciences)	Oversee and Govern	Securely Provision	Analyze	Operate and Maintain	Collect and Operate	Protect and Defend	Investigate
Master's degrees (University)	Analyze	Operate and Maintain	Securely Provision	Oversee and Govern	Collect and Operate	Protect and Defend	Investigate

It is evident from this that the bachelor's degree is pretty similar in all universities, except that scientific universities focus more on *Analyze*. In the master's degree the difference is that in applied sciences universities, the focus of the degree is more on *Oversee and Govern*, whereas in the scientific universities *Analyze* occupies the top spot. Table 13 summarizes the weights of the different degree levels.

TABLE 13 Weighted summary of the research results in Article IX

NICE category	Total Weight	Master's weights	Bachelor's weights
Securely Provision	25	11	14
Operate and Maintain	22	10	12
Analyze	21	12	9
Oversee and Govern	20	11	9
Protect and Defend	10	4	6
Collect and Operate	7	3	4
Investigate	4	2	2

Intake of Degree Programmes (in Universities of Applied Sciences)

The total annual throughput of the education system can be estimated from the total intake of students in the degree programmes. In this section, the intake of students in Universities of Applied Sciences is investigated through the education programmes based on the aim of the degree. Rather than making quantitative measurements of the courses and their category placement, the curriculum structure was more qualitatively observed by the author from public web pages and curriculum structure. Using these observations the following types of education were defined (and an explanation provided) in Table 14.

TABLE 14 Degree programme types defined and utilized in analysis of data

Type	Specification
A	Cybersecurity focused degree programme and directly available for application in Studyinfo
B	Degree programme that had cybersecurity as a specialization
C	Degree programme had cybersecurity as a mandatory course, but targeted another subject (e.g. Robotics or Game Development)
D	Degree programme had courses on cybersecurity as a specialization or elective
E	Degree programme did not have an cybersecurity course, however a parallel curriculum had one within the same university
F	Degree programme nor its parallel curricula had cybersecurity (within the same university)

Given these types of education, the intake students for academic year 2022–2023 was collected from Studyinfo system[2]. This provides us an idea of how

[2] https://opintopolku.fi/konfo/en/

much cybersecurity focused students are educated by the Universities of Applied Sciences in the Finnish education system. One must note that this is only degree programme students. Table 15 presents the intake in the master's degree programmes.

TABLE 15 Types of degree programmes and their starting places per year in master's degrees

Type	Amount of Degree Programmes	Starting places	% of starting places
A	4	79	11.11...%
B	0	0	0 %
C	8	150	21.10 %
D	2	70	9.85 %
E	6	182	25.60 %
F	10	230	32.35 %

There are only four degree programmes in Finland with a direct focus on cybersecurity in the Universities of Applied Sciences. Most other master's degrees have the possibility of choosing elective studies from these degrees. Table 16 presents the intake in the bachelor's degree.

TABLE 16 Types of degree programmes and their starting places per year in bachelor's degrees

Type	Amount of Degree Programmes	Starting places	% of starting places
A	3	85	2.22 %
B	5	390	10.18 %
BC	1	20	0.52 %
C	11	752	19.63 %
CD	12	618	16.14 %
CDE	1	40	1.04 %
CE	1	40	1.04 %
D	13	1163	30.37 %
E	12	447	11,67 %
F	5	275	7.18 %

With regard to the bachelor's degree, it is noteworthy that B-type degree programmes are present rather heavily. Based on the inqueries by the author of this dissertation to admission services, this is because the degrees were much more precisely following the Recommendations for Admission Criteria[3] by the The Rector's Conference of Finnish Universities of Applied Sciences[4] (or Arene). During the latter part of 2010 decade, these recommendations have begun to allow much more loose of an approach to the curricula names and typing. This

[3] https://www.arene.fi/julkaisut/raportit/ammattikorkeakoulujen-valintaperustesuositukset/

[4] https://www.arene.fi/the-rectors-conference-of-finnish-universities-of-applied-sciences-arene/

varied naming of the curricula is starting to place a vague fog on how each curriculum is typed into the fields set by the International Standard Classification of Education (UNESCO Institute for Statistics, 2015).

From all the degree programmes, purely cybersecurity-oriented courses were observed in the Universities of Applied Sciences. This revealed the heterogenous course offering of varying durations and names, which are presented in Table 17. The entire list of course names is presented in Appendix 1.

TABLE 17 Varying durations and names of cybersecurity courses

ECTS-size	Times of appearance
15	1
10	2
5	115
4	4
3	9
2	2
1	2

4.3 Cybersecurity Education Stakeholder Research (Articles IV, VII, and VIII)

4.3.1 Industry expectations

Deaconu et al. (2014) discuss on the difficult mission of the education system to match the needs of the labour market by developing the right competences for students. Education should aim to provide skilled workforce (Barnett, 2011). There are models proposed for a more industry-driven approach to measure the competences needed to be *work-ready* (Azevedo et al., 2012). Niemelä (2019) analysed the workforce need regionally in Finland through open vacancies bulletins and interviewing (n=5) personnel who were responsible for recruiting cybersecurity personnel.

The research approach chosen in Article IV, was to have an online survey directed towards the industry. The questionnaire received 50 answers. The amount of respondents were dissected through company size as recommended by European Comission (2003) and sector as described by Nai Fovino et al. (2019). This is visualized in Figure 11.

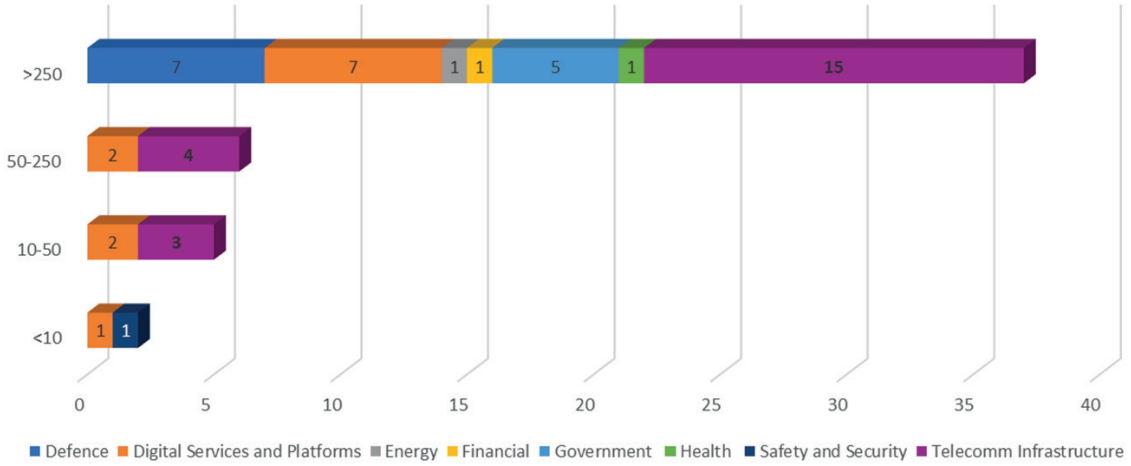


FIGURE 11 Respondents sector and size (n=50)

Noticeable is the size of companies that participated in the questionnaire with most of them aligning to *Telecomm Infrastructure*. *Digital Services and Platforms sector* is also very apparent on the second place of the respondents.

The respondents were asked to mark the importance of each of the learning goals of the cybersecurity maintenance module in vocational education. Figure 12 displays this data.

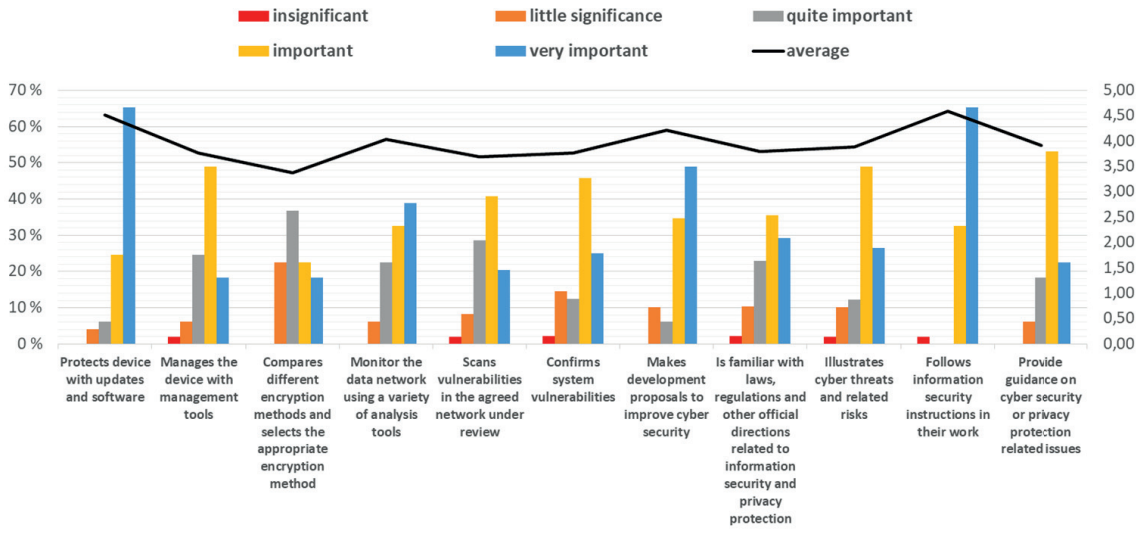


FIGURE 12 Vocational learning objectives and their importance by the industry (n=49)

What is evident is the protection of devices through updates and software although following information security instructions and proposing improvements come right after those. Active monitoring of the data network using analysis tools is deemed necessary on fourth place. Given these answers the respondents were asked about the importance of bachelor's degree education modules from the degree of the author's university. The answers are presented in Figure 13.

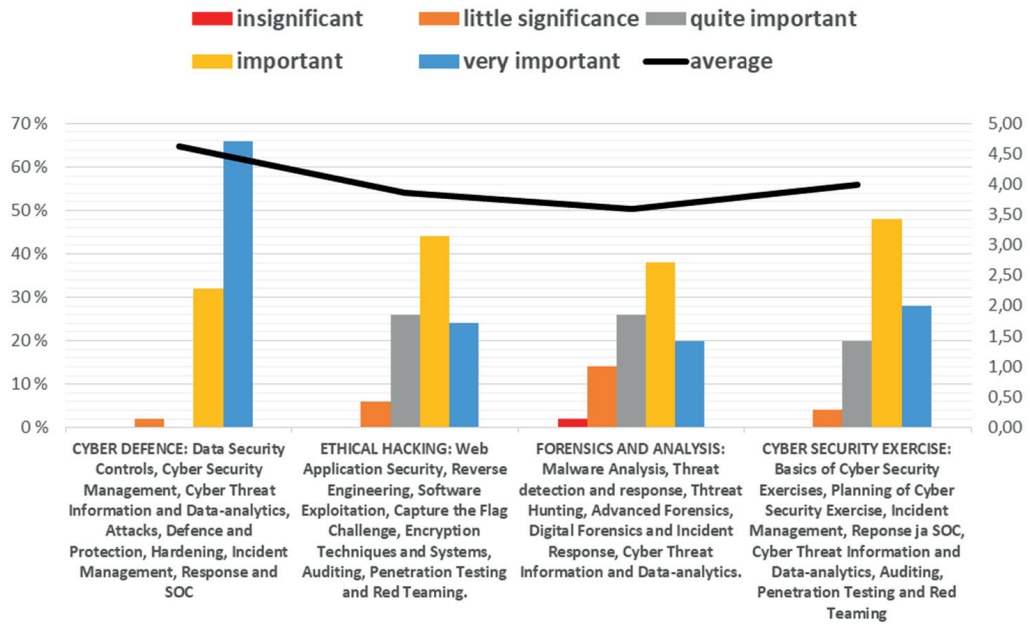


FIGURE 13 Importance of the bachelor's degree module (at Jamk) as stated in the industry (n=50)

The modules on vote have 30 ECTS courses that can be interpreted as part of different categories in the NICE framework. However, the module itself is deemed to belong to a certain category. As evident from the results of this research, the most demanded module would be Cyber Defence, which is a mix of *Oversee and Govern*, *Securely Provision* and *Operate and Maintain*. Second would be the Cyber Security Exercise (mainly *Protect and Defend*, but with a dash of *Analyze*) module and after those Ethical Hacking (*Collect and Operate*) and Forensics and Analysis (*Investigate*) modules.

Given this course emphasis, also the respondents were asked to estimate their recruitment needs when concerned with cybersecurity personnel. The level of education was handed out in Finnish and then later mapped to the EQF levels. Figure 14 presents the choices the participants answered the most.

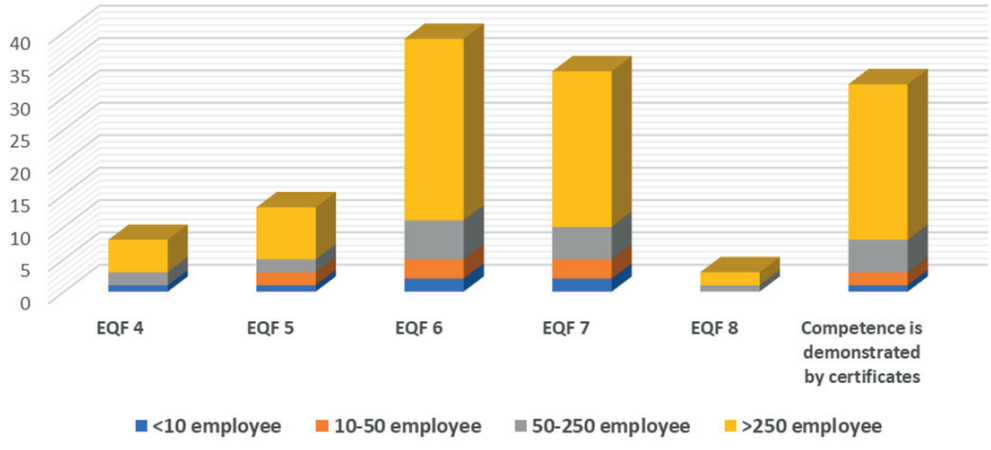


FIGURE 14 Target EQF levels for recruiting (n=129)

Most of the personnel recruited in cybersecurity appear to be EQF 6- and EQF 7-level candidates. After these is the option to provide proof of their capability through ICT certificates, irrespective of the degree level of the applicant.

The last section was concerned the required experience level or comprehension of the subject through Bloom's Taxonomy. This was to get an idea of how well trained or experienced the applicants must be. Figure 15 presents these results.

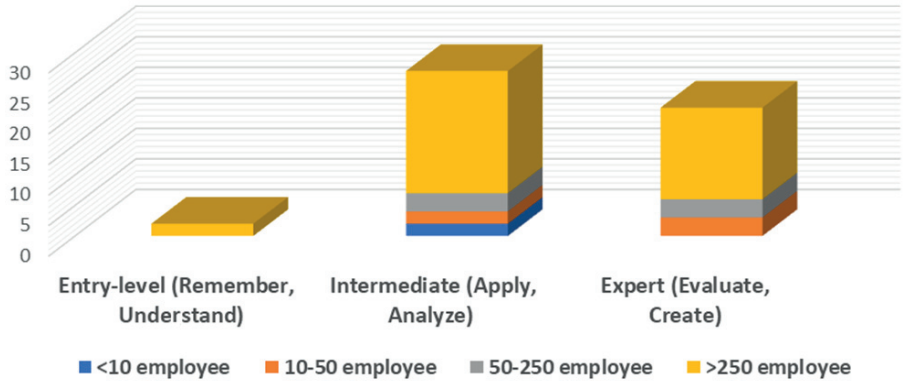


FIGURE 15 Experience levels of recruited personnel as Bloom's taxonomy (n=50)

It is evident that entry-level students are not deemed so desirable in smaller companies; however, irrespective of the company size, all of them are interested on intermediate level experience.

4.3.2 Graduate research

In Finland, the graduates from all the Universities of Applied Sciences are approached with a national questionnaire five years after their graduation[5]. However, this questionnaire is not sufficiently precise for analysing the cybersecurity graduates. The closest filter allowed is in the field of *Information and Communications Technology*, which in Finland has two different degrees: *Bachelor of Engineering* and *Bachelor of Business Administration*.

The focus of research in Article VII was on graduate alumni students from Jamk University of Applied Sciences who specialized in cyber security during the bachelor's degree. The main purpose was to identify where those who graduated were employed in the industry and with what kind of responsibilities. The questionnaire researched 19 students, which is around 30 % of the possible candidates. Figure 16 shows the placement through company size and public or private sector organization.

5 https://uraseurannat.fi/ammattikorkeakoulujen-uraseuranta/from-uas-to-career-career-data-for-all/

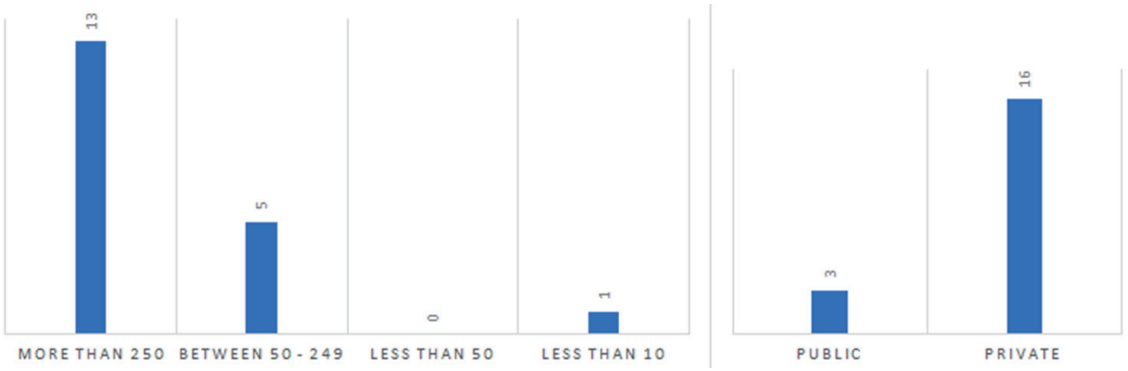


FIGURE 16 Organization size and sector

It is evident from figure that the alumni were mostly employed in larger organizations with most of them being privately owned. Similarly, as respondents from the industry chose their sector, the students selected their organization field based on the Cybersecurity Taxonomy presented in chapter 2.3. Figure 17 presents the distribution of where alumni were employed.

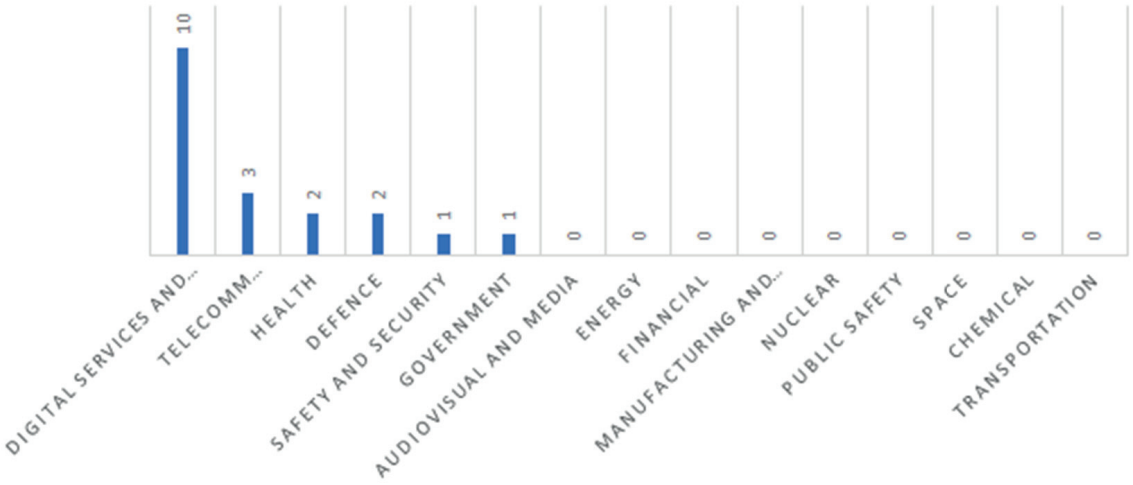


FIGURE 17 Organization field per taxonomy sector

It is evident from the data that *Digital Services and Platforms* were the most frequent sector and *Telecomm Infrastructure* came after that.

The alumni were asked to familiarize themselves with the NICE framework and its work roles. After this the researchers asked them to rate from first to fifth descriptive work role of their work. Figure 18 presents the distribution of work roles within the alumni.

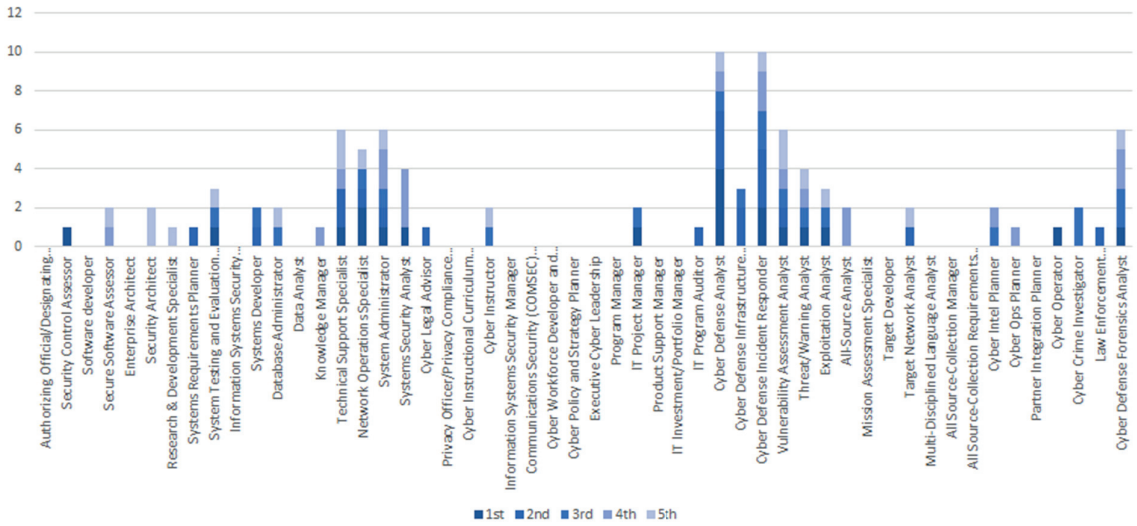


FIGURE 18 NICE framework work roles based on respondents' answers

The entire work role graph is rather extensive to look, but few work roles are clear from most answers: *Cyber Defense Analyst* and *Cyber Defense Incident Responder*. This most presumably comes from the uprising of Security Operation Centers within different organizations. Figure 19 represents the same data through the category abstraction layer.

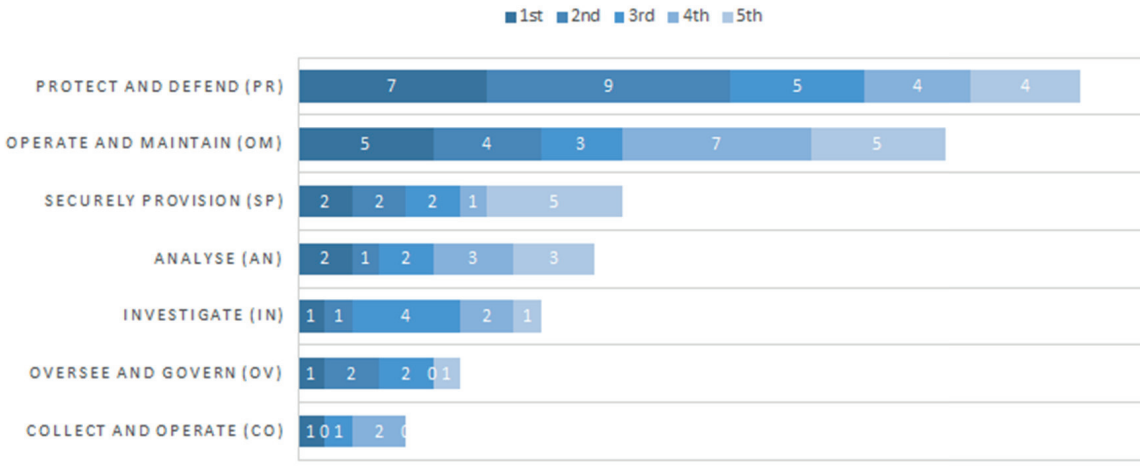


FIGURE 19 Top NICE framework categories on what best fits their work

The category weights of cybersecurity graduants is apparent in the figure. *Protect and Defend* is the top category for work responsibility, with *Operate and Maintain* and *Securely Provision* after it. The researchers also visualized the work roles through only the first and second options, which provided the following visualization represented in Figure 20.

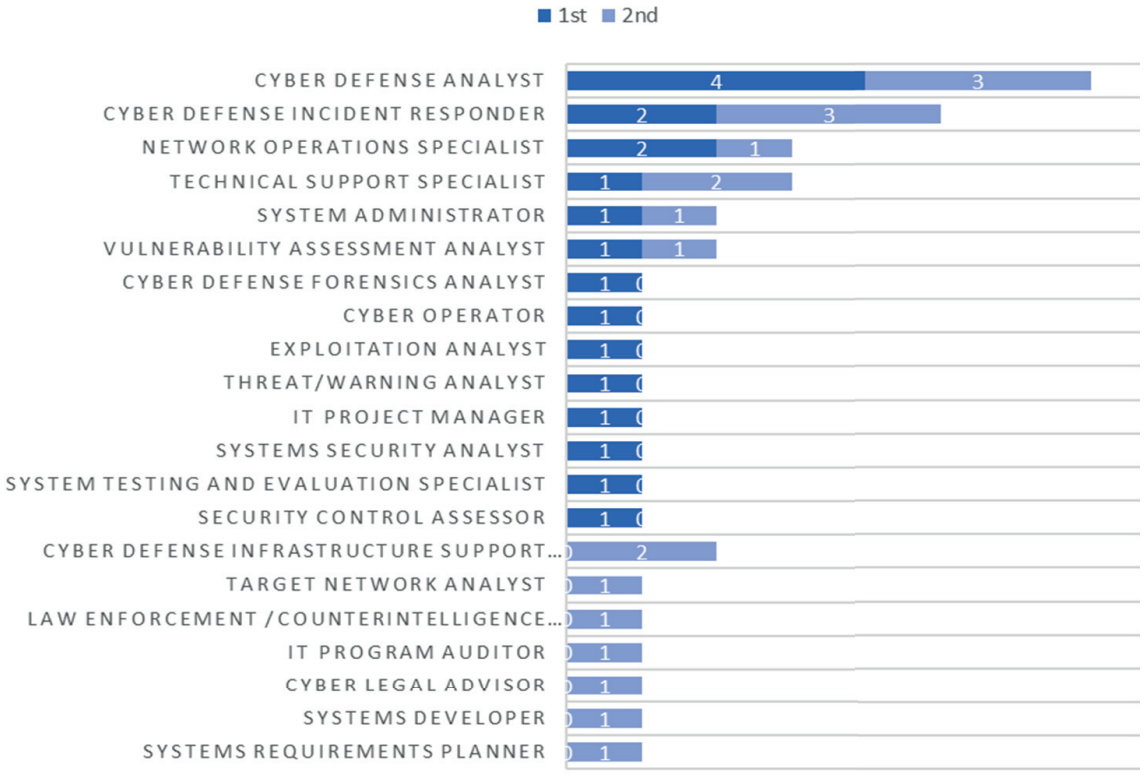


FIGURE 20 Top work roles based on first and second choices

After the research on current employment and responsibilities, one additional question was to choose their specialization module from the degree programme in which the graduates studied. The module choices are presented in Figure 21.

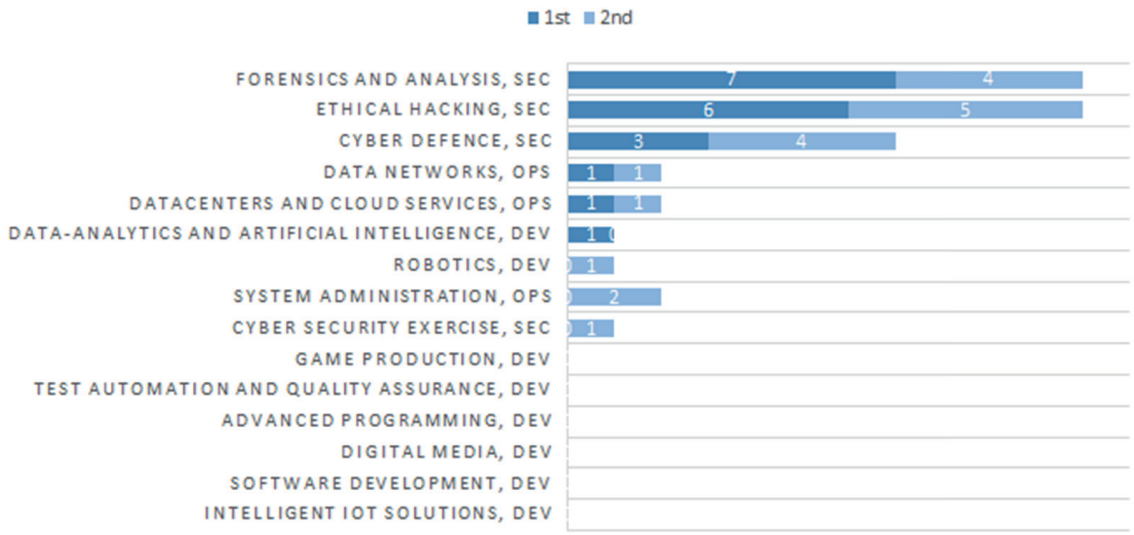


FIGURE 21 Module choices from the Jamk ICT engineer curriculum offering

As the graduates were employed most frequently in *Protect and Defend* category, and specifically with work roles in incident response and analyse, the most popular module was *Forensics and Analysis*. This is a module that was not offered to the graduates during their studies; thus, it is apparent that it is something to consider as an lifelong learning for example, in Open University studies. What is also evident from the data is the *Operate and Maintain* responsibilities through *Network Operations Specialist* and *System Administrator* work roles. The module choices also support these after the cybersecurity-oriented modules.

4.3.3 Thesis research

Theses are written typically at the end of a study. The topics should relate to their field of study and show application of their skills through development and scientific research. The goals of the thesis should follow the grading scheme of the university, which in turn should be based or at least follow the legislation guiding the university. In this research, only the publicly available theses were collected through either electronic repositories available on the internet or by having discussions with the library services of said universities. This research was focused on Central Finland, which hosts two different universities, with both running an active degree programme on cybersecurity:

- Jamk University of Applied Sciences, bachelor's degree (33 Theses)
- Jamk University of Applied Sciences, master's degree (75 Theses)
- University of Jyväskylä, master's degree (65 Theses)

It is worth noting that the bachelor's degree at the University of Jyväskylä was left out, as their theses were not clearly focused on the field of cybersecurity, but rather ICT in general. A total of 173 theses were collected and researched. Figure 22 presents the distribution of theses per NICE framework category.

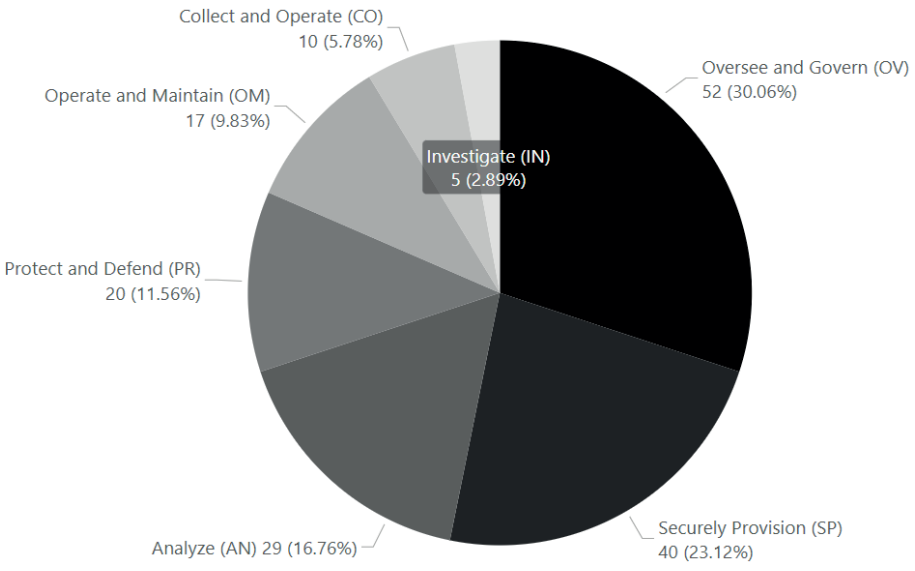


FIGURE 22 All theses spread over the NICE framework categories

As the majority of the theses were conducted on the master's degree, it is evident that *Oversee and Govern* is the main category for theses. The same data can be analysed per organization to see the differences between Universities and Universities of Applied Sciences. This is demonstrated in Figure 23.

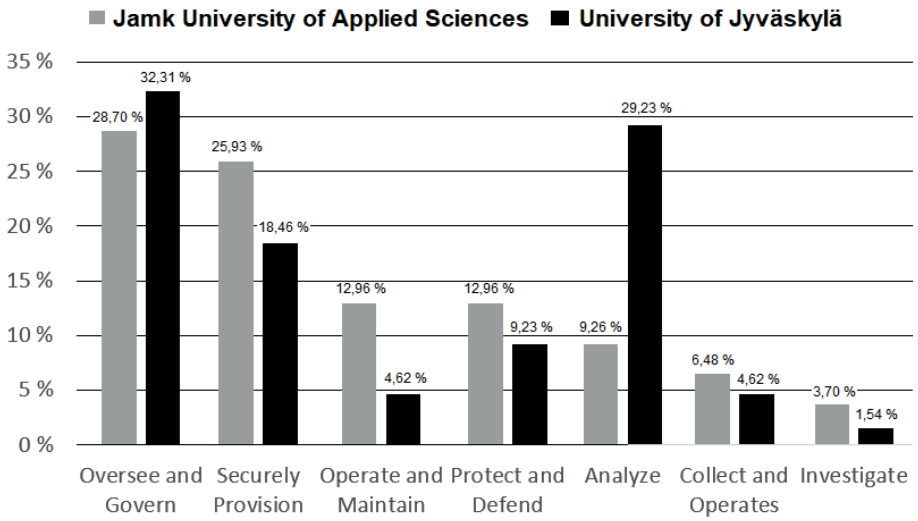


FIGURE 23 Comparison of NICE framework categories based on university or applied sciences

Not much notable difference is evident here, except for the high spike in *Analyze* category and a small amount of theses in *Operate and Maintain* category at the University of Jyväskylä. To see the differences between the degree programmes, the visualization in Figure 24 was created.

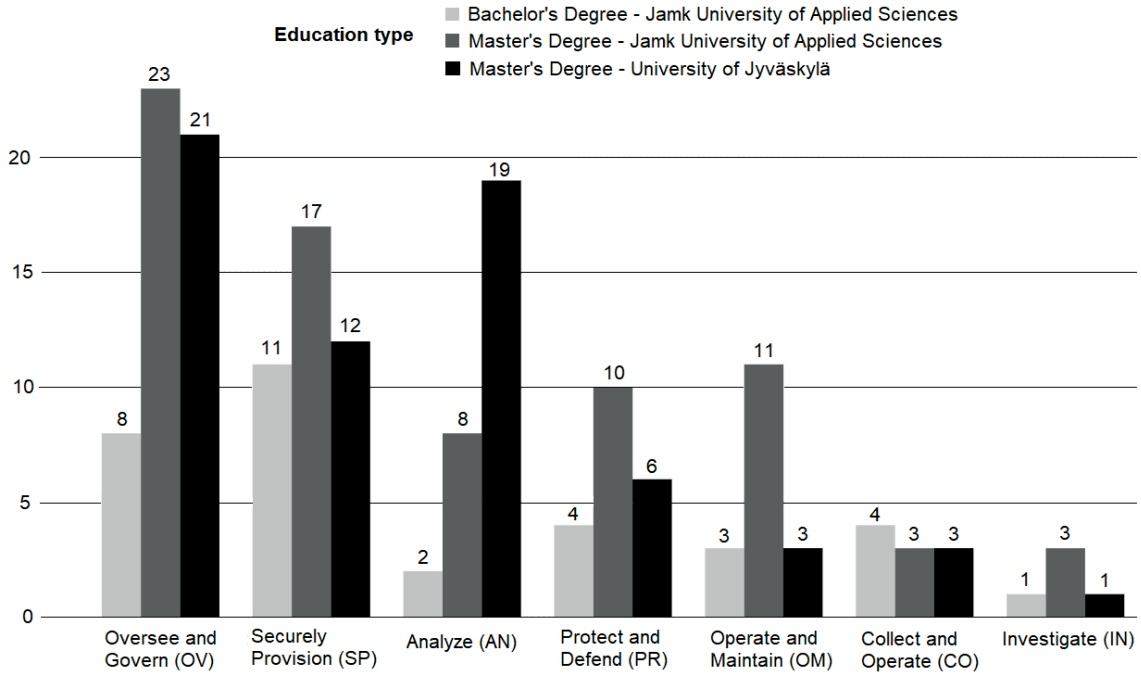


FIGURE 24 NICE framework category mapping of finalized theses per degree programme

The most noticeable differences between the degree programmes is that *Securely Provision* is a category where most of the theses are conducted in the bachelor's degree and *Analyze* is in second place in the University of Jyväskylä master's degree. The same data is also presented in Table 18.

TABLE 18 Category mapping of finalized theses per degree programme

Categories	Bachelor's (Jamk)	Master's (Jamk)	Master's (JYU)	Total
Oversee and Govern (OV)	8 (24.24%)	23 (30.67%)	21 (32.31%)	52 (30.06%)
Securely Provision (SP)	11 (33.33%)	17 (22.26%)	12 (18.46%)	40 (23.12%)
Analyze (AN)	2 (6.06%)	8 (10.67%)	19 (29.23%)	29 (16.76%)
Protect and Defend (PR)	4 (12.12%)	10 (13.33%)	6 (9.23%)	20 (11.56%)
Operate and Maintain (OM)	3 (9.09%)	11 (14.67%)	3 (4.62%)	17 (9.83%)
Collect and Operate (CO)	4 (12.12%)	3 (4%)	3 (4.62%)	10 (5.78%)
Investigate (IN)	1 (3.03%)	3 (4%)	1 (1.54%)	5 (2.89%)
Total	33 (19.08%)	75 (43.35%)	65 (37.57%)	173 (100%)

Applied sciences legislation focuses on regional development[6], while scientific universities legislation points toward the progress of science and mankind[7]. With differing legislation for the organizations, applied sciences occasionally demand an orderer (organization) of a thesis, while the scientific universities can progress on the thesis topic through only scientific purposes. This causes many of the theses to be conducted in research and development projects at the universities counting towards Government sector in the taxonomy. This is evident in the theses data when analysed through sectors in Figure 25.

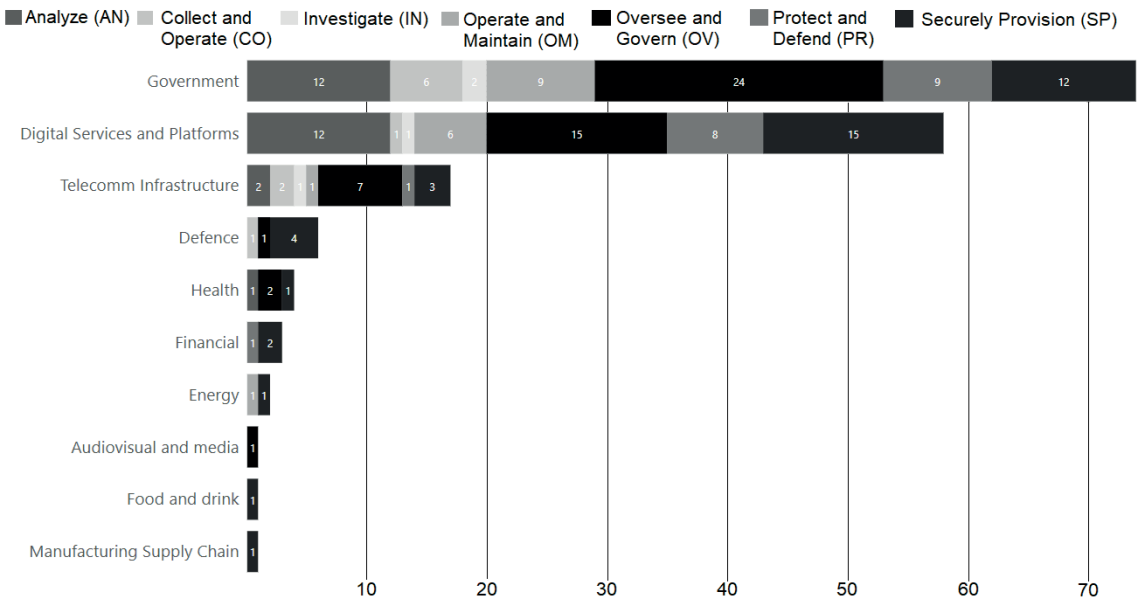


FIGURE 25 Theses conducted per taxonomy sectors

If *Government* is excluded from the data, it is evident that *Digital Services and Platforms* is the sector where theses are mostly performed and right after that is *Telecomm Infrastructure*.

6 https://finlex.fi/fi/laki/ajantasa/2014/20140932
7 https://www.finlex.fi/fi/laki/ajantasa/2009/20090558

The same data can also be analysed through work roles where the thesis would mostly be focused on; however, many of the theses could fit multiple work roles. Thus, the researchers had to make qualitative and subjective choices to produce the information presented in Table 19.

TABLE 19 Work role mapping of theses

Placement	Work Role	Count
1.	Threat/Warning Analyst	19
2.	Research & Development Specialist	18
3.	Cyber Policy and Strategy Planner	15
4.	Vulnerability Assessment Analyst	11
5.	Privacy Officer/Privacy Compliance Manager	8
6.	Cyber Instructor	7
7.	Cyber Legal Advisor	6
7.	Security Architect	6
9.	Cyber Crime Investigator	5
9.	Cyber Instructional Curriculum Developer	5
9.	Cyber Workforce Developer and Manager	5
9.	Network Operations Specialist	5
9.	Security Control Assessor	5
9.	System Requirements Planner	5
9.	Systems Security Analyst	5

These work roles can be also separated in accordance with degree. Thus, Figure 26 was created to reveal the possible focus points of different degrees.

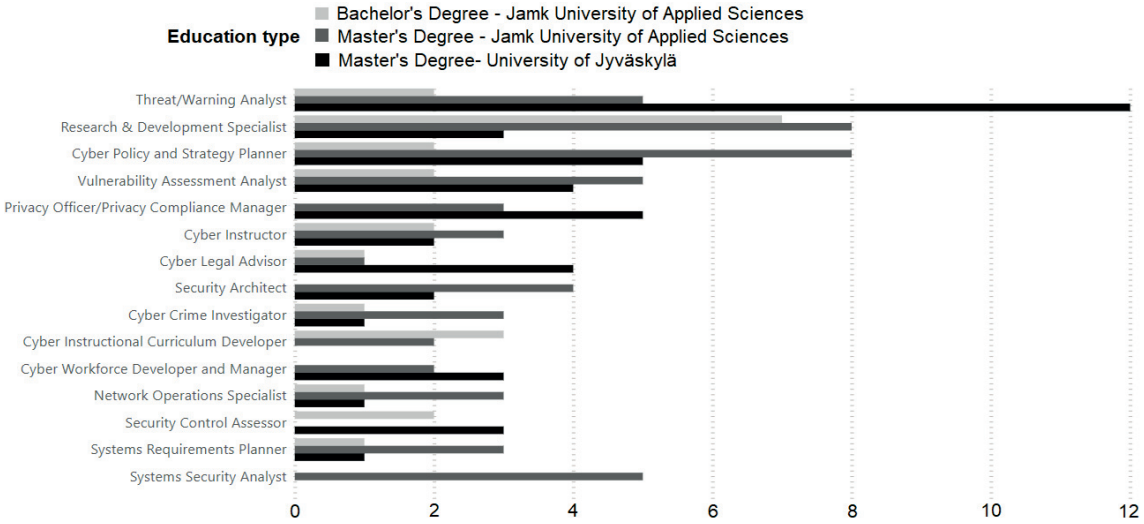


FIGURE 26 Mapped work roles by education

The work roles were rather spread out and no exact conclusion can be made from the theses work role data. With the work done it was still apparent to attach them to the results as one proof of usability of the different hierarchy levels in the NICE framework.

4.4 Improvement Proposals for Cybersecurity Education (Articles I, III, V, and VI)

4.4.1 Development of degree programme

Curriculum development and its underlying principles is a topic researched under many fields of education (McCormack et al., 2022; Sampson et al., 2022; Kähkönen and Hölttä-Otto, 2022). Article I of the dissertation was written as an idea by the author of this dissertation on how to combine the different educational and cybersecurity frameworks into one cohesive design. Even thought researching into the literature background, no such ground level model was found. Most of the research papers focused on defining the *knowledge areas*, *sectors*, or *categories* of cybersecurity rather than taking them into use in a curriculum.

The underlying data structure of the curriculum in place, before writing the paper, was challenged through an EUR-ACE audit and from the feedback given; the author of this dissertation dabbled with several data structures on how to combine, the occasionally contradicting or overlapping, frameworks. This idea, construct, or a model of development is presented in Figure 27.

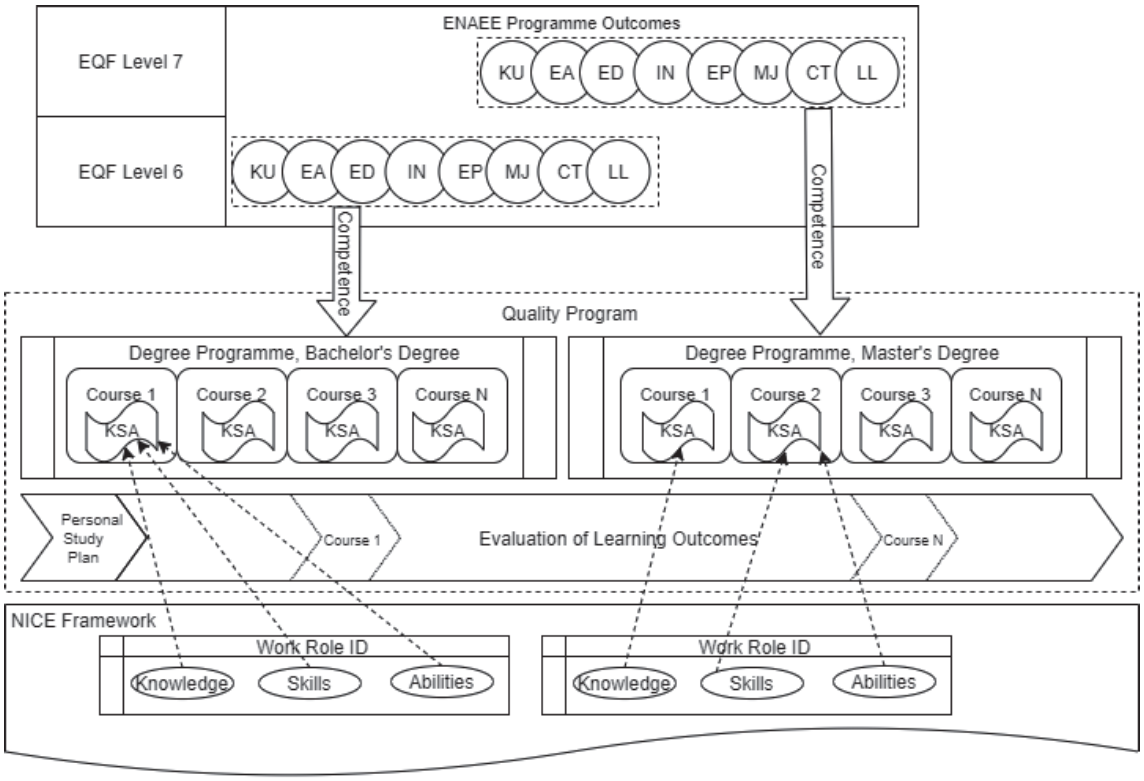


FIGURE 27 A visualization of a design model for a degree programme in cybersecurity

By having a relational database as a support for the curriculum structure, and writing necessary course descriptions to withold that information, one could also create a visualization for educators and students alike to browse the

said structure. Figure 28 presents a Power BI visualization which one could go through either by course names or modules on what NICE framework KSA's they develop and what work roles they prepare for, by using different filters.

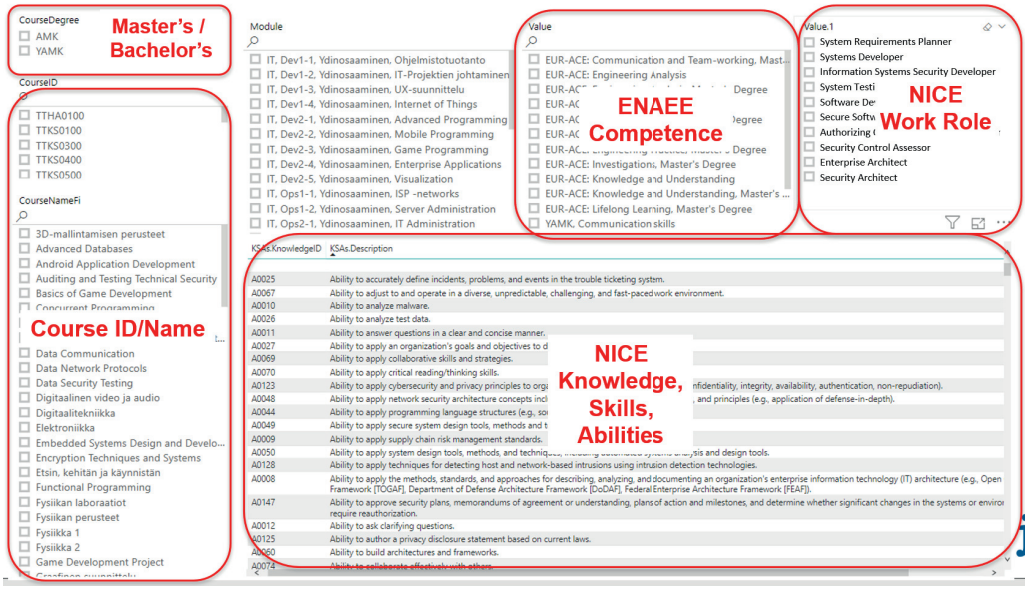


FIGURE 28 Design model for a degree programme in a Power BI dashboard

As the NICE framework is not recognized as a competence model in the European Union, the EUR-ACE competences were mapped to the courses on what they developed. The model also made it possible for the inclusion of several different frameworks or competences, which have not been a part of this dissertation, such as *Software Engineering Body of Knowledge* (SWEBOK) or *European e-Competence Framework* (e-CF) to name a few.

4.4.2 European Cybersecurity MOOCs quality assurance

The use and effectiveness of MOOCs is under research in different fields of education (Van den Broeck et al., 2020; Israel, 2015). Within Finland, because of high demand, cybersecurity MOOCs have already become available in the form of, for example, Cyber Security Base[8] (University of Helsinki and F-Secure company collaboration) and Citizens Cybersecurity (finnish: Kansalaisen Kyberturvallisuus) in University of Jyväskylä[9].

The aim of Article III, was to elicit a quality assurance criteria directed for MOOCs concentrating on cybersecurity. Inspirations for such a definition was drawn from already existing MOOC quality assurance and validation frameworks such as OpenupEd label (Rosewell and Jansen, 2014) and the Quality Reference Framework (QRF) for the Quality of Massive Open Online Courses (MOOCs) (Stracke et al., 2018) to name a few.

8 https://cybersecuritybase.mooc.fi/

9 https://www.avoin.jyu.fi/fi/opintotarjonta/informaatioteknologia/kyberturvallisuus

Cybersecurity MOOCs were divided into three separate categories: Academic level MOOCs, Continuous Learning MOOCs and MOOCs utilizing cyber ranges. It was also apparent that combinations of these could also be in use. Through these categorizations, the research proposed several criteria that were specific to cybersecurity. In the paper, these criteria were utilized in an initial evaluation of MOOCs:

- Continuous learning MOOC: 'Information Security: Context and Introduction' by Royal Holloway, UK Royal Holloway (2020)
- Continuous learning MOOC: 'Managing Security in Google Cloud Platform' by Google (2020)
- Academic MOOC: 'Netzwerksicherheit' by Technische Hochschule Luebeck (2020), Germany
- Academic MOOC: 'Privacy by Design' by Karlstad University (2020), Sweden
- Academic MOOC: 'Development of Secure Embedded Systems Specialization', by EIT Digital (2020) Cyber Security course
- Academic and continous learning MOOC: 'Cyber Security Base with F-Secure, Academic', by the University of Helsinki and F-Secure (2020), Finland

In the evaluation, the developed criteria was used for the first time. The process to utilize them can be described in the following manner. Independent evaluation was performed on the courses by several experts. After the initial phase, the results were consolidated with consensus discussions to reach decisions on borderline cases. The results of the initial evaluation were collected and presented in Table 20.

TABLE 20 Average distribution of criteria assessment ratings per criteria category for the evaluated MOOCs in percentage.

Category of Criteria	yes	partly	no	unclear
Qualification of the proposing institution	80.5	2.4	12.2	4.9
Course structure and content criteria	55.2	12.8	3.2	28.8
Qualification of instructors	52.8	8.3	2.8	36.1
Course examination, credentialisation, and recognition	40.6	4.2	32.3	22.9
Privacy requirements	37.1	8.6	14.3	40.0
Openness	33.3	0.0	0.0	66.7
Ethical considerations for teaching cyber security	25.0	4.2	20.8	50.0
Meeting professional expectation	14.3	0.0	21.4	64.3
Average	45.2	7.0	14.7	33.1

The process to obtain this result was seen as a good means of governance in the research. The process was deemed valid and recommended as a deliverable of the CyberSec4Europe project to be utilized in the European Cyber Security Competence Center. However, the lack of MOOCs utilizing cyber ranges

was apparent in the evaluation set, as such were not deemed available during the research. This leaves the criteria related to cyber range MOOCs that remain untested.

What was troublesome in the results obtained was that only half of the criteria were fulfilled within the MOOCs selected for evaluation. There were several categories where the criteria were not fulfilled to an acceptable rate as deemed by the researchers. These categories were *Privacy Requirements*, *Meeting Professional Expectation* and *Openness*. Through the usage of the developed quality criteria, hopefully more validated MOOC courses become available in the European Union.

4.4.3 European Cyber Range usage and improvement

Laboratory environments are considered as an integral part of engineering education (Nikolic et al., 2021). The COVID-19 pandemic led to a rapid transition towards online (or remotely used) laboratories due to the restrictions on face-to-face contacts (May et al., 2022). In cybersecurity, these laboratories are typically called cyber ranges (or cyber arenas). They are built ICT environments that facilitate education, training, and exercise in cybersecurity (Karjalainen and Kokkonen, 2020). The usage of these cyber ranges is of interest in the field of cybersecurity (Ukwandu et al., 2020).

For the research performed in Article V, the researchers utilized a survey directed to organizations known to have hosted a cyber range. The survey received a total of 44 responses, out of which 39 were considered valid answers based on reviews the answers. The survey did not utilize very taxonomic approaches, but rather included reseached data on cyber ranges on why they are used and by whom (amongst other details that are not relevant for this dissertation). Figure 29 presents the primary target groups utilizing the cyber ranges.

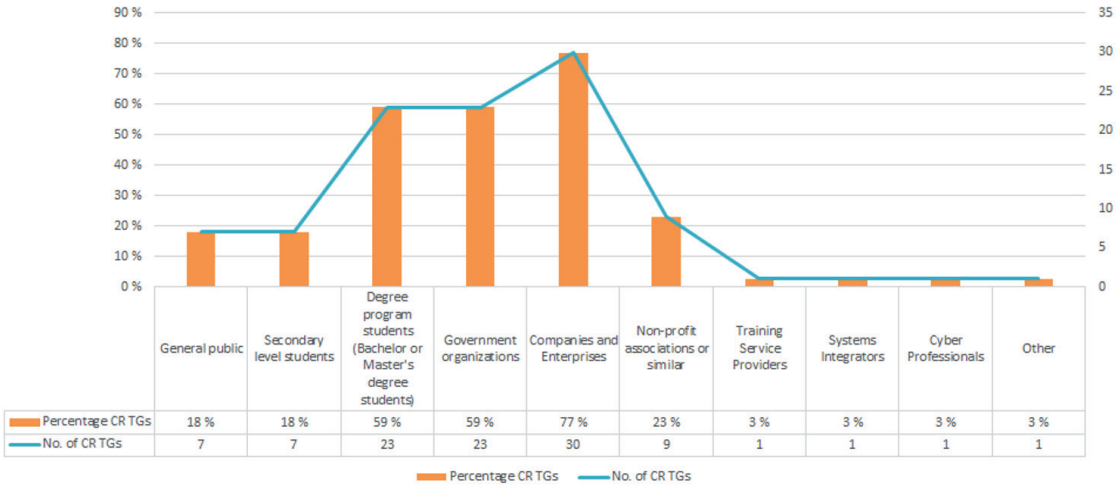


FIGURE 29 Target groups of the cyber ranges (n=39)

It is evident from the diagram that most frequent usage is around (private) companies and enterprises utilizing the cyber range. After this, side by side, is

the usage by government organizations and degree students studying for either master's and bachelor's degrees. The utilization of the cyber ranges for secondary level students and the general public was rather low.

The participants were also asked the main reason for them to utilize a cyber range. This is depicted in Figure 30.

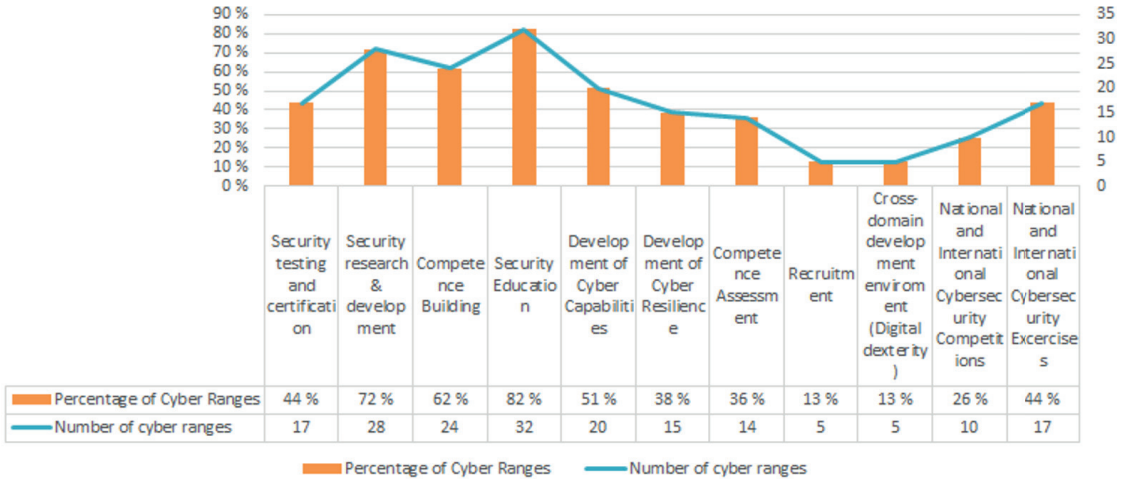


FIGURE 30 Use cases of cyber ranges (n=39)

From these answers, *Security Education* emerged on top, althought it is not evident as being directly focused on degree education. It might also be suitable for the personnel within public and private organizations and to support their understanding of cybersecurity through education events held within the cyber ranges. *Security research & development* is second within organizations utilizing the cyber range for the purposes of R&D-projects.

In Article VI, the writers of the paper proposed a model for having a preliminary questinnaire for participants (regardless of their target group) coming to a event held in a cyber range. This questionnaire model would give the organizers of such events the ability to understand the educational backgrounds and job responsibilities before the educational event in the cyber range. The formation of the questions bases on the taxonomies and frameworks represented in the theory backround section of this dissertation. Questions and their background can be seen from the original paper. The questionnaire was utilized in the Flagship 2 event of CyberSec4Europe project. Althought not in the paper nor included in this dissertation, a post exercise survey was also planned to be conducted utilizing the same principles. However, the author of this dissertation was not a part of that research.

5 CONCLUSIONS

During the decade of work by the author at the University of Applied Sciences in Jyväskylä, it was evident that the field of cybersecurity education boomed amidst the field of Information and Communications Technology education. Figure 31 depicts the development of degree programmes (in Finland), cybersecurity strategies, and frameworks published during the timeframe of this research.

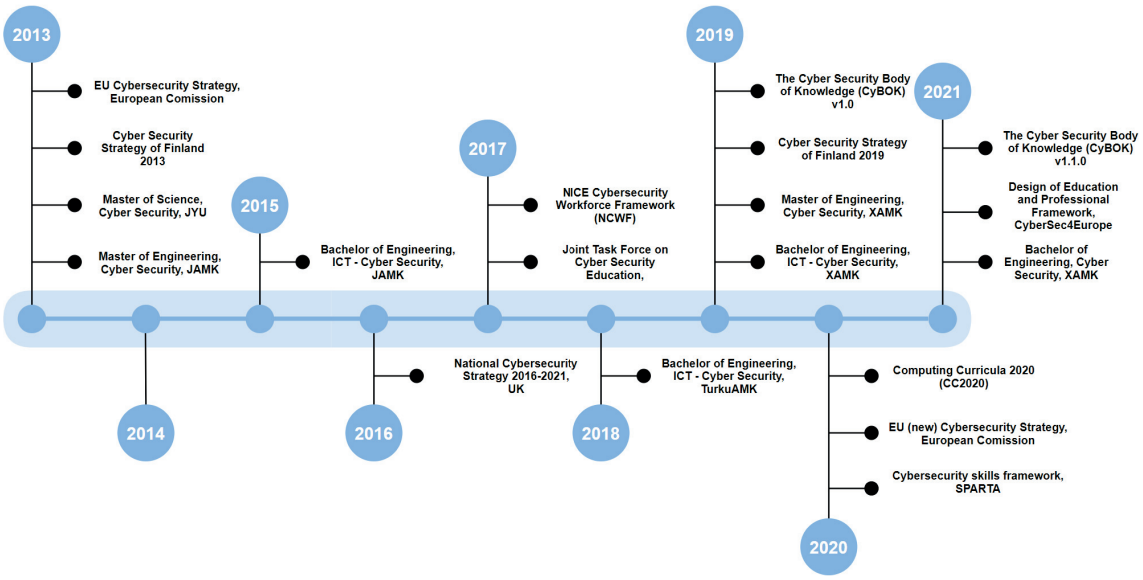


FIGURE 31 Timeline of cybersecurity development during the research

In his work experience, the author had delved into the field of education from multiple different perspectives, ranging from a laboratory engineer to a degree programme coordinator. With European Union funded research projects initialized during that decade, the author also had the opportunity to participate in multiple research papers concentrating to the field of cybersecurity education. Thus, the topic of this dissertation was identified even earlier than the timeline presents; the author will probably continue further research on the topic in the years to come.

5.1 Cyber Education

Based on the research conducted here, many of the learned elements could be utilised in the authors day-to-day work, even before the finalization of this dissertation. The research knowledge obtained was utilized while developing a newer curriculum and the courses within it at the Jamk University of Applied Sciences. Although during the research, as newer frameworks and degree programmes were published, the research questions were answered. In hindsight, the choice of beginning with one framework and not changing it throughout the process was deemed to be a successful choice.

RQ1: How should degree programmes utilize established frameworks and governmental guidance?

Given the research, there were not many degree programmes which clearly stated that they followed a certain framework for their curriculum structure. If they did, they were mainly located in the United States, similar to the NICE framework. At least in Finland, there were not too many public knowledge of frameworks being used for cybersecurity-oriented degree programmes. This was actually a survey question in Article X, where 81.25% of the participants were not aware of JSEC2017 or the NICE framework.

It was evident to the author that the European Qualifications Framework and its national counterpart, the National Qualifications Framework must be followed. Following these, the field-specific competence structures appeared to be either locally specified or tied to a field specific recommendation of competences. A similar phenomenon is evident in the author's own workplace: the generalized competence structure of the university and field-specific competences per degree programme.

The design model used in this dissertation was taken into use as the cybersecurity degree programme competence structure including the course descriptions of Jamk University of Applied Sciences. Unfortunately, in the change in the student management system from Asio to Peppi, these markings were not supported anymore in public course descriptions. The developed Power BI dashboard was left in place.

From among the current cybersecurity frameworks, the author would suggest choosing one and sticking with it, as the author did in this dissertation. The NICE framework was deemed to be useful in the University of Applied Sciences, which is regulated by the Finnish law to be more focused on industry, business, and regional development. Scientific Universities might consider some other frameworks more useful, such as the Cyber Security Body of Knowledge and its Knowledge Areas.

RQ1a: What competence foundations should cybersecurity education base on?

By acquiring knowledge and skills, the EQF deems the student to be competent and able to succeed at the work. The NICE framework can be thought of approaching this subject from the other way around – defining work and tasks and then writing out the required knowledge and skills. Both the frameworks define similar terms in *ability* (NICE framework) and *responsibility and autonomy* (EQF). Thus, the author feels that even by abiding to one, the curriculum developer would not cross the other.

This is also true with the combined usage of the EUR-ACE® framework. The ethical thinking, engineering design, and following competences were quite well documented in the NICE framework; however, using field specific language[1]. For the curriculum designer, the main issue in using field-specific frameworks is to cross-tabulate the competence structures to one another in a precise and documented manner. A sample of this procedure was demonstrated in Figure 28.

RQ1b: Which different categories of knowledge and skills should be emphasised on the degree?

This research question was answered through four different aspects: current curricula content situation at the national and international levels, theses conducted for the industry or science field, graduate work responsibility and employer expectations for cybersecurity recruits. The last two were not researched for master's degree students. Table 21 presents the standings of different categories from the overall research done on the bachelor's degree level.

TABLE 21 Summary of the bachelor's degree categories

NICE category	International[1]	Finland[2]	Theses[3]	Job responsibilities[4]	Recruitment modules[5]
Securely Provision	2nd	1st	1st	3rd	1st
Operate and Maintain	1st	2nd	5th	2nd	1st
Analyze	7th	3rd	6th	4th	4th
Oversee and Govern	3rd	3rd	2nd	6th	1st
Protect and Defend	4th	5th	3rd	1st	4th
Collect and Operate	6th	6th	3rd	7th	6th
Investigate	5th	7th	7th	5th	7th

[1] see Table 8
[2] see Table 13
[3] see Table 18
[4] see Figure 19
[5] see Figure 13

Table 21 provides an unbalanced view of the emphasis of each column. The conclusion of the dissertation would be that bachelor's degrees should concentrate on *Securely Provision*, *Operate and Maintain* and *Oversee and Govern* in cybersecurity studies. There is still a need for a concluding *Protect and Defend* course(s), as the main job responsibility lies in that category. The module choices of the

[1] e.g. K0003 - Knowledge of laws, regulations, policies and ethics as they relate to cybersecurity and privacy

recruiters supported this conclusion. Table 22 presents the standings of different categories from the overall research done on the master's degree level.

TABLE 22 Summary of the master's degree categories

NICE category	International[1]	Finland[2]	Theses[3]
Securely Provision	2nd	2nd	2nd
Operate and Maintain	1st	3rd	5th
Analyze	6th	1st	3rd
Oversee and Govern	3rd	2nd	1st
Protect and Defend	4th	5th	4th
Collect and Operate	7th	6th	6th
Investigate	5th	7th	7th

[1] see Table 8
[2] see Table 13
[3] see Table 18

Master's degree curriculums should concentrate on *Analyze* with *Oversee and Govern* and *Securely Provision*. *Operate and Maintain* is a category that has fallen in importance compared to the bachelor's degree curriculum. Moreover, when compared to the bachelor's degree, the active duty placed on *Protect and Defend* appears to be lower. This is evident between the degree levels; however, in this case there is no research on job responsibilities or recruitment course choices. Thus, additional research would be necessary to solidify this conclusion.

RQ2: How does the industry need and graduates align with given education?

It was evident from the research data that the most attractive employee would be an EQF-6 level graduate with cybersecurity certificates. Most of the employers seemed to be in the *Digital Services and Platforms* or *Telecomm Infrastructure* sectors. The companies mentioned earlier might even be subsidiaries of the latter metioned. *Defence*, *Health* and *Government* were also on the list; however, these had significantly lower numbers than the two mentioned earlier.

The research leaves a bit of an unoptimistic view on the need for the vocational education on cybersecurity. There was an researched and evident need for it. However, it was quite small. The author would recommend gaining additional cybersecurity certifications to validate the level of competence of the vocational degree holder. This would further enhance their possibilities of getting recruited.

Bachelor's and master's degrees were deemed most useful for acquiring a workplace in cybersecurity, which aligns with Finland's vision for education in 2030 (Ministry of Education and Culture, 2017). Higher education is needed for competent workforce to be available in cybersecurity. The author would recommend, based on this research, that students would focus on *Operate and Maintain* and *Securely Provision* on the bachelor's degree with a touch of *Protect and Defend* courses. This would directly align them with work place responsibilities.

Master's degree saw greater differences in education when analysed through an NICE framework. It was evident that Applied Sciences Universities clearly had more *Oversee and Govern* in their curricula. This is assumed to be because of the two year work experience requirement before this education track. Regular universities had more *Analyze* category courses as they were focused

on Scientific Research through research methodology and scientific publishing courses.

Possibilities for every higher education institution in Finland would lie in creating and offering more courses in the fields of *Protect and Defend*, *Collect and Operate* and *Investigate*. The cybersecurity exercise oriented courses are deemed to be very necessary for students based on the graduate work responsibilities. *Collect and Operate* aligns into the field of governmental intelligence and offensive cybersecurity. The *Collect* section would be an interesting field to mix in with courses or degrees in data-analytics and the latter *Operate* section is typically seen as a more 'entertaining' side of cybersecurity through ethical hacking and similar courses. If well established courses were more available in the curricula of Finland, based on the research within this dissertation, the author believes that all of the aforementioned courses would definitely have an active participant count.

RQ3: How can the overall quality of course implementations within a degree be enhanced?

At least in the field of cybersecurity MOOCs, the survey results presented in Table 20 were rather disappointing to the author. A similar quality inspection was not done for regular cybersecurity courses, but the disparity of cybersecurity course offerings within the curricula would suggest that the situation is not very much better in regular courses. This is a grim outlook of the situation, but a country the size of Finland could do better in creating a more cohesive track for cybersecurity education. One model for this was proposed in Kyberturvaaja[2] research and development program. Based on this research of the curricula in Finland, the results of the R&D project were not very widely taken into use within Finland. Nevertheless, from the perspective of the author of this dissertation, the project outcomes had promise.

The learning environments for these topics is an ongoing and active field of study. As this dissertation also partially covered the field of cyber range usage, the reason related to why platforms must be utilised would be a priority before deciding to place a course there. Bachelor's and even master's degree students might fare well in smaller environments at the beginning of their degree education. This all depends on the learning objectives defined for the course.

At the end of their education, it would be a good experience for all to utilize their learned competences and abilities at a cybersecurity exercise held at a cyber range with the main focus being on *Protect and Defend* to verify that the *'cyber domain is reliable and its functioning secured'*[3].

---

2 https://projects.tuni.fi/kyberturvaaja/

3 a slight variation of the original text in cyber security strategy of Finland 2013 (Secretariat of the Security Committee, 2013)

5.2 Trustworthiness of the research

In quantitative research, the aspects of internal and external validity, reliability and objectivity should be considered (Heikkilä, 2014; Eskola and Suoranta, 1998). In this dissertation, internal validity was handled through testing. Curricula were collected on several occasions from different sources with the same data structure. Multiple different calculation methods were experimented upon for use. These were discussed with several different researchers. There was uniform consensus to find a suitable one for each research paper. The data sets for these are open for inspection. The main relationship among the variables used was the relationship between the course and the lenghth of the curricula.

The external / international validity of the articles in this thesis is considered to be doubtful, as many of the research papers focus geographically on Finland. The same results might not extend to a different region. Periodical research should be performed to verify changes in, for example, workforce need. The main part of this research was to obtain an international curricula perspective and to compare these findings regionally. The author found similar findings in this research. Thus, the author would advise examining the papers done regionally in Finland and reproduce the research locally to verify transportability. One factor is also time as the research should be conducted periodically to witness change in e.g. workforce need in cybersecurity.

The level of reliability in this research is believed to be good, as curricula samples were taken from official publishing platforms of higher education institutions. The same phenomenon is apparent in publicly available theses. Further, employer surveys were conducted during a certain time frame to avoid experimenter bias.

Objectivity was the most difficult aspect of this dissertation as deciding the categories of, for example, courses and theses is based on the researchers understanding of the framework categories. This phenomenon was actualized when multiple researchers were conducting categorisation on the same data set. The presented attribute lists were one way to tackle this topic and opening the data sets to be available for external review before paper submission.

When discussing objectivity during the writing of the dissertation, it was relevant for the author to write conclusions based on the research performed rather than opinions that arose from the work history of the writer. This was kept in mind whilst writing, reviewing, and polishing numerous sections of this dissertation.

5.3 Further research

This dissertation paves way for numerous ideas for different research topics around the subject. However, a line had to be drawn to conclude this disserta-

tion. The following paragraphs offer possibilities for additional research.

A focused set of curricula could be selected to be periodically collected and analysed to measure the rate of change in the NICE framework categories. This could be done backwards in time as well to obtain a visualization of how the themes of the NICE framework are covered; and ascertain whether they are strengthening or weakening.

The course descriptions published have free-form fields of text specifying the course content. Such text fields could be collected for further text analysis through, for example, the attribute model presented in Article IX. This could be tied to the earlier research topic.

Mathematical principles of category weights could be improved rather than basing on averaging the course ECTS to the total ECTS count of the degree. Different fields of study; mandatory/core, speciality, or elective studies could also be further defined to match the calculations.

All of the above would benefit from the automation of curricula collection. Currently, the published data is organizationally dependant. A more sophisticated solution would be necessary to decrease the amount of hardwork in the collection and normalization of the data. Even though the solution was pondered upon, this tool would require multiple components to fit different publishing formats and, thus, was deemed too troublesome for the research objectives within this dissertation.

Open job vacancies could be systemically drawn from publishing platforms and analysed using the NICE framework work roles to obtain a statistical perspective into the recruitment needs of the industry. This would supplement the survey method that was used in Article IV.

Master's degree graduates should also be researched from the point of view of graduate work responsibility. This would further align the given education towards their actual work-life responsibilities. In this dissertation, this could only be discussed at the bachelor's degree level.

Curricula are merely templates from which the students actually choose and complete their studies. To get a realistic view of what actually was done in the degree programme, all the transcript of records from degree programme graduates would need to be collected. This is often tied very closely to the evaluation and personal identification information of the student and as such would be quite a sensitive topic for data collection. However, it would present an interesting research topic if sufficient data was collected from multiple organizations.

Lastly one could also perform the same analysis as that here through other frameworks related to cybersecurity education. This would provide an interesting perspective on how the different frameworks support the planning of cybersecurity education.

YHTEENVETO (FINNISH SUMMARY)

Digitalisoituvassa yhteiskunnassa kyberturvallisuuden merkitys on kasvanut jatkuvasti. Suomen kansallisessa kyberturvallisuusstrategiassa, sekä sen toimeenpano-, ja kehitysohjelmassa, kyberturvallisuuden osaaminen on laitettu merkittävään asemaan. Jo ensimmäinen strategia piti sisällänsä vaatimuksen kyberturvallisuuden opetuksen lisäämisestä kaikilla koulutusasteilla. Tämä kehitys vaatii myös koulutuksen järjestäjiltä ajankohtaista tutkimusta, jonka perusteella tarjota ja rakentaa johdonmukaisia tutkinto-ohjelmia kyberturvallisuuden alalle.

Viimeisen vuosikymmenen aikana on Suomalaisessa korkeakoulujärjestelmässä perustettu useita tutkinto-ohjelmia, jotka keskittyvät kyberturvallisuuteen. Työelämästä noussut tarve kyberturvallisuusalan työvoimalle asetti koulutuksen järjestäjille myös paineita julkaista kyberturvallisuusalan koulutusta usealla eri asteella; ammatillisessa koulutuksessa, ammattikorkeakoulututkintona ja ylempänä korkeakoulututkintona. Jo olemassa olleet tutkinto-ohjelmat sisälsivät kyberturvallisuuteen liitettäviä aiheita esimerkiksi tietoturvallisuuden kautta, mutta paine työvoimalle on ollut sen verran suuri, että suoraan alaan erikoistuvia tutkinto-ohjelmia Suomessa mitataan jo useissa sadoissa aloittavissa opiskelijoissa lukuvuonna 2022–2023. Elinikäinen oppiminen ja muut opintomahdollisuudet mukaan lukien on opiskelijoiden määrä varmasti jo tuhansissa.

Kuten yhteiskunnan digitalisaatio, myös kyberturvallisuus koskettaa valtavia määriä eri aloja. Tämä tekee kyberturvallisuuden opetuksesta haastavaa, jotta voidaan tunnistaa keskeiset aiheet opetettavaksi. Tässä tutkimuksessa kartoitettiin erillaisia teoreettisiä viitekehyksiä, johon kyberturvallisuuden opetuksen voisi perustaa. Tutkimuksessa valittiin yksi viitekehys, jota sovellettiin koko tutkimuksen ajan analysointityökaluna. Samaan kerättyyn dataan on täysin mahdollista käyttää myös muita viitekehyksiä.

Tutkimuksessa kerättiin tietoa olemassa olevien tutkinto-ohjelmien opetussuunnitelmista. Opetussuunnitelmat analysoitiin käyttämällä tutkimuksessa valittua viitekehystä. Viitekehyksen mallia käytettiin myös perustamaan tutkinto-ohjelman kompetenssirakenne alusta loppuun, jotta opiskelijalle muodostuisi mahdollisimman johdonmukainen oppimispolku. Näkökulmia aiheeseen haettiin myös opiskelijoiden opinnäytetöistä, valmistuneiden sijoittumisesta työelämään ja kyselyillä työelämältä. Tutkimuksen aikana tehtiin myös kehitysehdotuksia olemassa oleviin kyberturvallisuuden avoimiin verkkokursseihin (MOOCs) sekä kehitettiin esikyselyä opiskelijoille, jotka suorittavat oppimista kyberharjoitusympäristössä.

Tutkimuksen tuloksena valittu viitekehys osoittautui hyväksi tavaksi jäsennellä, analysoida ja pohjimmiltaan muodostaa kyberturvallisuuden opetusta. Tutkimustulosten perusteella tietyt viitekehyksen kategoriat olivat selkeästi enemmän edustettuina eri korkeakouluasteilla, joskin joidenkin kategorioiden tarjonta oli lähestulkoon olematonta tai erittäin vähäistä. Ammattikorkeakoulujen ja yliopistojen tarjoamissa tutkinto-ohjelmissa oli selkeästi eroavaisuuksia

kategorioiden välillä. Nämä olivat johdonmukaisia kunkin korkeakoulun lakisääteiseen tehtäävään liittyen. Työelämästä analysoidun tiedonperusteella kyberturvallisuusalalla parhaiten työllistyy ammattikorkeakoulutasoisella tutkinnolla, jonka lisäksi oli mahdollisesti suoritettu IT-alan sertifikaatteja osoittamaan kyvykkyyttä. Lisäksi selkeää oli tietyt painotukset viitekehyksen kategorioissa, johon opiskelijan tulisi painottaa opintojaan työllistyäkseen. Samaa tietoa voi käyttää opetussuunnitelmia valmistelevat, jotta tutkinto-ohjelmat palvelevat opiskelijan työllistymistä.

REFERENCES

Ahonen, A. K. 2021. Finland: Success through equity - the trajectories in pisa performance. In N. Crato (Ed.) Improving a Country's Education: PISA 2018 Results in 10 Countries. Cham: Springer International Publishing, 121–136. DOI: 10.1007/978-3-030-59031-4_6. URL:https://doi.org/10.1007/978-3-030-59031-4_6.

Altaf, S., Shehzad, A. & Akhtar, A. 2020. Finnish education system and its triumph in pisa: Lessons to learn for pakistan. Global Regional Review V, 479-487. DOI:10.31703/grr.2020(V-I).51.

Anderson, L., Krathwohl, D., Airasian, P., Cruikshank, K., Mayer, R., Pintrich, P., Raths, J. & Wittrock, M. 2001. A taxonomy for learning, teaching, and assessing : a revision of Bloom's taxonomy of educational objectives (Complete ed. edition). New York: Longman.

Armstrong, M. E., Jones, K. S., Namin, A. S. & Newton, D. C. 2020. Knowledge, skills, and abilities for specialized curricula in cyber defense: Results from interviews with cyber professionals. ACM Transactions on Computing Education 20 (4). DOI:10.1145/3421254. URL:https://doi.org/10.1145/3421254.

Azevedo, A., Apfelthaler, G. & Hurst, D. 2012. Competency development in business graduates: An industry-driven approach for examining the alignment of undergraduate business education with industry requirements. The International Journal of Management Education 10 (1), 12-28. DOI:https://doi.org/10.1016/j.ijme.2012.02.002. URL:https://www.sciencedirect.com/science/article/pii/S1472811712000031.

Barnett, D. 2011. Partnering Industry and Education for Curricular Enhancement: A Response for Greater Educational Achievement. URL:https://opensiuc.lib.siu.edu/ojwed/vol5/iss2/5/.

Bilgin, Y. 2017. Qualitative method versus quantitative method in marketing research: An application example at oba restaurant. In S. Oflazoglu (Ed.) Qualitative versus Quantitative Research. Rijeka: IntechOpen. DOI:10.5772/67848. URL:https://doi.org/10.5772/67848.

Bloom, B. S., Engelhart, M. B., Furst, E. J., Hill, W. H. & Krathwohl, D. R. 1956. Taxonomy of educational objectives. The classification of educational goals. Handbook 1: Cognitive domain. New York: Longmans Green.

Van den Broeck, L., De Laet, T., Lacante, M., Pinxten, M., Van Soom, C. & Langie, G. 2020. The effectiveness of a mooc in basic mathematics and time management training for transfer students in engineering. European Journal of Engineering Education 45 (4), 534–549. DOI:10.1080/03043797.2019.1641692. URL:https://doi.org/10.1080/03043797.2019.1641692.

Catota, F. E., Morgan, M. G. & Sicker, D. C. 2019. Cybersecurity education in a developing nation: the Ecuadorian environment. Journal of Cybersecurity 5 (1). DOI:10.1093/cybsec/tyz001. URL:https://doi.org/10.1093/cybsec/tyz001. (tyz001).

Craig, A. & Valeriano, B. 2016. Conceptualising cyber arms races. In Conceptualising cyber arms races. 2016 8th International Conference on Cyber Conflict, 141-158. DOI:10.1109/CYCON.2016.7529432.

Creswell, J. W. 2013. Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE.

Deaconu, A., Osoian, C., Zaharie, M. & Achim, S. A. 2014. Competencies in higher education system: an empirical analysis of employers' perceptions. Amfiteatru Economic Journal 16 (37), 857-873. URL:https://www.econstor.eu/handle/10419/168862.

Derntl, M. 2014. Basics of research paper writing and publishing. International Journal of Technology Enhanced Learning 6 (2), 105–123. DOI:10.1504/IJTEL.2014.066856. URL:https://www.inderscienceonline.com/doi/10.1504/IJTEL.2014.066856.

Eskola, J. & Suoranta, J. 1998. Johdatus laadulliseen tutkimukseen. Vastapaino.

Hajný, J., Levillain, O., Grigaliunas, S., Versinskiene, E., Bruze, E. & Zylius, R. 2020. Cybersecurity skills framework. SPARTA project.

Heikkilä, T. 2014. Tilastollinen tutkimus. Edita Publishing Oy.

Henriksen, A. 2019. The end of the road for the UN GGE process: The future regulation of cyberspace. Journal of Cybersecurity 5 (1). DOI:10.1093/cybsec/tyy009. URL:https://doi.org/10.1093/cybsec/tyy009.

Israel, M. J. 2015. Effectiveness of integrating moocs in traditional classrooms for undergraduate students. The International Review of Research in Open and Distributed Learning 16 (5). DOI:10.19173/irrodl.v16i5.2222. URL:https://www.irrodl.org/index.php/irrodl/article/view/2222.

Jacob, J., Peters, M. & Yang, T. A. 2020. Interdisciplinary cybersecurity: Rethinking the approach and the process. In K.-K. R. Choo, T. H. Morris & G. L. Peterson (Eds.) National Cyber Summit (NCS) Research Track. Cham: Springer International Publishing. Advances in Intelligent Systems and Computing, 61–74. DOI:10.1007/978-3-030-31239-8_6.

Jones, K. S., Namin, A. S. & Armstrong, M. E. 2018. The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. ACM Transactions on Computing Education 18 (3). DOI:10.1145/3152893. URL:https://doi.org/10.1145/3152893.

Jones, S. L., Collins, E. I. M., Levordashka, A., Muir, K. & Joinson, A. 2019. What is 'Cyber Security'? Differential Language of Cyber Security Across the Lifespan. In Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems. New York, NY, USA: Association for Computing Machinery. CHI EA '19, 1–6. DOI:10.1145/3290607.3312786. URL:https://doi.org/10.1145/3290607.3312786.

Karjalainen, M. & Kokkonen, T. 2020. Comprehensive cyber arena the next generation cyber range. In Comprehensive Cyber Arena The Next Generation Cyber Range. 2020 IEEE European Symposium on Security and Privacy Workshops, 11-16. DOI:10.1109/EuroSPW51379.2020.00011.

Karjalainen, M. 2020. Pedagogical Basis of Live Cybersecurity Exercises. Ph. D. Thesis. URL:http://urn.fi/URN:ISBN:978-951-39-8738-1.

Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R. & Shetty, S. 2021. Simulation for cybersecurity: state of the art and future directions. Journal of Cybersecurity 7 (1), tyab005. DOI:10.1093/cybsec/tyab005. URL:https://doi.org/10.1093/cybsec/tyab005.

Koskinen, I., Zimmerman, J., Binder, T., Redstrom, J. & Wensveen, S. 2011. Design Research Through Practice : From the Lab, Field, and Showroom. Elsevier Science & Technology.

Kuusisto, T. 2014. Kybertaistelu 2020. Maanpuolustuskorkeakoulu. URL:https://www.doria.fi/handle/10024/103034.

Kähkönen, E. & Hölttä-Otto, K. 2022. From crossing chromosomes to crossing curricula – a biomimetic analogy for cross-disciplinary engineering curriculum planning. European Journal of Engineering Education 47 (3), 516–534. DOI:10.1080/03043797.2021.1953446. URL:https://doi.org/10.1080/03043797.2021.1953446.

Lehtiranta, L., Junnonen, J.-M., Kärnä, S. & Pekuri, L. (Ed.) 2015. Designs, Methods and Practices for Research of Project Management. Gower Applied Business Research, 95–106.

Lehto, M., Limnell, J., Kokkomäki, T., Pöyhönen, J. & Mirva, S. 2018. Strategic management of cyber security in Finland. Prime Minister's Office. URL:https://tietokayttoon.fi/documents/10616/6354562/28-2018-Kyberturvallisuuden+strateginen+johtaminen..pdf/efea3c33-3c74-4cf6-b237-d49b4f10ab83/28-2018-Kyberturvallisuuden+strateginen+johtaminen..pdf.

Lehto, M. & Limnéll, J. 2021. Strategic leadership in cyber security, case Finland. Information Security Journal: A Global Perspective 30 (3), 139–148. DOI:10.1080/19393555.2020.1813851. URL:https://doi.org/10.1080/19393555.2020.1813851. (Publisher: Taylor & Francis).

Limnéll, J. 2016. The cyber arms race is accelerating – what are the consequences? Journal of Cyber Policy 1 (1), 50–60. DOI:10.1080/23738871.2016.1158304. URL:https://doi.org/10.1080/23738871.2016.1158304.

May, D., Morkos, B., Jackson, A., Hunsu, N. J., Ingalls, A. & Beyette, F. 2022. Rapid transition of traditionally hands-on labs to online instruction in engineering courses. European Journal of Engineering Education 0 (0), 1-19. DOI:10.1080/03043797.2022.2046707. URL:https://doi.org/10.1080/03043797.2022.2046707.

McCormack, B., Magowan, R., O'Donnell, D., Phelan, A., Štiglic, G. & van Lieshout, F. 2022. Developing a person-centred curriculum framework: a whole-systems methodology. International Practice Development Journal 12 (Suppl), 1–11. DOI:10.19043/ipdj.12suppl.002. URL:https://www.fons.org/library/journal/volume12-suppl/article2.

McIntosh, J. 2019. Pisa country rankings valid? results for canada and finland. Scandinavian Journal of Educational Research 63 (5), 670-678. DOI:10.1080/00313831.2017.1420687. URL:https://doi.org/10.1080/00313831.2017.1420687.

Mikk, J. 2015. Explaining the difference between pisa 2009 reading scores in finland and estonia. Educational Research and Evaluation 21 (4), 324-342. DOI:10.1080/13803611.2015.1062400. URL:https://doi.org/10.1080/13803611.2015.1062400.

Nai Fovino, I., Neisse, R., Hernandez Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M. & Lazari, A. 2019. A Proposal for a European Cybersecurity Taxonomy. Publications Office of the European Union. DOI:10.2760/106002.

Nai Fovino, I., Neisse, R., Lazari, A., Ruzzante, G., Polemi, N. & Figwer, M. 2018. European Cybersecurity Centres of Expertise Map - Definitions and Taxonomy. Publications Office of the European Union. DOI:10.2760/622400.

Newhouse, W., Keith, S., Scribner, B. & Witte, G. 2017. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. DOI:10.6028/nist.sp.800-181. URL:http://dx.doi.org/10.6028/NIST.SP.800-181.

Niemelä, J. 2019. Kyberturvallisuusalan työvoiman kysyntä, saatavuus ja kehittäminen vastaamaan työvoiman tarvetta Suomessa. University of Jyväskylä. Master's Thesis. URL:https://jyx.jyu.fi/handle/123456789/64289.

Nikolic, S., Ros, M., Jovanovic, K. & Stanisavljevic, Z. 2021. Remote, simulation or traditional engineering teaching laboratory: a systematic literature review of assessment implementations to measure student achievement or learning. European Journal of Engineering Education 46 (6), 1141-1162. DOI:10.1080/03043797.2021.1990864. URL:https://doi.org/10.1080/03043797.2021.1990864.

Paananen, R. 2021. Cyber Security Development Programme. URL:http://urn.fi/URN:ISBN:978-952-243-599-6.

Parekh, G., DeLatte, D., Herman, G., Oliva, L., Phatak, D., Scheponik, T. & Sherman, A. 2018. Identifying Core Concepts of Cybersecurity: Results of Two Delphi Processes. DOI:10.1109/TE.2017.2715174.

Parrish, A., Impagliazzo, J., Raj, R. K., Santos, H., Asghar, M. R., Jøsang, A., Pereira, T. & Stavrou, E. 2018. Global perspectives on cybersecurity education for 2030: A case for a meta-discipline. In Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education. New York, NY, USA: Association for Computing Machinery. ITiCSE 2018 Companion, 36–54. DOI:10.1145/3293881.3295778. URL:https://doi.org/10.1145/3293881.3295778.

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A. & Witte, G. 2020. NIST Special Publication 800-181 Revision 1. National Institute of Standards and Technology. DOI:https://doi.org/10.6028/NIST.SP.800-181r1.

Rahman, T. F. b. A., Anuar, N., Said, R. F. M. & Safiai, S. 2018. How a proposed ratio of bloom's taxonomy enhances learning in c programming. European Proceedings of Social and Behavioural Sciences Technology & Society: A Multidisciplinary Pathway for Sustainable Development. DOI:10.15405/epsbs.2018.05.50. URL:https://www.europeanproceedings.com/article/10.15405/epsbs.2018.05.50.

Rantapelkonen, J. & Salminen, M. 2013. The fog of cyber defence. Maanpuolustuskorkeakoulu. URL:https://www.doria.fi/handle/10024/88689.

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M. & Peersman, C. 2018. Scoping the Cyber Security Body of Knowledge. DOI:10.1109/MSP.2018.2701150.

Rosewell, J. & Jansen, D. 2014. The OpenupEd quality label: Benchmarks for MOOCs. The International Journal for Innovation and Quality in Learning 2 (3), 88–100.

Sampson, L. K. Y., Kumi, J.-N. & Maxwell, S. K. 2022. Redesigning the college of education curriculum to meet the learner centered approach needs of the pre-service teacher for effective implementation of the standard based curriculum in ghana. Journal of Education and Practice 6 (6), 1–15. DOI:10.47941/jep.1077. URL:https://carijournals.org/journals/index.php/JEP/article/view/1077. (Number: 6).

Schneider, K. 2019. What does competence mean? Psychology 10, 1938-1958. DOI:10.4236/psych.2019.1014125.

Simola, H., Kauko, J., Varjo, J., Kalalahti, M. & Sahlström, F. 2017. Dynamics in Education Politics and the Finnish PISA Miracle. DOI:10.1093/acrefore/9780190264093.013.16.

Sobral, S. 2021. Bloom's taxonomy to improve teaching-learning in introduction to programming. International Journal of Information and Education Technology 11, 148-153. DOI:10.18178/ijiet.2021.11.3.1504.

Soh, K. 2014. Finland and singapore in pisa 2009: similarities and differences in achievements and school management. Compare: A Journal of Comparative and International Education 44 (3), 455-471. DOI:10.1080/03057925.2013.787286. URL:https://doi.org/10.1080/03057925.2013.787286.

Stracke, C. M., Tan, E., Texeira, A., Vassiliadis, B., Kameas, A., Sgouropoulou, C. & Vidal, G. 2018. Quality Reference Framework (QRF) for the Quality of MOOCs. http://www.mooc-quality.eu/QRF.

Švábenský, V., Vykopal, J. &Čeleda, P. 2020. What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. URL:https://doi.org/10.1145/3328778.3366816.

Ukwandu, E., Farah, M. A. B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., Tachtatzis, C., Bures, M., Andonovic, I. & Bellekens, X. 2020. A Review of Cyber-Ranges and Test-Beds: Current and Future Trends. DOI:10.3390/s20247148. URL:https://www.mdpi.com/1424-8220/20/24/7148.

Välijärvi, J., Linnakylä, P., Kupari, P., Reinikainen, P. & Arffman, I. 2002. The Finnish success in PISA—and some reasons behind it. OECD PISA.

Üstün, U. & Eryilmaz, A. 2018. Analysis of finnish education system to question the reasons behind finnish success in pisa. Studies in Educational Research and Development 2 (2), 93 - 114.

ACM, IEEE-CS, AIS SIGSEC and IFIP 2017. Cybersecurity Curricula 2017, (CSEC2017), Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. URL:https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf.

ACM and IEEE-CS 2020. Computing Curricula 2020, CC2020, Paradigms for Future Computing Curriculai. URL:https://cc2020.nsparc.msstate.edu/.

Council of the European Union 2017. Council Recommendation on the European Qualifications Framework for lifelong learning. Official Journal of the European Union. URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017H0615(01).

ENAEE 2021. EUR-ACE Framework Standards and Guidelines. URL:https://www.enaee.eu/wp-content/uploads/2022/03/EAFSG-04112021-English-1-1.pdf.

European Comission 2003. EUR-Lex - 32003H0361. URL:https://eur-lex.europa.eu/eli/reco/2003/361/oj.

European Commission 2017. ECTS Users' Guide 2015. Publications Office. DOI: doi/10.2766/87592.

European Council 2017. Council recommendation of 22 May 2017 on the European Qualifications Framework for lifelong learning. URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017H0615%2801%29.

ENISA 2016. Definition of Cybersecurity - Gaps and overlaps in standardisation. URL:https://www.enisa.europa.eu/publications/definition-of-cybersecurity.

Finnish Government 2020. Oppivelvollisuuslaki. URL:https://www.finlex.fi/fi/laki/alkup/2020/20201214.

Finnish National Agency for Education 2021. Vocational qualification in Information and Communications Technology, 102. URL:https://eperusteet.opintopolku.fi/eperusteet-service/api/dokumentit/8201493.

ISO 2018. ISO/IEC 27000:2018. URL:https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/39/73906.html.

ITU-T 2008. X.1205 Overview of cybersecurity. URL:https://www.itu.int/rec/T-REC-X.1205-200804-I.

UNESCO Institute for Statistics 2015. International Standard Classification of Education Fields of education and training 2013. UNESCO Institute for Statistics, 96. DOI:10.15220/978-92-9189-179-5-en. URL:http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-fields-of-education-and-training-2013-detailed-field-descriptions-2015-en.pdf. Accessed on 2–0–22-04-01.

EIT Digital 2020. Development of Secure Embedded Systems Specialization. https://www.coursera.org/specializations/embedded-systems-security, accessed 21 Jan 2020.

Finnish Government 2019. Programme of Prime Minister Sanna Marin's Government. URL:https://julkaisut.valtioneuvosto.fi/handle/10024/161935.

Google 2020. Managing Security in Google Cloud Platform. https://www.coursera.org/learn/managing-security-in-google-cloud-platform.

Karlstad University 2020. Privacy by Design. https://www.kau.se/cs/pbd.

Ministry of Education and Culture 2017. Korkeakoulutus ja tutkimus 2030-luvulle; Taustamuistio korkeakoulutuksen ja tutkimuksen 2030 visiotyölle. URL:https://julkaisut.valtioneuvosto.fi/handle/10024/160456.

Ministry of Education and Culture 2021a. Ammattikorkeakouluille myönnetyt uudet lisäpaikat vuodelle 2022. URL:https://okm.fi/documents/1410845/4392480/AMK-uudet+lis%C3%A4paikat+2022.pdf/7a9befe4-

8019-135c-fbb1-381094f5d67f/AMK-uudet+lis%C3%A4paikat+2022.pdf?t=1639985949325.

Ministry of Education and Culture 2021b. Korkeakoulujen aloituspaikkoja lisätään vuodelle 2022 noin 2 300:lla - OKM. URL:https://okm.fi/-/korkeakoulujen-aloituspaikkoja-lisataan-vuodelle-2022-noin-2-300-lla.

Ministry of Education and Culture 2021c. Yliopistoille myönnetyt uudet lisäpaikat vuodelle 2022. URL:https://okm.fi/documents/1410845/4392480/YO-uudet+lis%C3%A4paikat+2022.pdf/99457406-0502-9d05-c081-ad683d6f76d1/YO-uudet+lis%C3%A4paikat+2022.pdf?t=1639985924200.

National Cyber Security Centre 2020. Education and Skills, Cyber Security Body of Knowledge. https://www.ncsc.gov.uk/section/education-skills/cybok.

Royal Holloway 2020. Information Security: Context and Introduction. https://www.coursera.org/learn/information-security-data.

Secretariat of the Security Committee 2013. Finland's Cyber security Strategy, Government Resolution 24.1.2013. URL:https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

Secretariat of the Security Committee 2019. Finland's Cyber security Strategy, Government Resolution 3.10.2019. URL:https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf.

Technische Hochschule Luebeck 2020. Netzwerksicherheit. https://www.oncampus.de/weiterbildung/moocs/netzwerksicherheit.

The Finnish National Agency for Education and Ministry of Education and Culture 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. URL:https://www.oph.fi/sites/default/files/documents/report_on_the_referencing_of_the_finnish_national_qualifications_framework.pdf.

University of Helsinki and F-Secure 2020. Cyber Security Base with F-Secure, Academic. https://cybersecuritybase.mooc.fi/.

APPENDIX 1 CYBERSECURITY COURSE NAMES AND APPEARANCES

As also visible in the finnish language version of Article PX.

Course Name	ECTS	appearances
Advanced Project on Networking and Cyber Security	5	1
Aloitusprojekti, kyberturvallisuus	5	1
Application Security	5	1
Auditing and Testing Technical Security	5	1
Auditointi, Penetraatiotestaus ja Red Team -toiminta	5	3
CCNA: Network Security	5	1
CTF -haaste	5	1
Cyber Security	5	2
Cyber Security Exercise	5	1
Cyber Security Implementation in Practice	5	1
CyberOps Associate	5	1
Cybersecurity Analyst	5	1
Cybersecurity and data privacy	3	1
Cybersecurity for Industrial Networks	5	1
Cybersecurity Hackathon Project	3	1
Cybersecurity Project	5	1
Cybersecurity Situational Awareness	5	2
Cybersecurity Working Life Practices	2	1
Data Protection and Privacy	5	1
Data Security	5	1
Digitaalinen forensiikka ja poikkeamienhallinta	5	1
Digiturva ja kyberhygienia	5	1
Edistynyt forensiikka	5	1
Eettinen hakkerointi	5	2
E-FIRST -verkkokurssi -poliisina kybertoimintaympäristöissä	1	1
Enterprise Networking, Security and Automation	5	2
Enterprise Security and Practitioners	5	1
Esimies ja tietoturva	5	1
Etiikka ja vastuullisuus tiedolla johtamisessa	5	1
Git -versionhallinta ja Gitlab -projektien hallintaympäristö	1	1
Haittaohjelmien analysointi	5	1
Hyökkäykset ja puolustusmenetelmät sekä suojaaminen	5	3
Hyökkäävä kyberturvallisuus	5	2
Information Security Management	5	1
Information Security Risk Management	5	1
Information Security Testing and Assessment	5	2
Internet Infrastructure and Security	10	1

Introduction to Cybersecurity	5	1
Introduction to Information Security	5	2
IoT-tietoturva	5	1
Johdanto kyberturvallisuuteen	5	3
Johdatus tietoturvaan	5	2
Kehittynyt kyberturvallisuus	5	1
Koventaminen	5	2
Kyberturvallisuuden erikoiskurssi	5	1
Kyberturvallisuuden hallinta	5	2
Kyberturvallisuuden matematiikka ja fysiikka	5	1
Kyberturvallisuuden perusteet	5	2
Kyberturvallisuus	3	1
Kyberturvallisuus	4	3
Kyberturvallisuus I	5	1
Kyberturvallisuus II	5	1
Kyberturvallisuus ja liiketoiminta	5	1
Kyberturvallisuus pilviympäristössä	4	1
Kyberturvallisuus projekti	5	1
Kyberturvallisuusauditointi ja kyberhygienia	5	1
Kyberturvallisuusharjoituksen suunnittelu	5	1
Kyberturvallisuusharjoitus	5	1
Kyberturvallisuusharjoitusten perusteet	5	1
Kyberturvallisuusliiketoiminta	5	1
Kyberturvallisuusprojekti	5	1
Kyberturvallisuusprojekti 1	5	1
Kyberturvallisuusprojekti 2	5	1
Kyberturvallisuustoiminnot	5	1
Kyberuhkatieto ja data-analytiikka	5	4
Käytännön kyberturvallisuus	5	1
Linux käyttö ja hallinta	5	1
Lähiverkkojen perusteet ja turvallisuus	5	1
Network and Applications Security	5	1
Network Protocols and Security	5	1
Network Security	5	2
NG palomuurin hallinta	5	1
Offensiivinen kyberturvallisuus	5	1
Ohjelmistohaavoittuvuudet ja niiden hyväksikäyttö	5	1
Ohjelmistojen tietoturva	5	1
Ohjelmistotestaus	5	1
Ohjelmoinnin perusteet	5	1
Operational Security	5	2
Organisaation tietoturva	3	1
Organisaation tietoturva	5	1
Palomuurin perusteet	2	1
Penetraatiotestaus	5	1

Poikkeamien hallinta ja kyberturvakeskukset	5	3
Programming for networks and information security	5	2
Puolustava kyberturvallisuus	5	3
Salausmenetelmät	5	1
Salaustekniikat ja -järjestelmät	5	1
Security Fundamentals	5	1
Security Management in Cyber Domain	5	1
Sovellettu matematiikka: Kryptologia	3	1
Systems Security	5	1
Takaisinmallintaminen	5	1
Tekninen tietoturva	3	1
Tieto- ja kyberturvallisuuden hallinta	10	1
Tieto- ja kyberturvallisuus	5	1
Tietoliikenteen ja tietoturvan perusteet	5	1
Tietosuoja ja turvallisuus sosiaali- ja terveydenhuoltojärjestelmässä	5	1
Tietoturva	3	1
Tietoturva	5	2
Tietoturva IoT -ratkaisuissa	5	1
Tietoturva ja tietosuoja	5	1
Tietoturva ja tietosuoja digitaalisissa järjestelmissä	5	1
Tietoturva sovelluskehityksessä	5	1
Tietoturva, kyberturvallisuus ja etiikka	3	1
Tietoturvakontrollit	5	2
Tietoturvalaitteet	5	1
Tietoturvalliset järjestelmät	5	1
Tietoturvalliset yritysverkot	5	1
Tietoturvallisuus	5	2
Tietoturvan hallinta	5	1
Tietoturvan perusteet	5	1
Tietoturvan perusteet	5	2
Tietoturvan perusteet luottamuksesta lohkoketjuun	5	1
Tietoturvan riskien hallinta ja yksityisyyden suoja	5	1
Tietoturvan yleiset perusteet	3	1
Tietoturvaohjelmointi	4	1
Tietoturvatietoisuus	5	1
Tietoverkkojen ja tietoturvan perusteet	5	2
Tietoverkkojen kyberturvallisuus	5	3
Tietoverkkojen turvallisuus	5	1
Tietoverkot	5	1
Tietoverkot ja tietoturva	3	1
Tietoverkot ja tietoturva	5	1
Towards Data Mining	5	1
Tunkeutumistestaus	5	1
Turvalliset reititysverkot	5	1

Turvalliset tietoverkot	5	1
Turvalliset web-palvelut	5	1
Turvalliset yritysverkot	5	1
Turvallisten tietoverkkojen suunnittelu	5	1
Turvallisten tietoverkkojen ylläpito	5	1
Uhkien havannointi ja vastetoiminta	5	1
Uhkien metsästys	5	1
Web-sovellusten turvallisuus	5	1
Virtualization: Networks and Security	15	1

ORIGINAL PAPERS

PI

A DESIGN MODEL FOR A DEGREE PROGRAMME IN CYBER SECURITY

by

Karo Saharinen, Mika Karjalainen and Tero Kokkonen 2019

ICETC 2019: Proceedings of the 2019 11th International Conference on Education Technology and Computers (pp. 3-7), New York, NY, USA.

DOI: https://doi.org/10.1145/3369255.3369266
URN: https://urn.fi/URN:NBN:fi-fe202002216171

A Design Model for a Degree Programme in Cyber Security

Karo Saharinen
JAMK University of Applied Sciences
Piippukatu 2
40100 Jyväskylä
+358 50 410 4415
karo.saharinen@jamk.fi

Mika Karjalainen
JAMK University of Applied Sciences
Piippukatu 2
40100 Jyväskylä
+358 40 574 8012
mika.karjalainen@jamk.fi

Tero Kokkonen
JAMK University of Applied Sciences
Piippukatu 2
40100 Jyväskylä
+358 50 438 5317
tero.kokkonen@jamk.fi

ABSTRACT

The need for skillful cyber security workforce has increased dramatically during the last ten years. The contents of the degree programmmes have not been able to respond to this need adequately and the curriculum contents have not always met the industry s knowledge needs.

In this paper, we describe a model for designing a degree programme in Cyber Security. We establish the guiding frameworks and requirements within the European Union for a degree programme. Given the researched background, we propose a systematic way to implement knowledge, skill and competence objectives to a degree programme by using generally accepted frameworks. The framework targets engineering education in information technology, cyber security given on university level.

By having a well-established model for the degree programme, the private and public sector can flourish by having competent personnel at their use as employees.

CCS Concepts

• Social and professional topics → Professional topics → Computing education → Model Curricula

Keywords

Cyber Security, Education, Competence, Skill, Knowledge, European Qualifications Framework, Degree Programme

1. INTRODUCTION

Workforce need for Cyber Security professionals has grown in the field of information technology with a fast pace. ICASA White Paper on the State of Cyber Security 2019 reports that the need for technical cyber security personel is rising and enterprises are struggling to fill their open positions [1]. According to the research from $(ISC)^2$ Cybersecurity Workforce Study report, the worker gap is 142 000 in Europe, the Middle East and Africa [2].

The education sector is under pressure to fulfil the needs to train competent workforce for the needs of industry. According to Burley et al. [3], cyber security degree programs are seen to be undeveloped. It seems that there is a lack of university level education in the field of cyber security. Cohen et al. pointed out in their paper that it is essential to recognize the demanded skills needed in government, industry and company levels [4]. Ciampa et al. argued in their paper that keeping the curricula up to date in relation to industry needs is very challenging [5] due to the fast development of ICT technology. Hence, threat vectors in cyber security also develop and change very rapidly.

CSIS - Center for Strategic International Studies - publication from January 2019 shows critique to the education system about how Cyber Security is organized in the Education systems: "Organizations are also frustrated by the current cyber security education ecosystem, which lacks common metrics or rankings to help employers understand what programs, certifications, and degrees are the most effective." [6]. Raj et al. argue in their paper that it is crucial to standardize the cyber security curricula and the expected board of skills needs to be defined based on cyber security domain needs [7]. It can be undeniably said that there is a need for clear frameworks that describe the competence needs of the substance. After describing the skill needs, the model can be modeled under the curriculum to be built, which will ensure that the curriculum responds to the industry s competence needs and focuses sufficiently on the intended area of expertise.

In this paper, we researched the frameworks within Cyber Security education sector and the general frameworks regulating and guiding academic education in the area of the European Union. These frameworks are presented in chapter 2. The proposed model for designing a degree programme is established in chapter 3, and examples are given in chapter 4. Finally, we conclude with remarks on future research that should be conducted in this area.

2. EDUCATIONAL FRAMEWORKS

2.1 Frameworks in the European Union

Within European Union the European Qualifications Framework EQF [8] EQF categorizes qualifications and competences into eight different levels, from EQF Level 1 to EQF Level 8. EQF also defines the characteristics of education to Knowledge, Skills and Competence, the explanations of which are given in table 1.

Table 1. EQF terminology [8]

Skills	means the ability to apply knowledge and use know-how to complete tasks and solve problems. In the context of the EQF, skills are described as cognitive involving the use of logical, intuitive and creative thinking or practical (involving manual dexterity and the use of methods, materials, tools and instruments)
Knowledge	means the outcome of the assimilation of information through learning. Knowledge is the body of facts, principles, theories and practices that is related to a field of work or study. In the context of the EQF, knowledge is described as theoretical and/or factual
Competence	means the proven ability to use knowledge, skills and personal, social and/or methodological abilities, in work or study situations and in professional and personal development

To harmonize, increase quality and enable student possibilities for multinational education within the EU, the member states are required to publish National Qualifications Frameworks [9]. These NQFs describe how current degree programmes within a member state map to the level requirements of the EQF.

ECTS User's Guide [10] describes and gives recommendations how degree programme supporting documents should be written.

This is to promote transparency and transferability of studies within the European Higher Education Area (EHEA .

European Network for Accreditation of Engineering Education ENAEE gives out a framework for engineering education that ensures quality in all branches of engineering education [11]. EUR-ACE® label is awarded to degree programmes as a sign of quality of the degree programme. EUR-ACE categorizes the Programme Outcomes into eight learning areas, which are same for both the Master's Degree and the Bachelor's Degree:

- Knowledge and Understanding - KU
- Engineering Analysis - EA
- Engineering Design - ED
- Investigations - IN
- Engineering Practice - EP
- Making Judgements - MJ
- Communication and Team-working - CT
- Lifelong Learning – LL

Additionally, in the home country of the writers, the Finnish Cyber Security strategy insists that cyber security skills should be a part of all education levels of the Finnish education system [12].

2.2 Education Frameworks within the Cyber Security

Cybersecurity education Joint Task Force (JTF) has launched curriculum guidelines for post-secondary degree programs in cybersecurity [3] where the Association for Computing Machinery ACM), IEEE Computer Society (IEEE-CS) and Association for Information Systems Special Interest Group on Information Security and Privacy AIS SIGSEC) combined their views on curriculum development. The report also takes into account the different knowledge areas of cyber security. The report also presents well the wide range of knowledge's and the complexity of cyber security as it also has to take into account the relation to the IT environment where the needed cyber security skills are applied. Thus, in curriculum development one needs to accurately select the skills and abilities that one is aiming to educate. The overall picture of cyber security is too wide to be covered by one curriculum.

Internationally recognized accreditation body for engineering programs ABET) has proposed the accreditation criteria for cybersecurity [13].

In Comprehensive National Cybersecurity Initiative [14] US President Barack Obama recognized cybersecurity as a critical challenge of economic and national security. By that recognition National Initiative for Cybersecurity Education NICE) was initiated with the idea that an important resource in cyber resilience are the people with appropriate skills [15].

NICE framework is published by The National Institute of Science and Technology (NIST [16]. Fundamentally NICE originates and focuses on the US; however the global nature of cyberspace is noticed there by partnering and global communities [15].

NICE framework describes and categorizes the work in cybersecurity into Work Roles and tasks assigned to those Work Roles. Those tasks require certain Knowledge, Skills and Abilities shortened as KSAs. With the mapping of KSAs to work roles, Educators can have awareness of how to map them into current course curricula. As stated in [15] "*Educators and trainers can use the framework to help answer these critical questions: What am I preparing my students for? What knowledge and skills do they need? What should I be teaching?".* In this study, that mapping is carried out as the design approach for a Degree Programme in Cyber Security.

The National Security Agency in the United States recognises two types of Centers of Academic Excellence (CAE): one in Cyber Defence (CAE-CD) and one in Cyber Operations (CAE-CO). NSA lists these degree programmes on their webpages, acknowledging the degree programme's quality, however, NSA does not directly fund the degree programmes. [17]

Cyber Defence CAE-CD consists of Knowledge Units. These Knowledge Units have been assigned to fit into NICE Framework Categories [18]. The Knowledge Units are for example:

- Cybersecurity Principles - SPY
- Basic Cryptography - BCY
- Security Program Management - SPM
- Basic Cyber Operations - BCO

Cyber Operations has only the criteria for measurement according to NSA [19] [20] but no valid Knowledge Units could be found during the writing of this paper. National Cyberwatch Center of the United States hands out a guide for mapping degree programme courses to the Knowledge Units of CAE-CD [21]. Based on the presentation "What They Are Teaching Kids These Days - Comparing Security Curricula and Accreditations to Industry Needs" at Black Hat 2017 [22], the degree field of the United States is in discussion how to implement Cyber Security in to their degree programs.

3. PROPOSED MODEL FOR DESIGNING A DEGREE PROGRAMME IN CYBER SECURITY

Given the developments of different frameworks into the field of Cyber Security, we propose the following model for Educational Organizations given in figure 1.

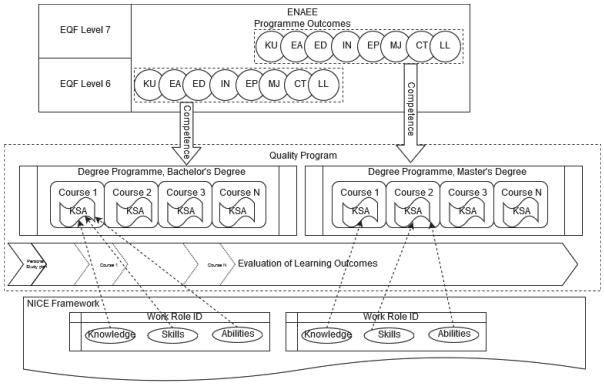


Figure 1. Model for Cyber Security Education Framework

The Programme Outcomes of ENAEE are described as competences of the degree programme. In order to achieve these

ICETC, 11th International Conference on Education Technology and Computers, October 28-31, 2019, Amsterdam, Netherlands.

DOI: http://dx.doi.org/10.1145/12345.67890

outcomes the courses are mapped to develop these competences accordingly to their degree level. Degree levels are mapped to the European Qualifications Framework according to National Qualifications Framework.

NICE Framework gives strict Work Role ID's that demand the development of certain Knowledge, Skills and Abilities to perform in given tasks assigned to the Work Role ID. These KSAs should be distributed as learning outcomes for the courses within the degree programme. These outcomes are also mapped to competences.

The development of the learning situations, laboratory exercises and types of assessment is left for the given course lecturer to choose the pedagogical solutions, which might include e.g. personal or group assignments, presentations, essays and exams.

Nonetheless the assignments should always develop the learning outcomes of the course. In addition, whatever evaluation method is used, it should assess the students' capability in the given NICE Knowledge, Skill or Ability.

4. RESULTS

4.1 Competences

Competences should be mapped to different courses as described earlier in chapter 2. The ECTS User's Guide also promotes that these should be recorded as the learning outcomes of the programme. In our course descriptions these are seen as the competences -field.

In table 2, we present our mapping of the ENAEE competence model and how it is brought down to our Master's Degree courses in our degree programme at JAMK University of Applied Sciences [23].

Table 2. Competence Mapping to Courses

Cyber Security, Master's Degree	ECTS	KN	EA	ED	IV	ER	CT	LL
Security Management in Cyber Domain	5	X	X					
Cyber Security Implementation in Practice	5		X	X				
Auditing and Testing Technical Security	5				X	X		
Cyber Security Exercise	5						X	X

In our model the last course, Cyber Security Exercise, summarizes the degree programme and promotes life-long learning competence. The student, under the guidance of an educator, can evaluate all the earlier competences in the exercise, run in a safe learning environment.

Given table 2, the following chapters give examples as a case study for the Cyber Security Implementation in Practice course [24].

4.2 Learning Objectives

The learning objectives in our model are a double-edged sword. In the ENAEE competence model, we have generalized competences that every engineer should possess. In NICE framework, we have very specific tasks that competent personnel should handle in the field of Cyber Security. The Learning Objectives in the course description should have the best of both worlds.

Cyber Security Implementation in Practice course [24] has had cryptography as a field of implementation: How are mathematical algorithms are written in different computer languages and how cryptographic material is stored and used in computer systems? This learning objective is tied to two different work roles (as an example) in NICE:

- Cyber Defense Analyst (PR-CDA-001)
  - Knowledge of cryptography and cryptographic key management concepts, K0019
- Communications Security (COMSEC) Manager (OV-MGT-002
  - Knowledge of encryption algorithms, K0018
  - Skill in using Public-Key Infrastructire PKI) encryption and digital signature capabilities into applications e.g. S/MIME email, SSL traffic), S0138
  - Ability to manage Communications Security COMSEC) material accounting, control and use procedure, A0165

In the ENAEE competence model, these tie to Engineering Analysis: how do the algorithms work and are written? The understanding of what different dependencies computer systems have in the written cryptographic libraries. They are also bound to Engineering Design competence on how to manage the cryptographic material in different computer systems and how it is created, distributed and used within the organization. This is summarized by the Learning Objective of Cryptography in Computer Systems.

Thus, the KSAs that NICE framework presents are mapped to learning objectives that are presented in the curriculum's course description in the learning outcomes -field.

4.3 Learning Situations & Assessment

Given student assignments should reflect the learning objectives. In the Cyber Security Implementation in Practice -course, the cryptography topic is further delved into with having lectures on the subject, classroom implementations as step-by-step guides followed by a research/implementation paper written on the chosen topic by the student. The written paper is then peer-reviewed and graded in the course by a fellow student. The lecturer grades the paper, multiple peer reviewers grade the paper, and the grade is then given for the whole assignment using a mathematical equation agreed at the start of the course.

Lectures increase knowledge, but also by writing and peer reviewing the student's understanding is further enhanced. Step-by-step classroom implementation enhances the theory into implementation skills, and the given implementation or research project enhances the ability to take this knowledge and skills into use. Understanding of the phenomenon further enhances as the students peer review each other's work.

As stated earlier, the learning situations can be from lectures to increase Knowledge and Understanding, to Investigations on researching and writing research/implementation papers, however, to enhance Communications and Team-working, full cyber security exercises could be run by the degree programme.

The assessment should concentrate on the KSAs assigned for the course and also be visible to the students in the course description. Different taxonomies such as Bloom's [25] or Solo's [26] Taxonomy could be used for assessing the levels of learning.

Technical competences were highly demanded in the background literature [1] [2] [4]. Based on our experience, a technical cyber range should be implemented to fully grasp the concepts of Cyber Security. Individual laboratory exercises can, in our opinion, develop the understanding and skills of some technical detail; however, cyber security often covers the interdependency of multiple technical details. Such interdependency, and resilience to withstand problems facing that interdependency, can only be taught in a realistic cyber environment, often called a cyber range.

At JAMK University of Applied Sciences in the Master's Degree programme [23], the competences are developed and can be

publicly viewed. In addition, different courses can be further examined on what NICE KSAs they develop [27] [24] [28] [29].

Quality of the Degree programme should be monitored by the Quality Program within the Education Organization. In the European Union we recommend official accreditation programs such as ENAEE EUR-ACE® -label.

5. DISCUSSION

As the need for cyber security expertise grows in the industry, the need for an up-to-date degree program also increases. It is vital that when building the curriculum, the degree program should use some existing generally accepted framework researched from the industry. As the field of cyber security is broad, these frameworks help to focus on the learning objectives in the curriculum.

By providing good education on a well-established model, we can provide students a with a well-organized study path and the industry with clear visibility on the developed competences of the student. Increasing the performance of both the student and the industry.

Thus, we have mapped the EQF framework into our curricula and accredited one of the curricula by ENAEE, EUR-ACE –label. In this research paper, we mapped the curriculum courses to NICE framework to ensure that our degree programme is up-to-date and the education meet the needs of the industry. NICE framework is an extensive and multidimensional frame that can be used as a guideline for scoping the degree program and to ensure that the learning outcomes meet the industry demands.

Given the wide variety of different frameworks, some more specified to cyber security than others, the terminology within the frameworks overlaps, has different meanings and the interpretation is left to the reader. One example is Knowledge from the EQF which translates in ENAEE as Knowledge and Understanding. Another is Abilities in the NICE Framework, while EQF only recognizes Knowledge, Skills and Competence.

One inconsistency of the NICE Framework is that one singular knowledge is too specific and another one is too broad. As an example of this, the Knowledge of computer algorithms K0015 is very abstract. However, encryption algorithms do not count as computer algorithms as they are categorized as a different Knowledge's K0018)?

In our opinion, the knowledges expand from EQF level to another, further deepening the students' grasp of the concept. Thus, even though it isn't a part of the learning outcomes of a course, or an item of assessment, it should not be completely discarded from the course. This gives many interpretation problems for the teacher of the course and might be seen as an inconsistency of the degree programme.

In addition, some courses (e.g. the Cyber Security Exercise [27]) in the degree program, are so vast that they develop multitude of different knowledge, skills and abilities. These cannot be all evaluated within the course but are known to develop during the course. These cases are problematic to describe in the course description.

6. FUTURE WORK

Cyber Security is taught in the area of the EU; however future research should be made to study different competence models and course descriptions within those educational organizations. We know that in the area of ICT the labor force can move globally; hence, the research should also compare degree programs between the EU and for example USA or Asia.

One aspect for the future research is also to study how the students achieve the NICE KSA skills, brought down to the degree programme by this model, by conducting a survey study with the students attending the programme. In the survey, the student experience of the learning outcomes could be measured to reflect the NICE KSAs given for the course.

In addition, the workforce needs change based on the physical locations of the education organization, thus maybe the frameworks of describing cyber security workforce should differentiate between the locations. Further market inquiries could be made on how to match the industry needs of a location.

7. REFERENCES

[1] State of Cybersecurity 2019: Current Trends in Workforce Development. 2019. White Paper. ICASA.

[2] $(ISC)^2$ Cybersecurity Workforce Study. 2018. $(ISC)^2$.

[3] Burley, D., Bishop, M., Buck, S., Ekstrom, J., Gibson, D., Hawthorne, E., Kaza, S., Yair, L., Mattord, H. and Parrish A. Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. 2015. DOI: http://doi.acm.org/10.1145/3184594

[4] Cohen, B., Albert, M.G. and McDaniel, E.A., 2018. The Need for Higher Education in Cyber Supply Chain Security and Hardware Assurance. International Journal of Systems and Software Security and Protection (IJSSSP), 9(2), pp.14-27.

[5] Ciampa, M. and Blankenship, R., 2019. Do Students and Instructors See Cybersecurity the Same? A Comparison of Perceptions About Selected Cybersecurity Topics. International Journal for Innovation Education and Research, 7(1), pp.121-135.

[6] The Cybersecurity Workforce Gap. 2019. CSIS.

[7] Raj, R.K. and Parrish, A., 2018. Toward Standards in Undergraduate Cybersecurity Education in 2018. Computer, 51(2), pp.72-75.

[8] COUNCIL RECOMMENDATION of 22 May 2017 on the European Qualifications Framework for lifelong learning. 2017. Retrieved March 20, 2019 from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017H0615(01)&qid=1552997420044&from=EN

[9] Government Decree on the National Framework for Qualifications and Other Competence Modules. 2017. Finland. Retrieved April 2, 2019 from https://www.oph.fi/download/182107_Government_Decree_120-2017_27.2.2017_.pdf

[10] ECTS Users' Guide. Publicatins Office of the European Union. DOI: 10.2766/87192

[11] EUR-ACE® Framework Standards and Guidelines. 2015. ENAEE. Retrieved April 1, 2019 from https://www.enaee.eu/wp-assets-enaee/uploads/2017/11/EAFSG-Doc-Full-status-8-Sept-15-on-web-fm.pdf

[12] Finland's Cyber security Strategy. 2013. Ministry of Defence. Retrieved March 21, 2019 from https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

[13] Proposed Accreditation Criteria for Cybersecurity Academic Programs, ABET, Inc., Nov. 2017, [online] Available:

www.abet.org/blog/news/abet-seeks-feedback-on-proposed-accreditation-criteria-for-cybersecurity-academic-programs

[14] United States. White House Office, Comprehensive National Cybersecurity Initiative, Apr 2010.

[15] C. Paulsen, E. McDuffie, W. Newhouse and P. Toth, "NICE: Creating a Cybersecurity Workforce and Aware Public," in *IEEE Security & Privacy*, vol. 10, no. 3, pp. 76-79, May-June 2012. DOI: 10.1109/MSP.2012.73

[16] National Initiative for Cybersecurity Education NICE) Cybersecurity Workforce Framework. 2017. NIST. DOI: https://doi.org/10.6028/NIST.SP.800-181

[17] Centers of Academic Excellence in Cybersecurity. Retrieved April 2, 2019 from https://www.caecommunity.org/content/what-is-a-cae

[18] Centers of Academic Excellence Cyber Defence Knowledge Units. Retrieved March 27, 2019 from https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf

[19] Criteria for Measurement for CAE in Cyber Operations Fundamental. NSA. Retrieved March 27,2019 from https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-fundamental/

[20] Criteria for Measurement for CAE in Cyber Operations Advanced. NSA. Retrieved March 27, 2019 from https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-advanced/

[21] A Guide for Mapping Courses to Knowledge Units. National Cyber Watch. Retrieved March 27, 2019 from https://www.nationalcyberwatch.org/ncw-content/uploads/2017/12/NCC_Resource_Guide_A_Guide_for_Mapping_Courses_to_Knowledge_Units_v2.pdf

[22] Olson, R. and Sanders, C. What They're Teaching Kids These Days. 2017. Retrieved March 27, 2019 from https://www.blackhat.com/docs/us-17/wednesday/us-17-Sanders-What-Theyre-Teaching-Kids-These-Days-Comparing-Security-Curricula-And-Accreditations-To-Industry-Needs.pdf

[23] Master's Degree Programme in Information Technology, Cyber Security. 2019. JAMK University of Applied Sciences. Retrieved April 18, 2019 from https://asio.jamk.fi/pls/asio/asio_rakenne_julkaisu.rakenne_komp_osaamisalue?ckohj_YTC_csuunt_99999_cvuosi_9S&caste_J_cark_2019-2020_lan=e

[24] Cyber Security Implementation in Practice. Course Information. JAMK University of Applied Sciences. Retrieved April 12, 2019 from https://asio.jamk.fi/pls/asio/asio_ectskuv1.kurssin_ks?ktun_YTCP0200&knro_ark_lan_e

[25] Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H. and Krathwohl, D. R. (1956 *Taxonomy of educational objectives Handbook 1: cognitive domain*. London, Longman Group Ltd.

[26] Biggs, J. and Collis, K. 1982. Evaluating the Quality of Learning The SOLO Taxonomy Structure of Observed Learning Outcome). Academic Press.

[27] Security Management in Cyber Domain. Course Information. JAMK University of Applied Sciences. Retrieved April 18, 2019 from https://asio.jamk.fi/pls/asio/asio_ectskuv1.kurssin_ks?ktun_YTCP0100_knro &lan=e&ark=

[28] Auditing and Testing Technical Security. Course Information. JAMK University of Applied Sciences. Retrieved April 18, 2019 from https://asio.jamk.fi/pls/asio/asio_ectskuv1.kurssin_ks?ktun_YTCP0300_knro &lan=e&ark=

[29] Cyber Security Exercise. Course Information. JAMK University of Applied Sciences. Retrieved April 12, 2019 from https://asio.jamk.fi/pls/asio/asio_ectskuv1.kurssin_ks?ktun_YTCP0400&knro_ark_lan_e

PII

ASSESSING CYBER SECURITY EDUCATION THROUGH NICE CYBERSECURITY WORKFORCE FRAMEWORK

by

Karo Saharinen, Jaakko Backlund and Jarmo Nevala 2020

ICETC 2020: Proceedings of the 12th International Conference on Education Technology and Computers (pp. 172-176), New York, NY, USA, 172 – 176.

DOI: https://doi.org/10.1145/3436756.3437041
URN: https://urn.fi/URN:NBN:fi-fe2022030121335

Assessing Cyber Security Education through NICE Cybersecurity Workforce Framework

Karo Saharinen
JAMK University of Applied Sciences
Piippukatu 2
40100 Jyväskylä
+358 50 410 4415
karo.saharinen@jamk.fi

Jaakko Backlund
JAMK University of Applied Sciences
Piippukatu 2
40100 Jyväskylä
+358 45 353 3733
jaakkobacklund@gmail.com

Jarmo Nevala
JAMK University of Applied Sciences
Piippukatu 2
40100 Jyväskylä
+358 50 463 4720
jarmo.nevala@jamk.fi

ABSTRACT
This paper presents the results of research and assessment of cyber security education in higher education in Europe and the United States of America. The quantitative research data of the education curricula was gathered and mapped to NICE Cybersecurity Workforce Framework (NCWF) categories to provide a common background for data comparison and analysis.

The research found the education heavily responding to and emphasizing *Operate and Maintain* and *Securely Provision* categories of the framework, with others being present, but with smaller ECTS (European Credit Transfer System) offering in the institutions providing higher education. This leaves doubt if the used framework accurately describes the workforce, or if the education fails to deliver on all categories. Based on these results, more adapt curriculum and course design can be conducted by educators focusing on cyber security.

CCS Concepts
• Social and professional topics→Professional topics →Computing education

Keywords
Cyber Security, Education, European Qualifications Framework, Degree Programme

1. INTRODUCTION
As stated in the Cybersecurity Strategy of the European Union [1], Our economy and daily life is ever more dependent on the cyber security of our digital infrastructure. During times of crisis people rely more and more on the digitalization of our economy. [2] As our society is getting more digitalized, the information kept in these information systems is increasing in value. [3] With more keen eyes targeting at that valuable information to be sold on marketplaces established to trade personal information, confidential enterprise data and other commodities such as tools to exploit vulnerabilities in information systems. This calls for competent, trained workforce to secure our digital information and the environments and networks they are processed on [4].

The education sector is responding to this need by publishing degree programmes concentrating on cyber security and standardizing the field with e.g. Curricula Guidelines for Cyber Security 2017 [5]. The entire recommendations for curricula are under change at ACM as revision work is carried out for the whole Computing Curricula in 2020 [6] with request for comments online as this paper is being written.

2. Measuring Education and Research Methodology
The purpose of the research was to measure quantitatively the current cyber security degree programmes in higher education. The measurement was delineated to involve only higher education (In Europe, EQF [7] levels 6 and 7). The quantitative data was gathered from course catalogues published at the universities offering cyber security focused degree programmes.

In total, 69 degree programmes were investigated and measured. Of those 69, the distribution of degree programmes was as follows:

- 36 degree programmes from the United States
  - 21 Master's Degrees (graduate)
  - 15 Bachelor's Degrees (undergraduate)
- 33 degree programmes from within the European Union
  - 19 Master's Degrees
  - 14 Bachelor's Degrees

The courses were categorized into seven different work force categories according to the NICE Cybersecurity Workforce Framework [8] (later NCWF). When measuring the data, the authors based their judgement on the categorization on the course name. If the course name was ambiguous, the description was taken into account, if and when available. The categories are as follows:

1. *Analyze*
2. *Collect and Operate*
3. *Investigate*
4. *Operate and Maintain*
5. *Oversee and Govern*
6. *Protect and Defend*
7. *Securely Provision*

As the curricula contained courses regarded as "basic IT skills", such as programming, they were assigned a category of the NCWF based on the Work Role that utilized that course contents the most. Table 1 represents an example of this categorization.

Table 1. Example of the work force & course name mapping

Operate and Maintain
Data Administration, Databases
Networking, TCP/IP, Protocols, Network Security, Firewalls, IDS, Routing
Operating Systems, Server, Applications, Linux, Windows, Unix
Securely Provision
Risk Management, Disaster recovery, Data loss preventation
Programming, Coding, Scripting, Software Development, Algorithms
System Architecture, System Development, Parallel computing

Note that the course name did not have to precisely follow the naming/mapping patterns [9]. E.g. "Databases" in Table 1 could be named "Database Management Systems" in the curriculum, as often these topics are taught together in the field of IT. Also,

Software Development is a specialty area of *Securely Provision*, thus all programming courses were counted towards it. Some courses had to be collectively marked as unrelated (e.g. languages) as they had no good category in the referenced NICE Framework.

This categorization marked the course ECTS lengths to quantitatively count towards a certain NCWF category. This category was then used to compare what the different degree programmes were emphasizing on.

3. Analyzing the results

While analyzing the education data, it came apparent that there was a quantitative problem when comparing degree programmes with the different durations. Thus, the data was divided and analyzed based on the European Credit Transfer System (ECTS) length of the degree programme, to provide a more comparable data. The division was done as follows:

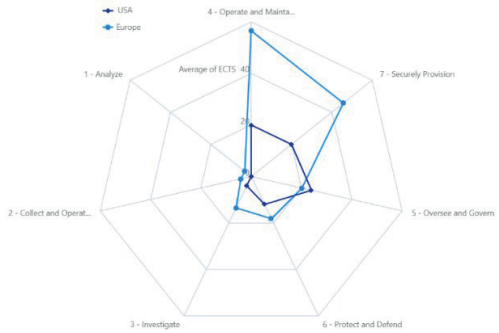
- Bachelor's Degree
  - 168 to 210 ECTS
  - 240 to 252 ECTS
- Master's Degree
  - 60 to 90 ECTS
  - 120 to 139 ECTS

Expressing the curricula and stakeholder demands as radar charts allows for a clearer picture of the distribution, with more noticeable anomalies.

3.1 Bachelor's Degree in Cyber Security

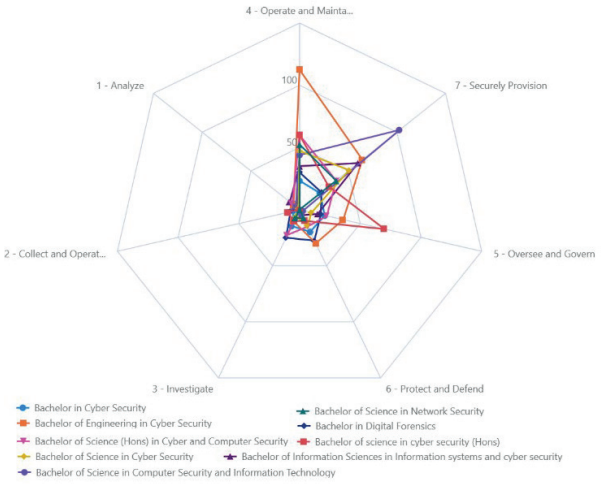
3.1.1 Bachelor's Degrees between 168 to 210 ECTS

Figure 1 visualizes the average distribution of ECTS in bachelor's degree between 160 to 180 ECTS when regarding the NCWF categories.



A clear emphasis can be seen towards *Operate and Maintain* and *Securely Provision*. In USA, *Oversee and Govern* is slightly emphasized when compared to Europe. Noticeable also is the easily categorizable courses in Europe versus in USA. This counts towards higher values of ECTS in the NCWF categories and thus, a higher average in general on the radar chart.

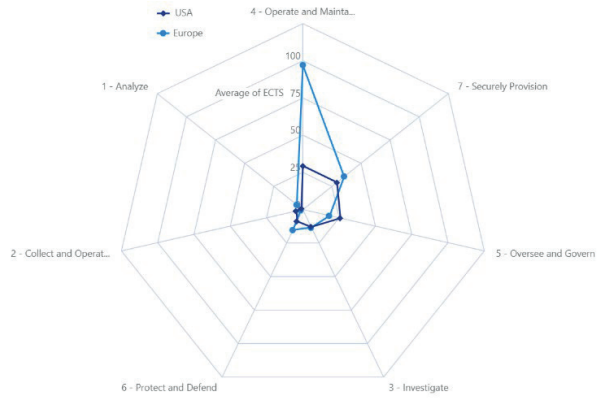
Figure 2 represents the same data when drawn of individual degree programmes of both geographic areas.



It is evident that few of the degree programmes specialize heavily on a certain category; however, all of the categories are present.

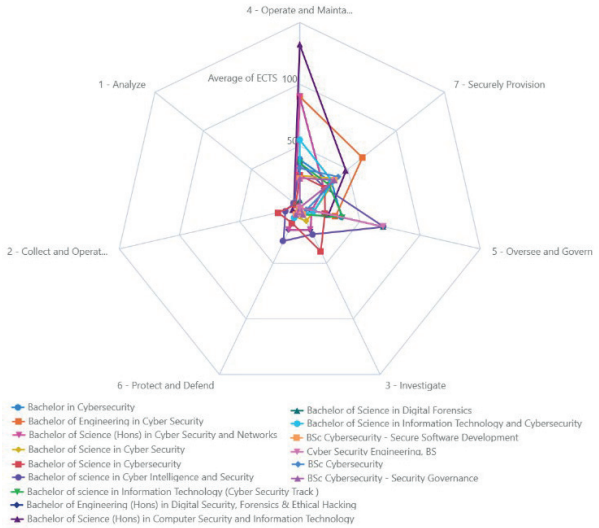
3.1.2 Bachelor's Degrees between 240 to 252 ECTS

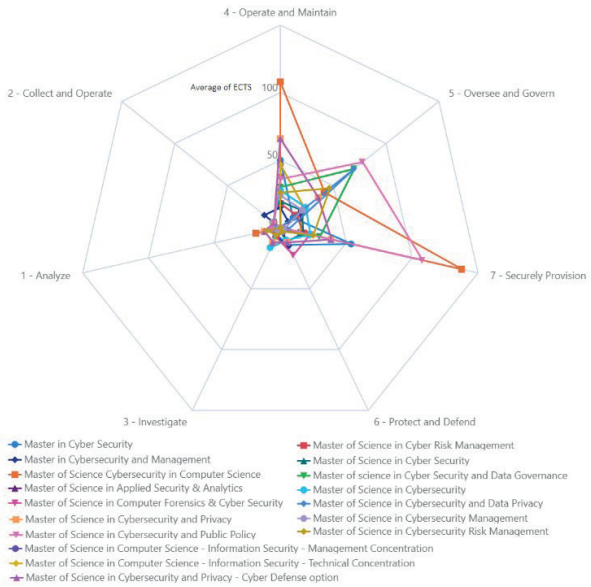
Figure 3 visualizes the average distribution by geographical area, but in bachelor's degree programmes between 240 to 252 ECTS.



In Europe, *Operate and Maintain* is highly emphasized in this section. Securely Provision is close behind. In USA, the degree programmes are following the same pattern as earlier, but *Operate and Maintain*, *Securely Provision* and *Oversee and Govern* are more evenly emphasized.

Once more we look at this through the perspective of degree programmes in figure 4.



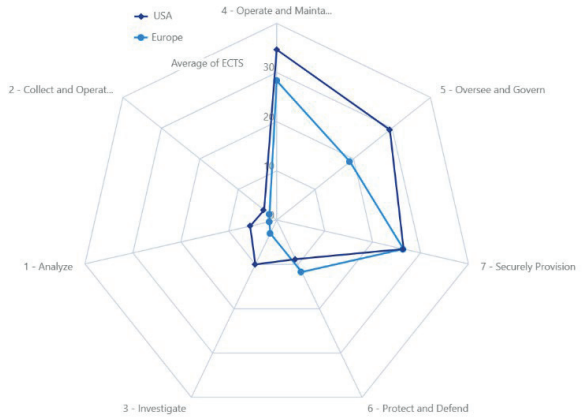


Few bachelor's degrees focus heavily on *Oversee and Govern*, but most are emphasizing *Operate and Maintain* with *Securely Provision*.

3.2 Master's Degree in Cyber Security

3.2.1 Master's Degree between 60 to 90 ECTS

Figure 5 visualizes the average distribution of ECTS in master's degrees between 60 to 90 ECTS when regarding the NCWF categories.

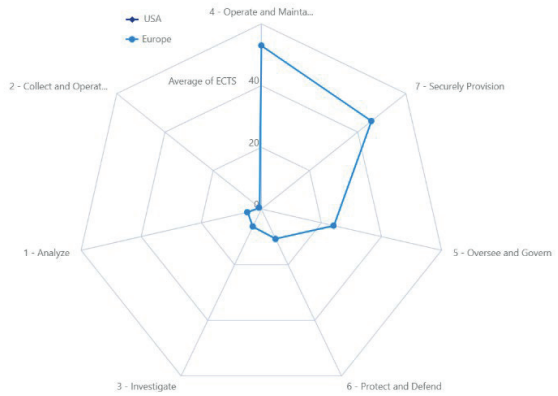


In this segment, *Operate and Maintain* is the highest, however *Oversee and Govern* is higher than *Securely Provision*. In this segment the degree programmes are often specializing to some area. Cyber Security Management and Regulation fall under *Oversee and Govern* category, thus it shows when at the end courses of the master's degree. Figure 6 explains this through the perspective of the degree programmes.

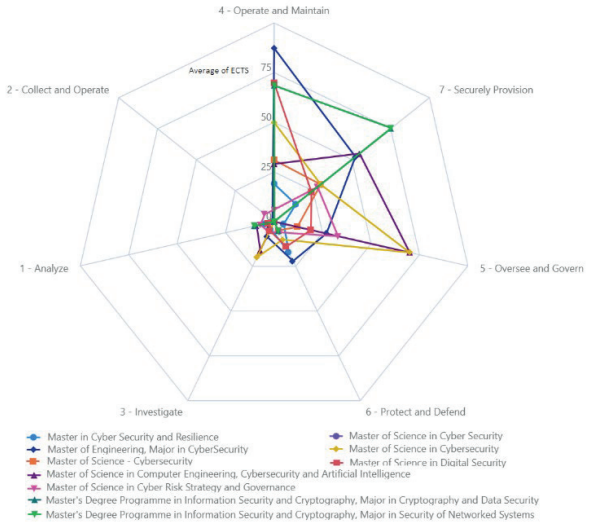
In the visualization above we come across the problem of large course offering of a degree programme. This gives room for selection; however, it causes certain averages to be above the degree length. It still emphasizes the NCWF category offering of the degree programme, while simultaenously it causes confusion in quantifying and analyzing the data.

3.2.2 Master's Degree between 120 to 180 ECTS

This section of degrees only shows European degree programmes as the United States did not have master's degree programmes (or graduate programmes) on this EQF level. Figure 7 shows this absence.



This segment holds a lot of general studies (e.g. object oriented programming) in the field of Information Technology. This length of master's degrees are done typically after a 180 ECTS bachelor's degree, thus *Securely Provision* takes its place after *Operate and Maintain*. The reason can be found in Figure 8.



The widest variety of specializing degree programmes can be found in this segment. As noted earlier, Oversee and Govern is in strong emphasis in some of the master's degrees.

4. CONCLUSIONS & FUTURE RESEARCH

Quantitative measurements are problematic in degree programme comparison as the curricula are often modular, leaving decision making to the students on how to build their knowledge, skills and competence. Also, the amount of elective studies varies heavily and could be counted to efficiently further the students' capability in cyber security, or to deviate from the field completely. Some degrees offer more courses than the degree length in a modular structure, which has to be taken into account, but heavily affect the average weighting of a degree programmes focus on the NCWF categories.

The research data proves that the education curricula are currently responding to the need of the industry. *Securely Provision* and *Operate and Maintain* are evidently taught and emphasized on bachelor's and master's degree levels, with *Oversee and Govern* coming as a close third and mostly gaining the second place in the master's degree.

When we used the NICE Framework as the reference point of this research, it leaves one with the doubt if the seven categories reflect the cyber security workforce evenly. If that were the case, should not all the categories have an even distribution of education? This research proves that education is carried out in all the categories, however *Collect and Operate* and *Analyze* were found to be most absent of all the categories.

If this is the education offering categorization emphasis, then further research could be done on what is the actual industry demand. As this research was done, the European Union Cybersecurity taxonomy [10] was released and it offers a way of classifying the (cyber security) industry sectors.

Each of the industry sectors could be investigated more thoroughly on what categories of workforce they demand. This would give a good reference on course and curriculum design targeting each sector. This future research would provide useful when cyber security education is included in different fields of education, instead of being a degree programme of its own.

5. ACKNOWLEDGMENTS

This work was carried out as part of Cyber Security 4 Europe - project (CS4E) under work package 6 – Cybersecurity Skills & Capability Building.

6. REFERENCES

[1] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 2013. European Comission. Retrieved May 21, 2020 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN

[2] Internet performance during the COVID-19 emergency. Graham-Cumming, J. 2020. Retrieved May 20, 2019 from https://blog.cloudflare.com/recent-trends-in-internet-traffic/

[3] Seh, A.H., Zarour, M., Alenezi, M., Sarkar, A.K., Agrawal, A., Kumar, R., Khan, R.A. 2020. Healthcare Data Breaches: Insights and Implications. *Healthcare* **2020**, *8*, 133.

[4] Finland's Cyber Security Strategy. 2019. The Security Committee of Finland. Retrieved May 21, 2020 from https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

[5] Burley, D., Bishop, M., Buck, S., Ekstrom, J., Gibson, D., Hawthorne, E., Kaza, S., Yair, L., Mattord, H. and Parrish A. Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. 2015. ISBN: 978-1-4503-5278-9

[6] Alison Clear, Allen S. Parrish, John Impagliazzo, and Ming Zhang. 2019. Computing Curricula 2020: Introduction and Community Engagement. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education* (*SIGCSE '19*). Association for Computing Machinery, New York, NY, USA, 653–654. DOI: https://doi.org/10.1145/3287324.3287517

[7] COUNCIL RECOMMENDATION of 22 May 2017 on the European Qualifications Framework for lifelong learning. 2017. Retrieved May 20, 2020 from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017H0615(01)&qid=1552997420044&from=EN

[8] National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. 2017. NIST. DOI: https://doi.org/10.6028/NIST.SP.800-181

[9] Jaakko Backlund, Karo Saharinen and Jarmo Nevala. 2020. Open Research Data Behind this Publication. Retrieved May 29, 2020 from https://gitlab.labranet.jamk.fi/cs4e/assessing-cyber-education

[10] Igor Nai-Fovino, Ricardo Neisse, José Hernández-Ramos, Nineta Polemi, Gian-Luigi Ruzzante, Malgorzata Figwer and Alessandro Lazari. 2019. Proposal for a European Cybersecurity Taxonomy. https://doi.org/10.2760/106002

PIII

QUALITY CRITERIA FOR CYBER SECURITY MOOCS

by

Simone Fischer-Hubner, Matthias Beckerle, Alberto Lluch Lafuente, Antonio Ruiz Martinez, Karo Saharinen, Antonio Skarmeta and Pierantonia Sterlini 2020

13th IFIP WG 11.8 World Conference, WISE 13, Proceedings.

DOI: https://doi.org/10.1007/978-3-030-59291-2_4
URN: https://urn.fi/URN:NBN:fi-fe2022022420768

Quality Criteria for Cyber Security MOOCs

Simone Fischer-Hübner[1], Matthias Beckerle[1], Alberto Lluch Lafuente[2], Antonio Ruiz Martínez[3], Karo Saharinen[4], Antonio Skarmeta[3], and Pierantonia Sterlini[5]

[1] Karlstad University
[2] Technical University of Denmark
[3] University of Murcia
[4] Jyväskylä University of Applied Science
[5] Trento University

Abstract. Cyber security MOOCs (Massive Open Online Courses) can enable lifelong learning and increase the cyber security competence of experts and citizens. This paper contributes with a review of existing cyber security MOOCs and MOOC quality assurance frameworks. It then presents quality criteria, which we elicited for evaluating whether cyber security MOOCs are worthy to be awarded with a quality seal. Finally, an exemplary evaluation of six selected European MOOCs is presented to exercise the quality seal awarding process. Additionally, the evaluation revealed that criteria for assuring privacy, ethics, meeting professional expectations and openness were on average not clearly met.

Keywords: Cyber Security · Security Education · MOOCs · Quality Assurance and Evaluation.

1 Introduction

The CyberSec4Europe project will, as one of the EU H2020 pilot projects for a future European Cyber Security Competence Network, test and demonstrate potential governance structures for such a network of future competence centres. One area, for which the project will define and evaluate governance structures, is the area of quality assurance for cyber security education provided by MOOCs (Massive Open Online Courses), which have emerged over the last years as an alternative to formal education and as an enabler for life-long learning to a broad group of students.Cyber security MOOCs can thus increase the cyber security competence of experts but also a larger group of the population in Europe. For defining a quality assurance process, a list of quality criteria is needed for evaluating MOOCs if they are worthy to be awarded with a quality seal by a European Cyber Security Competence Network. For eliciting such quality criteria, we have first conducted an initial review of existing cyber security MOOC offerings and of existing rules and practices of operating them at EU level for assuring quality. While MOOC quality assurance frameworks were already proposed by different organisations, we have been particularly interested in eliciting

those quality assurance criteria that should be met specifically by cyber security MOOCs, including cyber range MOOCs, in addition to generic MOOC quality assurance criteria. The objectives of this paper is to present and motivate quality criteria for cyber security MOOCs, and to present and discuss the exemplary evaluations of selected cyber security MOOCs according to those criteria and conclusions drawn from it.

The remainder of this paper is structured as follows: Section 2 provides a short review of existing offerings of cyber security MOOCs in Europe and the existing rules and practices of operating them for providing quality, and concludes with requirements for quality criteria and open issues. Section 3 is briefly summarising the related work of existing Quality Assurance frameworks for MOOCs. In Section 4, we are presenting quality criteria for cyber security MOOCs, which are extending the existing MOOC quality criteria and are addressing the identified open issues. These criteria are then used for an exemplary evaluation of selected cyber security MOOCs for testing a process for awarding a quality seal to cyber security MOOCs based on these criteria, as presented in Section 5. Finally, Section 6 is presenting overall conclusions and next steps to be taken.

2 Review to Existing European Cyber Security MOOCs

This section summarises the review of the landscape of European cyber security MOOCs and the rules for operating them that we conducted for CyberSec4Europe. Our survey of the current landscape showed that cyber security specific topic channels or platforms do not exist yet - existent cyber security MOOCs are rather offered on the dominant learning platforms, such as Coursera, EdX, FutureLearn, Udacity, Edemy, or Canvas. Cyber security MOOCs can be grouped into academic level MOOCs, continuous learning MOOCs and MOOCs utilising cyber ranges, or can be combinations of those categories, and will be reviewed in the following sections.

Among the different MOOC offering, the EIT Digital (a division of the EIT, European Institute of Innovation and Technology) stands out with its focus on the area of Innovation and Entrepreneurship (I&E) education in ICT and the implementation of blended I&E courses. We will review them in the Academic level section albeit they may also fit the Continuous Education section.

2.1 Academic Level MOOCs

Academic level courses or programmes are those offered primarily to students enrolled at a University and award credit points or academic degrees to those enrolled students. Online academic courses can be divided into classical MOOCs that are open to all kinds of participants in addition to enrolled students, and other online courses or programmes, which can only be accessed by students that are formally enrolled at the offering academic institution.

While classical MOOCs for cyber security topics are mostly offered by academic institutions, most of them are MOOCs for continuous learning, whereas

classical academic MOOCs are still rare and only a handful of them could be identified via a search on Class Central and via the Web [1].

Academic courses are typically already governed by existing regulations and university's own rules and quality plans for guaranteeing high quality education. For instance, national higher education acts and ordinances usually regulate student admission criteria, qualification requirements for course instructors and for the publication of course evaluations. For issuing ECTS credits, the university must have an accreditation approved by the Education Accreditation Commission (EQAC) and must provide transparency on course workload and learning outcome, as required by the EU Commission.

The EIT Digital approved courses are slightly different than classical academic MOOCs from the perspective of the governance and approval process.[6] The qualification of the proposing institutions is guaranteed by the involvement of the EIT Digital Network of European universities. The approval of the MOOCs follows a submission-based model similar to the traditional calls for research funding, that typically involves a consortium. More specifically, the development of the courses is based on a cross-university collaboration in accordance with the current EIT Digital I&E education guidelines. The partners submit a proposal to the EIT Digital for co-financing the implementation of a specific MOOC and, if approved by the EIT Digital, the MOOC is realised and ported in the learning platform for the actual execution.

2.2 MOOCs as Continuous Education Courses

Continuing education courses are meant to provide all citizens with specialised education through all phases of their lives and are characterised by a huge variety of formats and characteristics. The dominant classes of providers of Cyber Security MOOCs are higher education institutions and private companies, but some are also offered by non-profit organisations or individuals. Most MOOC platforms have headquarters in the US, hence not necessarily adhering to EU regulations such as the EU General Data Protection Regulation 2016/679 (GDPR).

Access to the courses is often unrestricted, but there are cases in which enrolment is limited by several criteria that may include nationality constraints, for example due to sanctions to specific countries, typically dictated by the platform's legal headquarters: the US in most cases. Academic qualifications are rarely a mandatory criteria to access a course. Most courses, indeed, are offered with no specific criteria on the students' qualifications and previous knowledge, although informal recommendations are usually given. Platforms tend to provide information about content, learning objectives, and professional expectations in an informal way. Certificates are sometimes issued automatically upon completion of the course but without a formal verification.

[6] An example of technical specialisation is available at: `https://www.coursera.org/specializations/embedded-systems-security` whereas a I&E specialization is available at: `https://www.coursera.org/specializations/value-creation-innovation`

The typical qualification for courses provided by higher education institutions is that of a teacher at the corresponding institutions (lecturer/professor). In the rest of the cases, teachers are often experienced professionals with a variety of profiles, but qualification criteria for those instructors are usually not provided by the platforms.

2.3 MOOCs utilising Cyber Ranges

The definition of a cyber range currently varies greatly between organisations giving cyber security education. The size of the cyber range currently varies from one virtual machine to thousands. Thus declaring a MOOC to a "Cyber Range MOOC" is troublesome and needs clear criteria.

MOOCs in particular have the problem of being tied to the platform providing registration and distribution of material for the MOOC. Larger platforms might not support technical laboratories (other than basic quizzes or multiple-choice answers) leaving out the technical aspect of cyber security. This leaves universities with the problem of hosting the cyber range by themselves. Generating accounts and instructions on how to use the cyber range next to the MOOC platform requires automatisation and integration of the environments. This also provides challenges to the student, with multiple accounts or environments, who thus may require online support, which in turn increases costs and may hinder the scalability of the cyber range course.

These reasons might be the troublesome parts of the cyber range MOOCs, which without answers leaves the industry without competent, technically oriented workforce. For this reason cyber range MOOCs are currently basically non-existent yet, while rather traditional cyber range courses are offered by several European Universities, such as Tallinn University of Technology (in collaboration with NATO), NTNU and JAMK University of Applied Sciences. Apart from that, also the openness (which is one of the inherent MOOC characteristics) of course attendance and of course material is often, due to the security sensitivity of the course content, an issue for courses on cyber ranges, which therefore typically have restrictions in place.

2.4 Conclusions and Gaps

From our review, we want to highlight especially the following conclusions in terms of quality assurance criteria needed for the different types of cyber security MOOCs: In general, criteria for assuring fairness and transparency in regard to course admission, access to course content and evaluations will need attention. This is especially important for cyber security MOOCs teaching sensitive information about hacking and vulnerabilities. So far, cyber range MOOCs are non-existent, but if developed in future, they will require ethical rules on the openness of course content, student admission and course material.

Furthermore, MOOC platforms and channels are typically hosted by US providers, which means that personal data including student attendance and performance tracking may be transferred to the USA, which raises privacy and

issues of compliance with the GDPR (EU General Data Protection Regulation), especially in regard to the transfers of personal data to third countries regulated in Chapter V of the GDPR.

3 MOOC Quality Assurance and Validation Frameworks

In CyberSec4Europe, we are particularly interested in eliciting quality assurance criteria for cyber security MOOCs including future cyber ranges MOOCs. The definition of such criteria is fundamental for course recognition, certification, and accreditation, and for awarding quality seals to MOOCs. As pointed out by Gaebel (2014) [2] for MOOCs making a change in higher education, they have to award credits, and thus quality assurance criteria for credentialisation play an important role too.

The OpenCred report by JRC [3] addressed the recognition practices of open learning achievements by European non-formal open learners. This study identifies elements of MOOC recognition by another Higher Education Institution (HEI) or employer, including the identity verification of learners, suitable supervised assessment, informative credential that acknowledge learning, and the award of credit points.

For the definition of the quality assurance criteria for cyber security MOOCs, we have considered the review of the main existing MOOC quality assurance and validation frameworks: the OpenupEd label [4], the Quality Reference Framework (QRF) for the Quality of Massive Open Online Courses (MOOCs) [5], and the Instructional and Assessment Design Framework (IADF)[7]. Such specific frameworks for MOOCs were developed, since, as indicated by Hood and Littlejohn (2016) [6], the quality measures and indicators used so far for other type of courses are not always suitable for MOOCs, and quality is not objective because it is a purpose-specific measure. These measures could be even dependent on pedagogy [7], which means that they could differ between MOOCs and courses taught in another form.

The OpenupEd Quality Label [4] is a framework designed to improve the quality of OpenupEd's MOOCs. OpenupEd is an alliance of institutional MOOC providers, which is coordinated by the European Association of Distance Teaching Universities (EADTU). Their MOOCs have eight distinctive features: openness to learners, digital openness, learner-centred approach, independent learning, media-supported interaction, recognition options, quality focus, and spectrum of diversity.

The OpenupEd Quality Label has been derived from the E-xcellence label [8], which provides a methodology to assess the quality of e-learning in higher education and it is based on several benchmark statements. These statements are arranged into six dimensions: Strategic Management, Curriculum Design, Course Design, Course Delivery, Staff Support, and Student Support. As e-learning in HEIs is evolving and changing, the E-xcellence label has undergone several updates from the feedback of its reviewers to reflect this evolution. Through a

[7] https://www.eitdigital.eu/eit-digital-academy/

mapping between the benchmarks and the OpenupEd distinctive features, it is possible for a MOOC to provide evidence confirming that it supports OpenupEd features. These evidences can be gathered by different stakeholders such as management, academics, course designers, tutors, and students.

The Quality Reference Framework (QRF) for the Quality of MOOCs [5] is a development of the European Alliance for the Quality of Massive Open Online Courses (MOOCs), called MOOQ. For the definition of this framework, MOOQ has been based on ISO/IEC 40180. The research they have made by means of Global MOOC Quality Surveys, semi-structured interviews, and the feedback from several MOOQ workshops. In the QRF, they have defined three dimensions: Phases, Perspectives, and Roles. The phases, in turn, are divided into processes. Furthermore, for the design and development of MOOCs, the framework provides the QRF Key Quality Criteria and the QRF Quality Checklist. The former are action items for those actions that could be performed in different processes. The latter consists of leading questions for the defined dimensions to remind the key issues to be considered in the MOOC design and development.

The Instructional and Assessment Design Framework (IADF) has been developed by EIT Digital with the other Knowledge and Innovation Communities (KIC) to assess the quality assessment of courses. This framework consists of four components: Instructional Design, Assessment, Functional Requirements, and Learning Analytics. These components have to be considered by teachers for the design of their courses and by evaluators to evaluate the product developed. However, this is an *evaluation framework that is not tailored to security.*

To the best of our knowledge, no cyber security specific quality assurance or validation framework is existing yet.

4 Proposed Quality Criteria for Cyber Security MOOCs

Our quality assurance criteria for Cyber Security MOOCs presented in this section were (1) derived the conclusions from our review of existing European MOOCs in section 2 in terms of gaps to be addressed and are (2) also based on criteria taken from existing quality assurance frameworks that were presented in section 3. Moreover, some of the criteria are (3) based on existing best practices and our experiences, as well as (4) derived from regulations and ethical standards.

Some of the criteria require the involvement of relevant stakeholders for cyber security MOOCs, which may include cyber security experts from industry or government, data protection officers, privacy activists, representatives from (ethical) hacker organisations and/or from national cyber security agencies.

The categories of quality criteria that we present in the following subsections are corresponding to categories used in the other quality assurance frameworks referred to in the previous section. In addition, we added categories for ethical rules, privacy and for cyber range specific quality assurance criteria, which as our review and gap analysis in section 2 showed, need special attention when it comes to cyber security MOOCs. Cyber security-specific criteria including criteria for

future cyber range MOOCs in each category are especially highlighted, except for three categories that have no cyber-security-specific criteria . The detailed list of all criteria for each category and the sources from which they were derived are available in the CyberSec4Europe project deliverable [1].

4.1 Criteria for the Qualification of the Proposer

In order to create and offer a MOOC of high quality, the proposing institution (proposer) should have the proper qualification and experiences to be able to develop, run and evaluate the MOOC in a professional manner. The quality of the proposer is also essential for the recognition of the MOOC by the community and for the recognition of credentials.

Cyber Security Specific Criteria: The proposer should especially be recognised by relevant stakeholders in cyber security, either through academic recognition or through their long experiences in the cyber security domain. Proposers of cyber range MOOCs should have expertise in applied technology & private-public partnership. The proposer's cyber range should be technical, work-life oriented which can mimic realistic phenomena (attack campaigns, threat actors, techniques & tools) from the cyber security field.

4.2 Admission Criteria and Qualification of Participants

It is important that participants (students) know what is expected from them in terms of prerequisites and that the teachers know what to expect from the participants. However, prerequisites that are not essential for the MOOC should not be used for excluding participants, as in principle the aim should be to be as inclusive as possible for enhancing cyber security competence in Europe. Participants must also be able to find out whether they are qualified for a MOOC and/or why they are not accepted for enrolment. Therefore, the acceptance process should be legit and transparent.

Cyber Security Specific Criteria: For cyber range MOOCs, the participant should have the skills necessary to operate a technical cyber range platform or the learning objective of the course should be that the participant learns how to operate such platform.

4.3 Criteria for the Qualification of Instructors

The qualification of the instructors (teachers) is fundamental to ensure a high quality MOOC. Instructors should usually have an academic degree and should have undergone pedagogical training - for academic MOOCs, national higher education acts often require that the academic degree of the examiner should be higher then the degree that is awarded by the course. For continuous learning MOOCS, relevant working life or industrial experiences should be required.

Cyber Security Specific Criteria: Since the cyber range requires technical operation, the instructor of a cyber range MOOC should have such technical skills for conducting and supervising such operations or the course should have dedicated personnel for this task (e.g. cyber range specialists).

4.4 Criteria for Examination, Credentialisation and Recognition

For awarding credits or certificates, course examination has to verify that the participant has achieved the goals of the education and assure that the awarded credits or the certificate correctly reflects the quality with that the goals were achieved. The examination must be fair and the goals must be transparent, so that the participants know what is expected from them in the exam and that the risk of fraud is minimised. For promoting life long learning, course certificates should be issued enabling recognition of the educational achievements in the professional or life-long/blended learning context. For ensuring recognition in the academic context, academic European MOOCs should be recognised as a valid credit-awarding course within the European credit transfer system.

Cyber Security Specific Criteria: The cyber range activities, laboratory work, and assignments that need to be completed for obtaining a course credential should be clearly stated.

4.5 Course Evaluation Criteria

MOOC evaluations allow student to give feedback and ratings for continuously improving the course quality, and by this, reduce the number of course dropouts. Published course evaluations provide information allowing to judge a MOOC and its usefulness from a participant's perspective. Course evaluations are commonly regulated in the academic sector. In particular, the Massive Online Open Education Quality (MOOQ) QRF Framework [5] provides key quality criteria for the evaluation planning, realisation, review and resulting improvements, which we propose as quality criteria together with criteria from rules and established practices from the academic sector.

Cyber Security Specific Criteria: An evaluation review and follow-up process should be in place that should involve relevant stakeholders, such as the MOOC design team, instructors, director of studies, but also relevant cyber security stakeholders, as the ones named above.

4.6 Criteria for Meeting Professional Expectations

For meeting professional expectations, suitable stakeholders, especially from working life and the employment side, should be involved in different MOOC phases.

Cyber Security Specific Criteria: When providing a cyber range course to a company or an organisation, it should be "realistic enough", i.e. simulate operational and supporting services and systems available for the participants. The extent of realism should be discussed and agreed upon during designing the course. When participants from an organisation attend a course given for that organisation which utilises a cyber range, the participants should, if there is agreement with the instructor, follow their own organisations' processes and guidelines when detecting abnormal or malicious activity and when starting or even performing incident management. This approach should bring to awareness the need to update the organisation's guidelines and process documentation.

4.7 Course Structure and Course Content Criteria

Criteria for the course structure guaranteeing the quality of the course content were partly taken from the OpenupEd suggested distinctive features [9], and some others were motivated by the Checklist for MOOC Accreditation in [10]. These criteria are requiring to clearly specify learning outcomes that can be achieved by the course content. We also require that continuous learning MOOCs offered by companies should not with an inappropriate bias promote commercial products or systems of that company, unless the entire focus of the MOOC is on the teaching or training of the usage of these products or systems.

4.8 Course Platform and Channels Criteria

Quality criteria for platforms and channels are derived from legal requirements. In particular, GDPR compliant platforms and channels must be selected. Moreover, the functionality of the platform should comply with the EU Directive 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies for ensuring inclusiveness.

4.9 Openness Criteria

Openness is a key element of a MOOC and important both in terms of the MOOC content and material (by using an open licensing, e.g. CC-BY-SA, allowing to freely reuse, mix and redistribute material), and in terms of being open to the learner's needs, enabling them to study at any time, place and pace of choice.

Cyber Security Specific Criteria: There should be clear, transparent and justifiable policies for defining any restrictions to digital openness (e.g. for the use of malicious or attack code for teaching purposes) and/or openness of course elements (e.g. those that are hacking-related or for other reason security-sensitive) to learners for ethical or security reasons.

4.10 Ethics and Privacy Criteria

Education in cyber security by its nature must also cover attack methodologies and how vulnerabilities arise and/or could be misused. This knowledge is needed for teaching how to secure systems against threats and weaknesses in computer-based systems, e.g. administrative systems, industrial control systems and computer networks. A deeper understanding of threats and risks is also needed when performing risk assessment, risk analysis and risk management. However, this knowledge could also be exploited for malicious purposes. Because of this dual nature of this knowledge, it is important to define, teach and enforce ethical principles for cyber security courses in regard to ethical hacking, handling security-sensitive information and personal data.

Moreover, many teaching platforms today store personal information about the participants for different purposes. In some cases, this information is used to profile participants for either platform improvement or for market purposes. This profiling can reveal sensitive personal data like political opinions, religious

believes or ethical origin e.g. when tracking and storing course preferences and browsing patterns. On platforms like YouTube or other types of "free" channels, the information is used for targeted advertisement and in some cases sold on for market purposes. With this in mind, it is important to give the participants choices for where to access the learning material and not force the student to disclose more personal data than it is necessary for fulfilment of the course and the examination. For example, if video course material is made available through YouTube, there should be an alternative more privacy friendly channel made available for accessing the material. It is also important that the "owner" of the course (i.e. the data controller) has an appropriate data processor agreement with the sites that distribute the course material stating how personal data may be processed in compliance with Art. 28 GDPR. There must be GDPR compliant privacy policy statement, both from the platform provider and the course owner that process personal data. The platform and course instances storing personal data about the participants must be secured by appropriate security controls and should be designed by the Data Protection by Design and Default principle (Art. 25 GDPR).

Cyber Security Specific Criteria: While ethics and privacy criteria should be enforced for all types of MOOCs, they are especially relevant to Cyber Security MOOCs teaching security and privacy, for demonstrating that privacy and ethics taught in the course are also enforced in practice, i.e. the course should live up to the standards taught.

4.11 Cyber Ranges Criteria

For cyber ranges to be utilised for future cyber range MOOCs certain quality criteria, in particular in regard to the technical and operational capabilities and capacities should be fulfilled. For instance, the institution's cyber range should provide systems and services for planning, running and doing post-exercise analysis and also provide systems and services for the defending team to prevent, detect, mitigate and recover from cyber incidents.

5 Exemplary Evaluation of MOOCs

The project partners conducted an exemplary evaluation of selected cyber security MOOCs by applying a subset of the defined quality criteria, with a focus on those criteria that are cyber security specific. Therefore, Table 1 does not include all criteria categories from Section 4. In addition, since no Cyber Range MOOCs were available, those criteria could not be tested.

The objective of the exemplary evaluation was twofold: First, we wanted to test a process for awarding quality seals to cyber security MOOCs based on our quality criteria in order to propose governance rules for awarding MOOC quality seals by a future European Cyber Security Competence Center and to test the applicability of our criteria. Second, we wanted to test how far information for evaluating the quality of exemplary cyber security MOOCs is openly available

online, so that the MOOCs can be easily assessed by interested students and to what extent the criteria are fulfilled.

5.1 Selection of Exemplary MOOCs

For the evaluation exercise, we selected the following six MOOCs from different European countries in the form of academic and/or continuous learning MOOCs offered by academic institutions and/or industry for having a broad range of different types of MOOCs:

- Continuous learning MOOC: "Information Security: Context and Introduction" by Royal Holloway, UK [11]
- Continuous learning MOOC: "Managing Security in Google Cloud Platform" by Google [12]
- Academic MOOC: "Netzwerksicherheit" by Technische Hochschule Lübeck, Germany [13]
- Academic MOOC: "Privacy by Design" by Karlstad University, Sweden [14, 15]
- Academic MOOC: "Development of Secure Embedded Systems Specialization", EIT Digital Cyber Security course [16]
- Academic and continous learning MOOC: "Cyber Security Base with F-Secure, Academic", by the University of Helsinki and F-Secure, Finland [17]

5.2 Evaluation Procedure

Our evaluation procedure had three phases and basically implemented a peer-review process, which was especially needed for evaluating those criteria that were rather subjective and open for interpretations. In the first phase, each MOOC was independently evaluated by five or six project partners. For each quality criterion, each partner decided to which degree the criterion was fulfilled and assessed it as "yes", "partly", or "no". If information was not retrievable from the openly published course information and material, the assessment was marked as "unclear". In addition, the source of information used for the assessment and a short explanation of the decision process were noted. In the second phase, these five to six evaluation lists were collected and combined into a single document. Afterwards, one partner, assigned for taking the lead, consolidated any unanimous ratings into a combined evaluation list. In the third phase, in case of deviating ratings for criteria, a consensus discussion among involved partners took place. Afterwards, the evaluation was finalised and graphical representations were generated.

5.3 Results and Discussion

Ratings and Openness of Information: Our evaluation exercise showed that not all information for evaluating the quality of MOOCs is openly available. This is illustrated in Table 1, which shows the average percentages of unclear ratings due to a lack of available information for different criteria categories.

Information about the proposing institute were rather visibly published. Also, information needed to evaluate the course examination, credentialisation, and recognition criteria as well as the course structure and content criteria were mostly available online. Considering that students that are interested to enrol, need that information to decide if a MOOC is suitable for them, this comes at no surprise. Nevertheless, it is astonishing that for several of these criteria information could not be found on the related websites.

Ethical considerations for teaching cyber security, including ethical rules for students for handling security-sensitive information, were only clearly addressed for a quarter of the analysed courses. One may argue that some of the selected MOOCs are not including ethical hacking exercises, and thus do not require such ethical instructions for students. Nonetheless, ethical standards are in general of relevance for cyber security experts and should thus be preferably addressed by any cyber security MOOC.

On average only a third of the privacy criteria were clearly fulfilled. In particular, most of the evaluated MOOCs did not have clear policy statements specifying how student-performance related data collected by the course platforms are used by the course owners. Hence, those MOOCs provide no good example of how to implement privacy requirements in practice. Finally it is also notable that criteria about meeting professional expectation were on average only clearly fulfilled in less than 15%. In particular, many of the courses missed to involve cyber security stakeholders in the course in the course design, implementation, realisation, and/or periodic review. This is a further shortcoming, as practical working-life cyber security experiences and perspectives may thus not be well reflected.

Table 1. Average distribution of criteria assessment ratings per criteria category for the evaluated MOOCs in percent.

Category of Criteria	yes	partly	no	unclear
Qualification of the proposing institution	80.5	2.4	12.2	4.9
Course structure and content criteria	55.2	12.8	3.2	28.8
Qualification of instructors	52.8	8.3	2.8	36.1
Course examination, credentialisation, and recognition	40.6	4.2	32.3	22.9
Privacy requirements	37.1	8.6	14.3	40.0
Openness	33.3	0.0	0.0	66.7
Ethical considerations for teaching cyber security	25.0	4.2	20.8	50.0
Meeting professional expectation	14.3	0.0	21.4	64.3
Average	45.2	7.0	14.7	33.1

Quality Seal Awarding Process. The three phase evaluation process consisting of independent evaluation by several experts, consolidation, and moderated consensus discussions and decisions, worked very well and is thus recommended as part of a governance structure for awarding the quality seal to MOOCs by a European Cyber Security Competence Network. We recommend to only award

a quality seal for MOOCs that clearly fulfil all quality criteria that are not formulated as optional. For any criteria that are not met, partly met or that are unclear, the proposer should be requested to address these open issues first and then resubmit the application for a quality seal. An evaluation process based on openly published information only, does not seem to work, even though this is not inline with the inherent openness characteristic of MOOCs. Nonetheless, we conclude that the MOOC proposers will have to add documentation demonstrating how quality criteria have been met by them when they submit their application for a quality seal. Ultimately, active participation in a MOOC might be needed to reliably retrieve all information needed for the evaluation.

6 Conclusions

In this paper, quality criteria for cyber security MOOCs were elicited and tested with an evaluation exercise for selected European cyber security MOOCs. The results provide a basis for defining a quality assurance process for MOOCs to be awarded with a quality seal by a European Cyber Security Competence Network. As a next step, governance models for a quality seal awarding process will be further developed and refined by the CyberSec4Europe project. Our exemplary evaluations revealed issues in regard to the openness of course meta information that restrain evaluators and interested students to assess the quality of MOOCs. Moreover, criteria for assuring privacy, ethical rules for course participants, as well as for ensuring that professional expectations of cyber security stakeholders are met, were to a large extent not fulfilled by the selected MOOCs. We therefore hope that our quality criteria will also enable cyber security MOOC designers, developers, and owners to generate better courses that will fulfil our criteria. Our criteria are especially important for enabling the development of high quality cyber range MOOCs in future, which will be further investigated by CyberSec4Europe.

Acknowledgements

This work was funded by the European Commission's H2020 Programme under the Grant Agreement Number 830929. We thank all contributors to the CyberSec4Europe Deliverable 6.1, especially Hans Hedbom, Fabio Massacci, Yani Päijänen, Petri Muka, Marko Vatanen, Lejla Islami and Mahdi Akil, for their valuable input.

References

[1] Simone Fischer-Hübner et. al. CyberSec4Europe Deliverable 6.1 – Case Pilot for WP2 Governance. `https://cybersec4europe.eu/publications/deliverables/`, 2019.

[2] Michael Gaebel. *MOOCs Massive Open Online Courses.* European University Association, 2014.

[3] Gabi R Witthaus, Andreia Inamorato dos Santos, Mark Childs, Anne-Christin Tannhauser, Grainne Conole, Bernard Nkuyubwatsi, and Yves Punie. Validation of non-formal MOOC-based learning: An analysis of assessment and recognition practices in Europe (OpenCred). *Joint Research Council, European Union*, 2016.

[4] Jon Rosewell and Darco Jansen. The OpenupEd quality label: Benchmarks for MOOCs. *The International Journal for Innovation and Quality in Learning*, 2(3):88–100, 2014.

[5] Christian M. Stracke, Esther Tan, António Texeira, B. Vassiliadis, A. Kameas, C. Sgouropoulou, and G. Vidal. Quality Reference Framework (QRF) for the Quality of MOOCs. `http://www.mooc-quality.eu/QRF`, 2018.

[6] Nina Hood and Allison Littlejohn. MOOC Quality: The need for new measures. *Journal of Learning for Development – JL4D*, 3(3), 2016.

[7] Valeria Aloizou, Sara Lorena Villagrá Sobrino, Alejandra Martínez Monés, Juan Ignacio Asensio Pérez, and Sara García Sastre. Quality Assurance Methods Assessing Instructional Design in MOOCs that implement Active Learning Pedagogies: An evaluative case study. In *Proceedings of Work in Progress Papers of the Research, Experience and Business Tracks at EMOOCs 2019*, pages 14–19. CEUR Workshop Proceedings, 2019.

[8] Keith Williams, Karen Kear, and Jon Rosewell. *Quality Assessment for E-learning: a Benchmarking Approach*. European Association of Distance Teaching Universities (EADTU), 2nd edition, 2012.

[9] Darco Jansen, Jon Rosewell, and Karen Kear. Quality frameworks for MOOCs. In *Open Education: from OERs to MOOCs*, pages 261–281. Springer, 2017.

[10] Commonwealth of Learning. Guidelines for Quality Assurance and Accreditation of MOOCs. *Commonwealth of Learning*, 2016.

[11] Royal Holloway. Information Security: Context and Introduction. `https://www.coursera.org/learn/information-security-data`, accessed 21 Jan 2020, 2020.

[12] Google. Managing security in google cloud platform. `https://www.coursera.org/learn/managing-security-in-google-cloud-platform`, accessed 21 Jan 2020, 2020.

[13] Technische Hochschule Luebeck. Netzwerksicherheit. `https://www.oncampus.de/weiterbildung/moocs/netzwerksicherheit`, accessed 21 Jan 2020, 2020.

[14] Karlstad University. Privacy by Design. `https://www.kau.se/cs/pbd`, accessed 21 Jan 2020, 2020.

[15] Simone Fischer-Hübner, Leonardo A Martucci, Lothar Fritsch, Tobias Pulls, Sebastian Herold, Leonardo H Iwaya, Stefan Alfredsson, and Albin Zuccato. A MOOC on Privacy by Design and the GDPR. In *IFIP World Conference on Information Security Education*, pages 95–107. Springer, 2018.

[16] EIT Digital. Development of Secure Embedded Systems Specialization. `https://www.coursera.org/specializations/embedded-systems-security`, accessed 21 Jan 2020, 2020.

[17] University of Helsinki and F-Secure. Cyber Security Base with F-Secure, Academic. `https://cybersecuritybase.mooc.fi/`, accessed 21 Jan 2020, 2020.

PIV

CRITICAL INFRASTRUCTURE PROTECTION – EMPLOYER EXPECTATIONS FOR CYBER SECURITY EDUCATION IN FINLAND

by

Janne Jaurimaa, Karo Saharinen and Sampo Kotikoski 2020

20th European Conference on Cyber Warfare and Security, 24th - 25th June 2021, Chester, UK.

DOI: https://doi.org/10.34190/EWS.21.015
URN: https://urn.fi/URN:NBN:fi-fe2022022420763

Critical infrastructure protection - Employer expectations for cyber security education in Finland

Janne Jaurimaa, Karo Saharinen, Sampo Kotikoski
JAMK University of Applied Sciences, Jyväskylä, Finland
m1270@student.jamk.fi
karo.saharinen@jamk.fi
sampo.kotikoski@jamk.fi

Abstract: In the human factor of cyber security, high level technical experts are considered as multidisciplinary technical gurus who are familiar with every aspect of IT environments including operating systems, code languages and protocols. University curricula and guiding frameworks, such e.g. NICE Cyber Security Workforce Framework, are designed to produce professionals to match the endless needs of working life. The cornerstones of achieving good working results can be considered as the level of expertise competence of the employee performing the task, as well as combining personal skills and abilities with the competence profile of the given task. Does the cyber domain need slightly lower educated, vocational level employees? As part of the National Security Policy in Finland, the vocational qualification in information and communications technology has recently started to produce suitable workforce for cyber labor on the European Qualifications Framework level 4 (EQF-4).

In this research paper we answer the question how well the vocational education meets the demands of the employers as suitable workforce in cyber security in Finland. The study also investigated what kind of cyber security employees the Finnish employers currently need; what is the required level of education, level of experience and direction of competence. The research data was collected through a structured questionnaire survey, which was directed to critical national infrastructure protection companies such as Finnish telecom operators, ICT service providers, defense sector, and other governmental actors. The questionnaire results were examined with quantitative methods.

Based on our results, regarding the content of education at EQF4-level, employers believe that the emphasis should be placed on basic technical skills and adherence to guidelines, while choosing more detailed specific areas of expertise is less important at this level of education. Based on the responses, in general cyber security related work has higher education level requirements than EQF4-level could provide. The results of the study can be used as guidelines for the development of the future curricula and in the strategic leadership of companies employing cyber security professionals.

Keywords: Human factor, Security Policy, Critical infrastructure protection, Strategic leadership

1. Introduction

Finnish Cyber Security Strategy was published on 24 January 2013 in the form of a government resolution (The Security Committee of Finland, 2013). It specifies the main goals and operation models to meet the challenges in the cyber domain and ensure its functionality. In this first version, strategy is mentioned: *"The study of basic cyber security skills must be included at all levels of education"* and in the update it is stated that all cyber and information and communications technology (ICT) related training programs, including vocational level, will be strengthened (The Security Committee of Finland, 2019).

The EQF is an eight level framework which is designed to facilitate the comparison of national qualifications between EU countries (European Union, 2017). Finnish vocational qualification has been placed in level 4 of the EQF. The updated curriculum of Finnish Vocational Qualification in Information and Communications Technology introduced in August 2020 consists 180 competence points (Finnish National Agency for Education, 2020). The vocational qualification program graduates' students with five different qualification titles. In all of them, the module related to maintaining cyber security can be selected as an optional module.

The National Institute of Standards and Technology (NIST) has been the executor of National Initiative for Cybersecurity Education (NICE) in cooperation with the industry, government, and academia in the United States. Since its establishment in 2010, NICE has developed a working document draft of the NICE

Cybersecurity Workforce Framework (NCWF), and in August 2017 it was published as NIST Special Publication 800-181 (NICE, 2017). The Framework is created to categorize and describe cyber security related work roles and tasks. It is designed to support many different parties including employers, employees, students, educators and technology providers. The framework provides a common lexicon as well as a taxonomy for the cyber security organizations and the workforce regardless of where or for whom the work is done.

At the highest level of the framework, cyber security work then divided into seven categories. Inside the categories, there are 33 separate areas of cyber security work are called specialty areas. Each of them illustrates concentrated work or function in cyber security. The specialty areas contain 52 groupings called work roles, which consist of a set of specific knowledge, skills, and abilities (KSA) required to accomplish different tasks.

To create easier comparability for future researchers globally, in this research, the Finnish vocational qualification titles are converted to match the nearest corresponding NCFW work roles. For the Software Developer qualification title, a work role with the same name and similar work role was found in Securely Provision category. In the Operate and Maintain category two suitable work roles were found: qualification title pairs Network Operations Specialist-Networks Installers and Technical Support Specialist-IT Support Specialist. The mapping used in this research between the NICE framework and the Finnish vocational education can be illustrated in Figure 1.

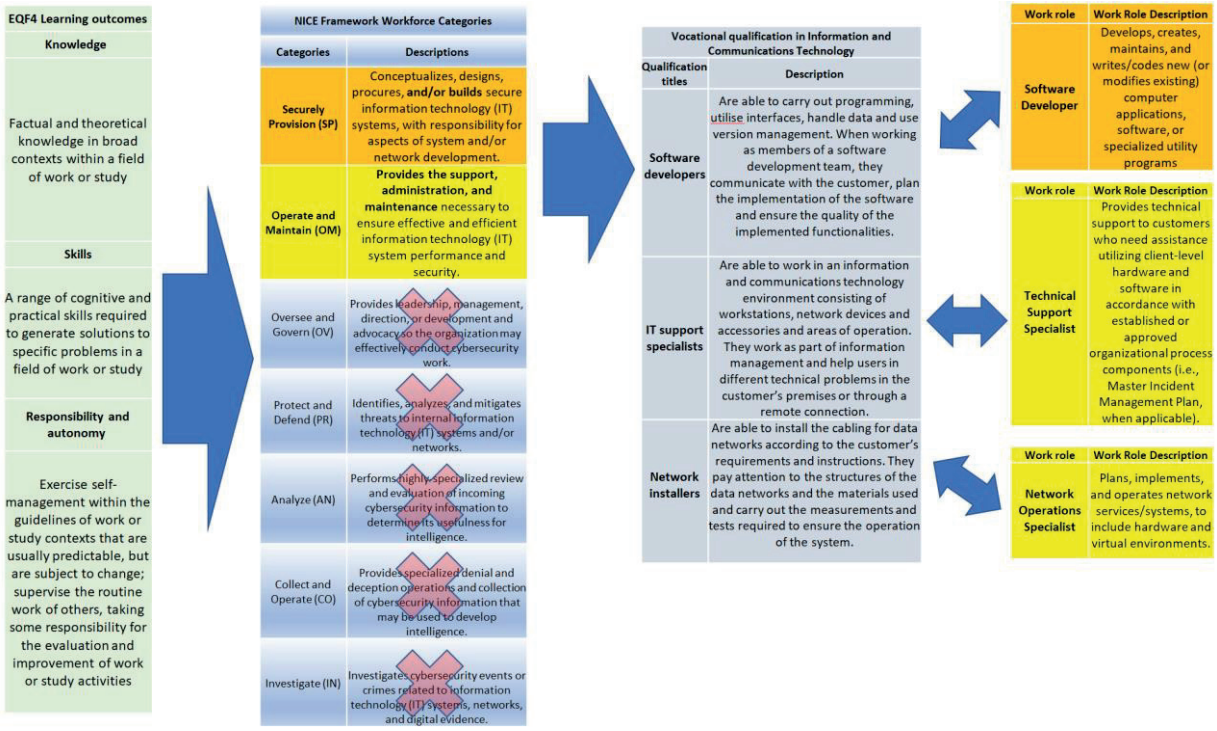


Figure 1: NCFW work roles and vocational qualification titles

2. Earlier research

The NICE framework has been used to develop degree programme structurization through *A Design Model for a Degree Programme in Cyber Security* to provide better targeted work role education for students on the Master's and Bachelor's Degree (Saharinen K., Karjalainen M., Kokkonen T., 2019). The emphases of different quantitative specialty areas have been researched regarding degree programme structuration (Backlund, J., 2020). The NCWF framework was utilized by matching the courses in curricula with the main categories of the framework. The research focused on the university level in the EU and the United States. The research contains a section on how the stakeholder demands between the industry and university education match one another.

Further influence was found in Jyväskylä Educational Consortium researched on the need for cyber security education in 2016 concentrating on Central Finland's SMEs. Simultaneously, also the teachers' perceptions of

cyber security and cyber training were researched (Nevala, J., 2018). Similarly, the C*urrent and future needs of the cyber expertise in public sector organizations* publication researched two public sector organizations and their needs for cyber professional expertise through NCFW framework (Willberg, N., 2017).

Demand, availability and development of the cyber security workforce respond to the need for labor in Finland examined the availability of cyber work in Finland from the recruiting organizations' point of view (Niemelä, J., 2019). In the study, the profile of a cyber professional employee is formed according to the requirements collected from employers. Cyber education in Finland is also evaluated focusing mainly on the universities and the universities of applied sciences.

As seen in the aforementioned paragraphs, there has been previous research on comparison of cyber education and frameworks with labor availability; however, the focus has not been on Finnish vocational education curricula or "apply" level workforce needs. This paper focuses its research on these sections, answering the question: Is vocational level cyber security education necessary as mandated in the Finnish Cyber Security Strategy?

3. Survey research from critical infrastructure the industry

The purpose of this survey was to find out the current suitability of Finnish cyber security education for different critical infrastructure industry in Finland. The main focus of the survey was on the Finnish Vocational Education (or qualification) in Information and Communications Technology. The survey also inquired and measured the importance of the education level and the amount of work experience required from the employer perspective in cyber related recruitment of jobs. Additionally, the labor needs for the cyber sector in Finland concerning near future were inquired about. As mentioned earlier, this research focuses on Network Installer, IT Support Specialist and Software Developer degree programmes and how necessary they are deemed.

The survey aimed at the organizations operating in Finland, which were classified according to sectorial division of the Proposal for a European Cybersecurity Taxonomy (JRC, 2019). The personnel size classification of companies is derived from an EU publication: The new SME definition (Publications Office of the EU, 2005). These commonly used classifications were used in the research to allow comparison with potential future research on the same kind of topic. The survey was conducted anonymously. The questions in the survey were implemented using a structured model to gather quantitative data. The questionnaire survey was active between 10 June 2020 - 26 July 2020 and it received a total of 50 responses. The responses came mainly from telecom operators, ICT service providers, defense sector and other governmental actors. The largest group of respondents were the large enterprises, which employ more than 250 employees. A sufficient number of Finnish actors in the field of critical infrastructure protection was involved. Figure 2 demonstrates the quantitative division of the respondents.

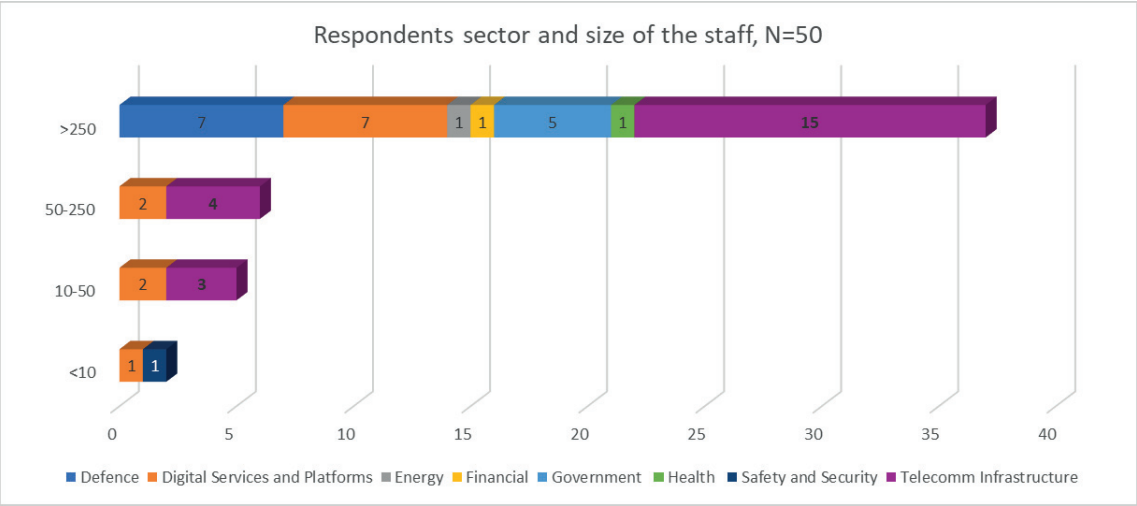


Figure 2: Respondents' sector and size of the staff

4. Results

The respondents were asked to classify the qualification requirements of the cyber security maintenance related module of the curriculum of vocational qualification in Information and Communications Technology (ICT), according to importance of their business.

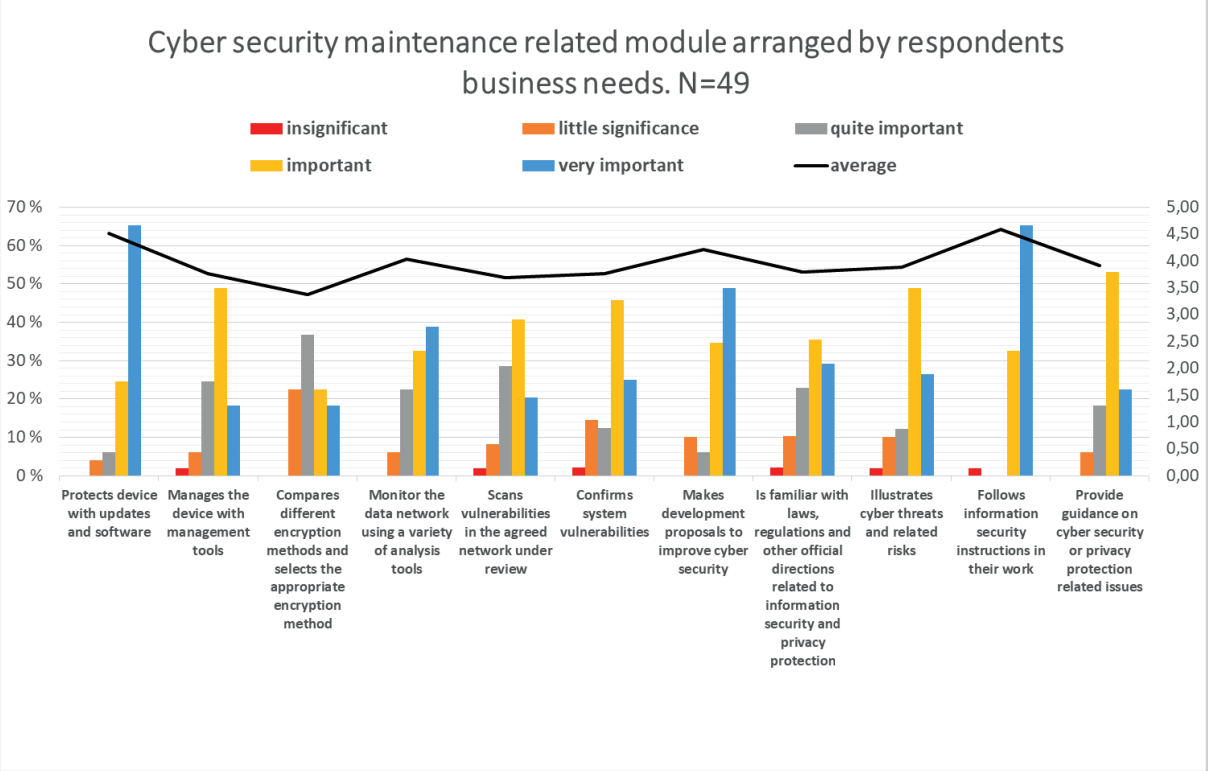


Figure 3: EQF4 Cyber security maintenance related module

On a scale of 1-5, the mean of the responses was 3.96. Two modules even exceeded the 4.5 average, *Follows the information security instructions in their work* was considered the most important topic with 4.59 result, and the second most important topic was *Protects device with updates and software* with 4.51. More than four averages were also reached by topics *Makes development proposals to improve cyber security* 4.22 and *Monitor the data network using a variety of analysis tools* 4.04. Based on the responses, *Compares different encryption methods and selects the appropriate encryption method* 3.37 and *Scans vulnerabilities in the agreed network under review* 3.69 were considered as less important sections. In summary, citing the results it can be stated that respondent organizations highly appreciate that at this level of education daily basic cyber security functions are carried out in accordance with the instructions.

The respondents were asked to classify the relevance of the cyber security modules in JAMK University of Applied Sciences' Information and Communication Technology degree program according to their importance to their business. The following Figure 4 demonstrates this distribution of answers.

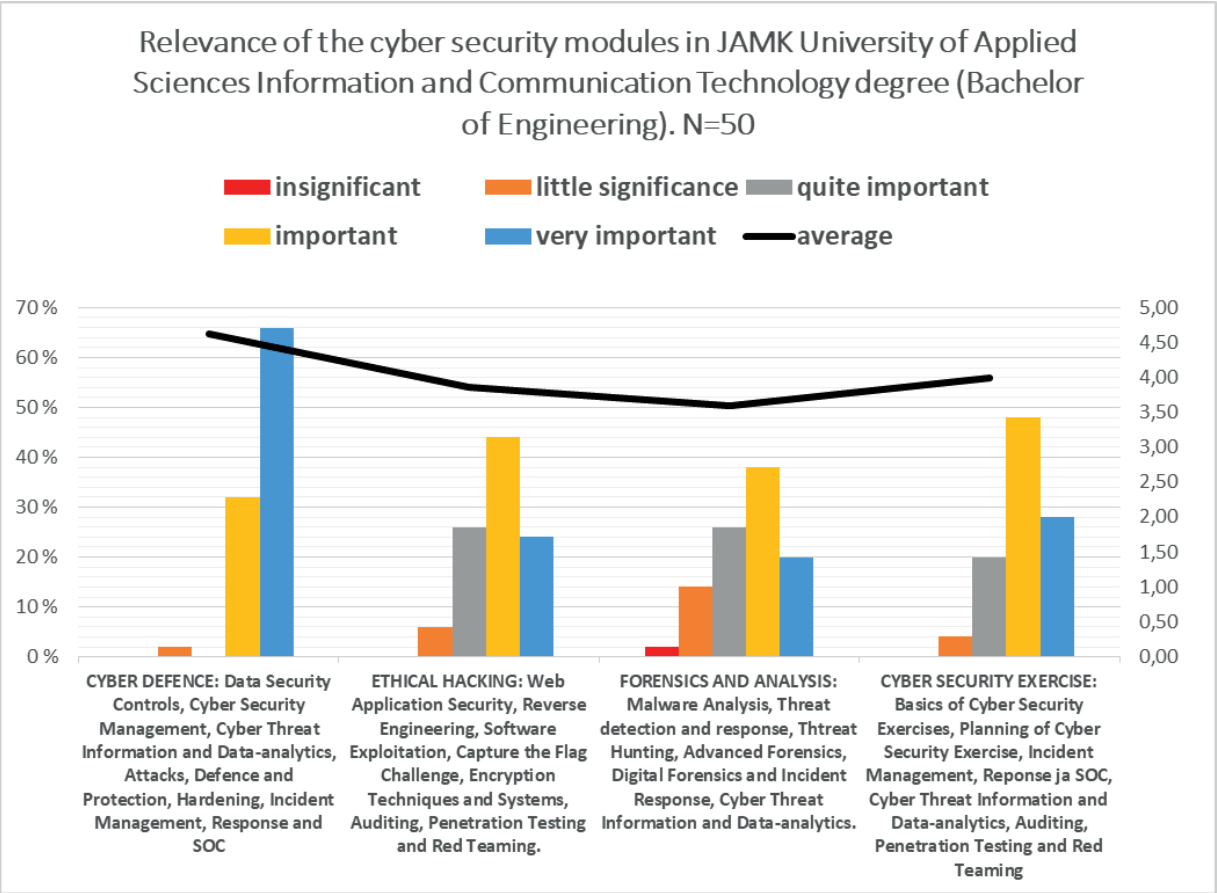


Figure 4: EQF6 Cyber security modules

Based on the responses, the same trend as earlier can also be seen in the content of the EQF6-level cyber security related modules; the modules are broader in content than at the EQF4 level, but there are fewer of them. In this section on a same scale of 1-5, the mean of the responses was 4.02. One module exceeded the 4.5 average: *Cyber defence* was clearly considered as the most important topic with a result of 4.62, and the second most important topic was *Cyber security exercise* with 4.00. *Ethical Hacking* with a 3.86 result and *Forensics and analysis* 3.60 were considered as less important sections. According to the responses, fundamental knowledge of the cyber branch and practical hands-on doing seem to be important, and parts where more in-depth expertise is needed, are seen less relevant at this education level.

The respondents were asked about the near future labor needs of the selected work roles with EQF4-level experience. In this section, Finnish vocational qualification titles are converted to match the nearest corresponding work role in the NICE Cyber Security Workforce Framework work role. The following sample of results is seen in Figure 5: Near future work role needs for the EQF4-level experience

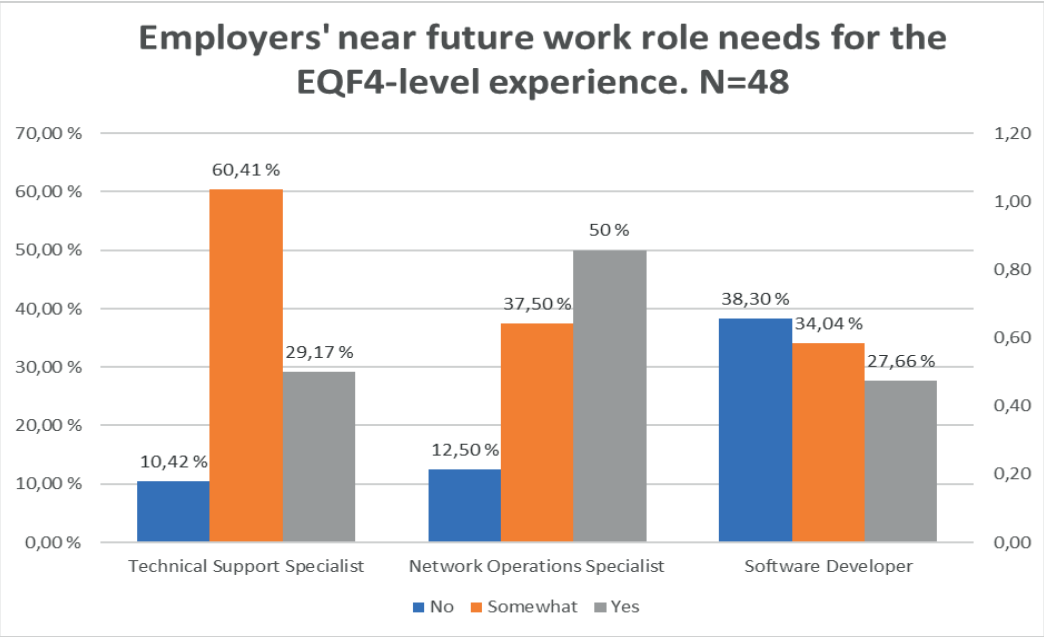


Figure 5: Near future work role needs for the EQF4-level experience

The greatest need for employees at this level of education is for network operations specialist and there may be a demand for technical support specialists. Software developers were the least needed at this level of education. High "Somewhat" bar might be explained by Technical support specialist role, which is often thought of as a helpdesk function, and many companies have outsourced this kind of role over the years. The respondents were asked about the target level of education when recruiting cybersecurity focused staff. In this question, it was possible to select multiple education level choices.

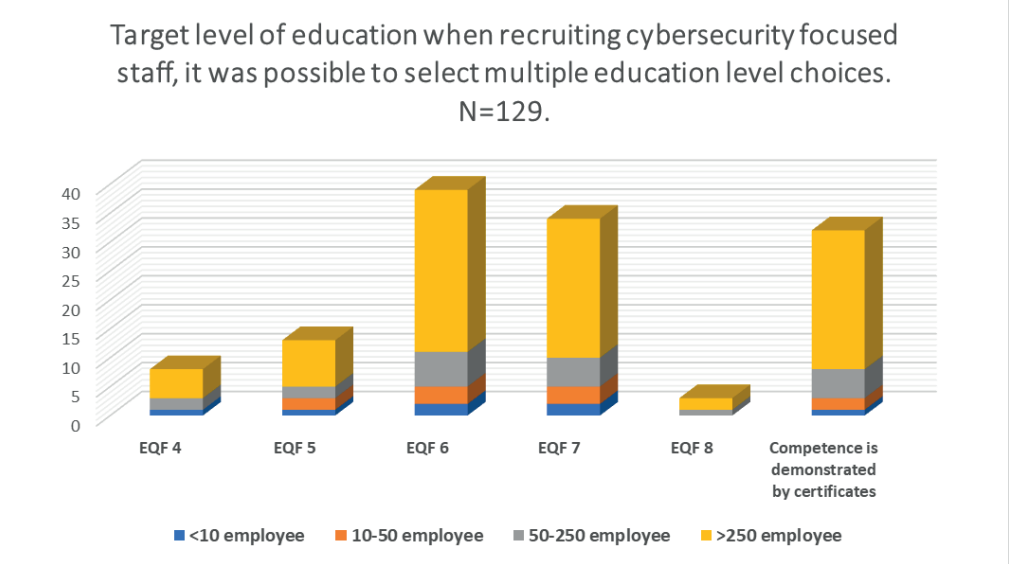


Figure 6: Target level of education

Based on the responses, cyber security related work in general have much higher education level requirements than EQF4-level could provide. University degrees and performed certificates are highly appreciated in the recruitment process. In addition to education level, another significant part in the selection process of the employee is the job applicant's work experience. The respondents were asked about the needed level of experience when recruiting cyber security focused staff. The distribution of target experience levels for recruitment is shown in Figure 7: Target level of experience.

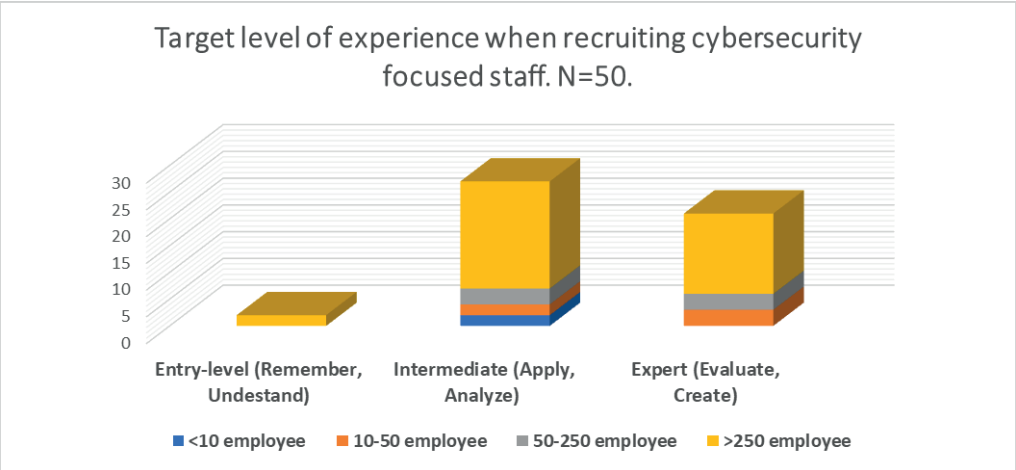


Figure 7: Target level of experience

The recruitment of entry-level employees is seen possible only in large companies. Career paths starting from the entry-level might be too challenging to smaller companies because they usually bind more experienced staff to the orientation process of a new entry-level employee. Based on the answers, intermediate experience level is the most popular class, but also the expert level is quite close to it.

Lastly, the respondents were asked to assess the distribution of their company's near future workforce needs based on the NCFW categories. The vocational qualification titles researched are divided into categories as follows: Securely Provision (SP) category includes vocational qualification title Software Developer. Operate and Maintain (OM) category includes titles Networks Installer and IT Support Specialist.

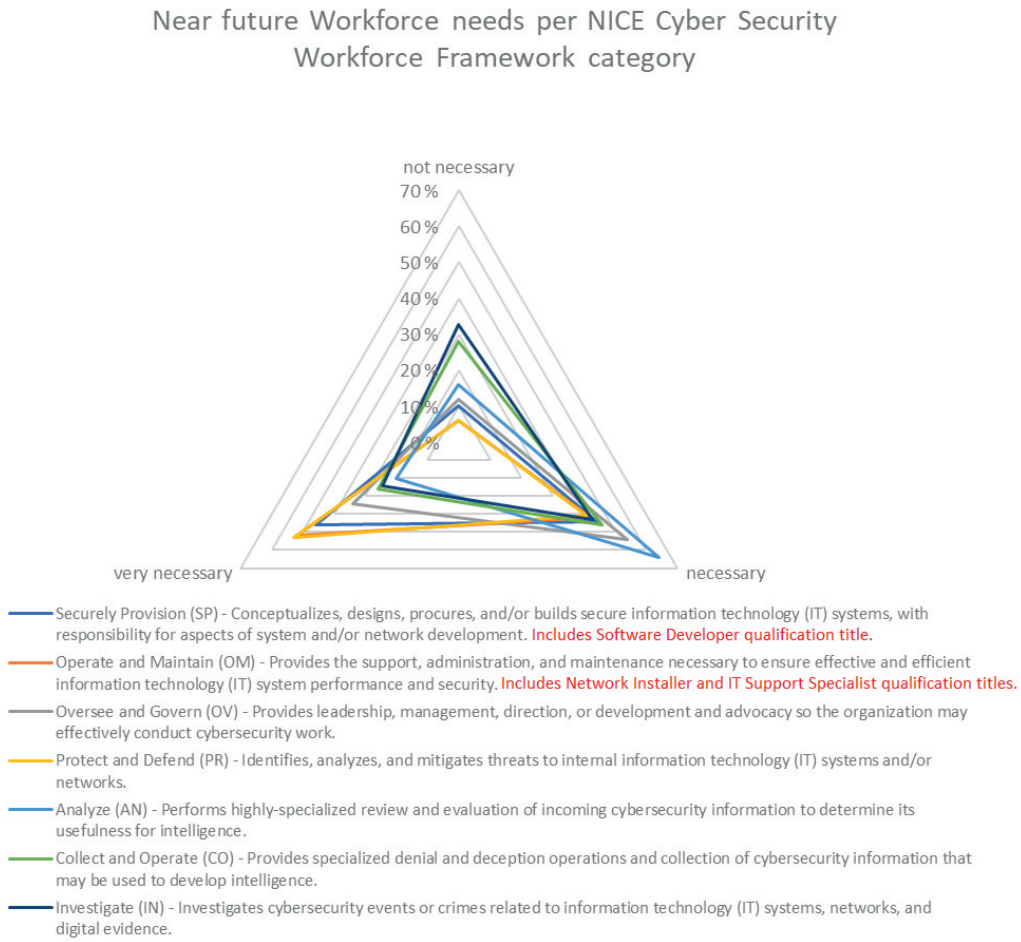


Figure 8: Near future workforce needs per NCFW category

The direction of the desired competence is strongly in Protect and Defend (PR) and Operate and Maintain (OM) categories; Securely Provision (SP) still fits in the top three categories. Analyze (AN) and Oversee and Govern (OV) clearly share the visions of respondent organizations; they both are seen necessary but also not necessary bar is high. Investigate (IN) and Collect and Operate (CO) categories are clearly seen as the least necessary.

Overall, from the employer's view, cyber security related subjects are seen as an important part of Information and Communication Technology education on both EQF-4 and EQF-6 levels. On a scale of 1-5, both modules were seen as averaging around four.

Based on our research, on EQF-4 level it can be stated that the respondents consider compliance of their information security policies to be a very important part of their IT asset protection and expect this from every employee as well. Protection of devices with updates and software can be considered as one of the easiest ways to protect your environment against cyber threats, and this basic protection function seems to be appreciated by employers. Deviation notifications or any security development proposals are always valuable, especially if they are made proactively to mitigate potential threats. Situational awareness is again one of the basic functionalities of protecting an organization's most valuable data assets. Based on these results, the focus of education at this level should be on matched with basic security operations in accordance with the instructions, and more specific specializations should be given little less attention. For comparison, the same trend can be also seen in the content of the EQF-6 level cyber security related modules. The respondents' top rated module covers the basic techniques of cyber security field, and the module rated second goes through them in realistic hands-on exercise.

According to the responses, EQF-4 level education was not seen very appropriate for cyber related labor needs in Finland due to the higher level of education required for the cyber security focused staff. Overall, the chosen work roles were seen moderately appropriate. Generally, the greatest need for employees, out of the chosen degree specializations, at EQF-4 level of education is for Network Operations Specialist. Somewhat perhaps surprisingly, Software Developers were the least needed. Possibly the knowledge of basic techniques is valued more on this level of education, and the competence requirements of Software Developers are on a higher level in the surveyed organizations. The most suitable level of education when recruiting cybersecurity focused staff in Finland was EQF-6 and close to it was EQF-7; also the competence demonstrated in the certificates was considered appropriate.

The experience level of cyber security related employees is expected to be at least intermediate level; entry-level recruitment was only seen possible in two large companies. If the employee has got the ability to apply knowledge and skills in routine work situations without continuous guidance, the employee does productive work at least most of the time and does not appear as a mere expense during work induction. On the other hand, the expert level could be higher if there were enough qualified candidates available for the open cyber related vacancies.

The most needed direction of competence seems to be under Protect and Defend (PR) and Operate and Maintain (OM) categories. Identification, analysis, and mitigation of threats seem to be phenomena that responder companies still want to strengthen internally to have better cyber resilience. This research shows that they are willing to recruit their own employees to enhance the capability. Applications and devices are constantly evolving; hence admins must update and patch existing systems while new features or systems are introduced. They also want to keep these basic functions in their own hands, and an operator for these responsibilities would also be needed internally. These responses describing labor needs show a clear link to needs related to education priorities, strong basic knowledge of computing and information security, and practical hands-on skills are valuable. From the research data of the surveyed companies it can be concluded, that if they use more advanced cyber security services, like forensics, advanced analysis, or ethical hacking services, they might mainly outsource them to high-tech partners and do not recruit these employees themselves. This would explain the low demand for labor in these sectors.

5. Conclusion and Future Research

Based on our research, the profile of most wanted cyber employees' direction of competence is strong system/network administrator who knows how to operate, maintain, and mitigate threats in the environment for which they are responsible, and they should have at least EQF-6 level education and a minimum of intermediate level work experience. The competences demonstrated with certificates were considered very important, so they can be seen as a significant part of professionalism also in the cyber field. An earlier research published in 2019 by Jukka Niemelä states that there is a clear shortage of suitable labor in the cyber sector in Finland. The expected level of competence of the applicants has been lowered, and it is hoped that in the future applicants will have a basic knowledge of the cyber branch and deep expertise in one of the key areas of cyber security. (Niemelä, J., 2019) On this basis, vocational qualification does not solve the problem encountered in the previous research, and in order to gain deep expertise further education or specialization in working life are still needed.

As mentioned earlier, there are no open cyber related vacancies for EQF4-level graduates as inspected by the authors of this paper. However, vocational qualification gives a good starting point for vocational work tasks, as well as the keys for life lasting learning in further education and in career progression. Strong practical hands-on skills should be achieved during vocational training, whether they consist of network technology, programming, or different operating systems. If it is desired to steer career pathway from the basic ICT tasks to the direction of cyber security, the options are either to carry out industry certifications or accomplish further education. The aim of further education should be to deepen strong basic skills to the specialization in the chosen cyber expertise area.

For future research, it would be interesting to investigate how cyber security has been implemented in other countries "on all levels of education" as Finland's cyber security strategy mandates. The qualitative research data also emphasized the 'soft skills' of sought out employees, not just the 'hard technical skills'. It is also a debatable subject, where the subject of cyber security should be sectioned and emphasized as an own educational field, as many of the curriculum proposals currently entangle it along every subject. This could be investigated through the workforce demand for different levels of education.

Acknowledgements

This work has been done in Jyväskylä University of Applied Science (JAMK) which is participating the Cyber Security Network of Competence Centres for Europe (CyberSec4Europe) project of the Horizon 2020 SU-ICT-03-2018 program. https://cybersec4europe.eu/about/

The authors would like to thank Tuula Kotikoski for her contribution in proofreading the English language on the paper.

References

Backlund, J. (2020) Examination of contemporary cyber security education [Online]. Available at URL http://urn.fi/URN:NBN:fi:amk-2020060416851 [Accessed 25 August 2020].
European Union (2017) Description of the eight EQF levels [Online]. Available at URL https://europa.eu/europass/en/description-eight-eqf-levels [Accessed 5 September 2020].
Finnish National Agency for Education (2020) Qualification requirements entered into force on 01.08.2020 (OPH-2596-2019) [Online]. Available at URL https://eperusteet.opintopolku.fi/eperusteet-service/api/dokumentit/6941346 [Accessed 25 August 2020].
Joint Research Centre (JRC), the European Commission's science and knowledge service (2019) A Proposal for a European Cybersecurity Taxonomy [Online]. Available at URL https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf [Accessed 5 September 2020].
National Initiative for Cybersecurity Education (2017) Cybersecurity Workforce Framework [Online]. Available at URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf [Accessed 1 August 2020].
Nevala, J. (2018) Cybersecurity situation analysis - Survey in Central Finland 2016-2018 [Online]. Available at URL http://urn.fi/URN:NBN:fi:amk-2018121721956 [Accessed 19 September 2020].

Niemelä, J. (2019) Demand, availability and development of the cyber security workforce respond to the need for labor in Finland [Online]. Available at URL http://urn.fi/URN:NBN:fi:jyu-201906032891 [Accessed 25 August 2020].
Publications Office of the EU. (2005) The new SME definition [Online]. Available at URL https://op.europa.eu/en/publication-detail/-/publication/10abc892-251c-4d41-aa2b-7fe1ad83818c [Accessed 5 September 2020].
Saharinen K., Karjalainen M., Kokkonen T., (2019) A design model for a degree programme in cyber security [Online]. Available at URL https://doi.org/10.1145/3369255.3369266 [Accessed 25 August 2020].
The Security Committee of Finland (2013) Finland's Cyber security Strategy [Online]. Available at URL https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf [Accessed 29 August 2020].
The Security Committee of Finland (2019) Finland's Cyber security Strategy 2019 [Online]. Available at URL https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf [Accessed 29 August 2020].
Willberg, N. (2017) Current and future needs of the cyber expertise in public sector organizations [Online]. Available at URL http://urn.fi/URN:NBN:fi:jyu-201706243034 [Accessed 25 August 2020].

PV

CYBER RANGE - PREPARING FOR CRISIS OR SOMETHING JUST FOR TECHNICAL PEOPLE?

by

Jani Paijanen, Karo Saharinen, Jarno Salonen, Tuomo Sipola, Jan Vykopal and Tero Kokkonen 2021

20th European Conference on Cyber Warfare and Security, 24th - 25th June 2021, Chester, UK.

DOI: https://doi.org/10.34190/EWS.21.012
URN: https://urn.fi/URN:NBN:fi-fe2021111956073

Cyber Range: Preparing for Crisis or Something Just for Technical People?

Jani Päijänen[1], Karo Saharinen[1], Jarno Salonen[2], Tuomo Sipola[1], Jan Vykopal[3] and Tero Kokkonen[1]
[1]JAMK University of Applied Sciences, Jyväskylä, Finland
[2]VTT Technical Research Centre of Finland, Tampere, Finland
[3]Masaryk University, Brno, Czech Republic
jani.paijanen@jamk.fi
karo.saharinen@jamk.fi
jarno.salonen@vtt.fi
tuomo.sipola@jamk.fi
vykopal@ics.muni.cz
tero.kokkonen@jamk.fi
DOI: 10.34190/EWS.21.012

Abstract: Digitalization has increased the significance of cybersecurity within the current highly interconnected society. The number and complexity of different cyber-attacks as well as other malicious activities has increased during the last decade and affected the efforts needed to maintain a sufficient level of cyber resilience in organisations. Due to Industry 4.0 and the advanced use of IT and OT technologies and the adaptation of IoT devices, sensors, AI technology, etc., cybersecurity can no longer considered to be taken lightly when trying to gain a competitive advantage in business. When transferring from traditional reactive cybersecurity measures to proactive cyber resilience, cyber ranges are considered a particularly useful tool for keeping the organisation in the game. With their background in defence research (e.g., DARPA NCP in 2008), cyber ranges are defined as interactive simulated platforms representing networks, systems, tools, and/or applications in a safe, legal environment that can be used for developing cyber skills or testing products and services. Cyber ranges can be considered vital in facilitating and fostering cybersecurity training, certification, and general education. Despite the definition, cyber ranges seem to be only used by military or so-called "technical people" when quite a few more organisations could benefit from them. This article attempts to reveal the secrets behind cyber ranges and their use focusing on suitable target environments, common functions, and use cases. Our main objective is to identify a classification of cyber ranges and skills related to these diverse types of ranges. We emphasise the cyber resilience of any type of organisation that demands the use of cyber range type of training. Different training scenarios improve different sets of organisational skills. The article is based on an extensive survey on cyber ranges, their use, and technical capabilities that was conducted in CyberSec4Europe project.

Keywords: cyber range, cyber resilience, cyber training, organisational skills, cybersecurity

1. Introduction

Given the concept of a cyber crisis (or even cyber war), one has to imagine a cyber weapon being used in a cyber-attack, for example of a malware program or a denial-of-service attack. This attack is usually directed towards a victim (organization or person) that is facing a crisis situation. Different countries have different laws protecting the victim against this kind of aggression. Outside the realm of cyber security, there are usually various kinds of laws prohibiting and restricting the usage of physical weapons, even to the point of having specialized physical shooting ranges abiding the law (Ministry of Interior, Finland, 1998/2003) for the practice of regular weaponry. In the cyber context, these kinds of cyber weapon shooting ranges are being formed as cyber arenas or cyber ranges; however, the development of regulations on how these platforms should be used is currently lacking.

Cyber ranges (or cyber arenas) are technical platforms that facilitate education, training, and exercise of cyber security (Karjalainen and Kokkonen, 2020a). According to Russo, Costa and Armado (2020), these ranges are complex infrastructures that simulate real-world cybersecurity scenarios. These technical platforms have developed in different organizations simultaneously from smaller technical laboratory environments to cloud-based solutions. They might have originally been platforms used to demonstrate products and technology, or even mirroring a technical production network to act as an introductory platform for new employees. Ukwandu et al (2020) have identified current trends, types, target domains and technologies used in cyber ranges and testbeds. On the other hand, the definition of cyber ranges does not limit or restrict use cases, target groups, or participant roles utilizing a cyber range (ECSO, 2020).

2. At whom cyber ranges are targeted?

Cyber ranges can be used for training or educating individuals or groups of people such as employees of companies or organisations. They can be used for cyber security research and development, hosting various kinds of events, certifying products or services, performing competence assessment, or recruiting people (ECSO, 2020; Yamin, Katt, and Gkioulos, 2020). Some cyber ranges can be used to train cyber defence (NATO CCDCOE, 2020; Vykopal at al, 2017). Events in a cyber range can be cyber security exercises or competitions targeted at a company (FINGRID, 2017), an organisation (Valtori, 2020; MITRE, 2014), international (NATO CCDCOE, 2020), or national cyber security exercises (Secretariat of the Security Committee, 2019). An exercise can target a specific audience without any shared training or background (CyberSec4Europe, 2021). Also, various cyber security related competitions such as Capture the Flag (CTF) competitions targeted at individuals or teams can be organised as a cyber range event. Firstly, the following sections introduce target groups benefiting from cyber ranges and secondly, use cases that the cyber ranges have supported.

2.1 Target groups

Individuals, Personal Knowledge, Skills and Abilities (KSA)

Cyber ranges offer a technical environment where citizens can train their understanding of the cybersecurity phenomena. The European Union has produced the European Qualifications Framework (EQF), which helps to improve transparency, comparability, and portability of people's qualifications between the nations in the EU. These qualifications are listed as learning outcomes Knowledge, Skills and Abilities (KSAs). Cyber ranges could be used in a Cyber Security Massive Open Online Course (MOOC) implementation (Fischer-Hübner et al., 2020), where the MOOCs offer a platform for everyone to improve their KSAs.

Curriculum students

These KSAs are developed through degree programmes following a curriculum suited for the respected EQF level. Curriculum students of higher education (Karjalainen, Kokkonen and Puuska 2019; Saharinen et al, 2019; Karjalainen and Kokkonen, 2020b) are sometimes required to pass courses that utilize these cyber ranges. Regardless these courses being either a mandatory or elective part of their studies, many education and research organizations are developing the capability (Frank et al, 2017) to host courses through these environments as the demand for capable workforce increases constantly in the field of Cyber Security.

Companies

Companies invest in protecting their environments, as digitalization is forcing them to be increasingly available online both in the private and public sectors. To uphold these availability requirements, companies need to employ a capable workforce provided by the education sector (Bell and Oudshoorn, 2018). Students with practical knowledge of handling a live cyber crisis are often valued, and the capability of upholding the cyber presence of a company simultaneously with a cyber crisis can be seen as a part of the cyber resilience of a nation.

Law enforcement

Additionally, individuals face the problem of a cyber crisis when e.g., their digital identity is stolen, or payment frauds are committed in the e-banking realm (Singh and Rastogi, 2018). In both companies and individual cases, these cyber crises end up in police cybercrime statistics. Cybercrimes are investigated by specialized police units that survey and handle cybercrimes for prosecution. Exact methods of cybercrime investigation are still a developing field, which also means the police forces need an educational environment for investigating cybercrimes.

Government

If the cyber crisis that either faces companies or individuals exceeds a certain threshold, a nation has to implement its laws and regulations to enter a state of war (Sevis and Seker, 2016). This means, depending on the country in question, that the military can start protecting its civilians and assets, be they physical or cyber.

After these laws or regulations are invoked, the protection of assets is commonly left to the nation's military forces.

Military cyber defence capabilities

The Defence Forces of different countries have been mentioned to use National Cyber Ranges: Norway (NTNU, 2018), Estonia (Republic of Estonia Centre of Defence Investment, 2020) and Finland (JYVSECTEC, 2017; EU2019.fi, 2019) to name a few. Additionally, multinational coalitions have practiced in self-contained cyber ranges brought about for the need, for example, Locked Shields (NATO CCDCOE, 2020). Different military forces have stated that cyber is the fifth domain of warfare after land, sea, air, and space (NATO, 2016).

Researchers

All the aforementioned entities have Cyber Security researchers (ENISA, 2020a; 2020b; 2020c) working separately and in coalition on different research projects. The development of cyber ranges as such is a less researched area, as the phenomena and results after working in the cyber range are typically more sought after.

2.2 Use cases for cyber ranges

Security research, testing, development, and certification: Development testbeds, research environments, and certification tracks have been used in the industry for longer than the term Cyber Range has existed. Development testbeds are usually set up by development teams to see how their updates work in an environment mimicking the production environment. Research environments aim at closeness to the real thing, or a phenomenon is researched by scientists, often relying on ICT environments separated from the Internet. Certification bodies require that the test samples pass through a set of phases on a track in order to gain a label of quality provided by the entity awarding the certificates.

Security Education through Competence Building and Assessment: Competence building follows the said certification bodies to offer practicing environments, i.e. cyber ranges, for students trying to reach validation for their skills. This thought has brought up the environment itself to be an active area for student assessment how their competence has developed while working within the environment.

Development of Cyber Capabilities and Resilience: The earlier mentioned competence building is a part of an individual's growth as an expert. The development of cyber capabilities and resilience looks at the phenomenon, outcomes using a cyber range, from the organisation´s viewpoint, e.g. Fingrid, 2017. One part of it is recruitment, where organizations look for competent workforce, and the interview process might have recruitment sections handled in a technical cyber environment. Additionally, ongoing personnel might be trained using organizational exercises.

Cross-domain development environment (Digital Dexterity): The digital dexterity of the whole domain is developed when multiple organisations from multiple industries participate in a cyber range dedicated to the particular industries. These exercises usually show the weak points of processes in multiple organizations, e.g., supply chain processes.

National and International Cybersecurity Competitions or Exercises: National or international cybersecurity competitions, in which individuals, organizations or nations compete against one another as well as national and international cyber security exercises, may both advance all the aforementioned use cases.

3. Cyber range usage based on a survey

In this section, we analyse the data from a conducted cyber range survey. The survey was conducted in the CyberSec4Europe project, and it was open from 23 April 2020 to 27 May 2020. A total of 44 responses were received, of which 39 responses were considered valid. The number of survey responses, 39, is considered valid based on the survey authors' experience in the subject. In the survey terms, we decided not to publish any cyber range specific features and capabilities. The survey consisted of single-choice, multiple-choice and open questions, and it did not contain any mandatory fields. (CyberSec4Europe, 2020)

3.1 Cyber range target groups

The survey data had a total of seven target groups (TGs) listed, and respondents provided three additional target groups. Hence, the data comprised a total of ten target groups: General public, Secondary level students, Degree program students (Bachelor's or Master's degree students), Government organizations, Companies and Enterprises, Non-profit associations or similar, Other, and respondent reported Training Service Providers, Systems Integrators, and Cyber Professionals. The respondents belonged to the following target groups: Training Service Providers, Systems Integrators and Cyber Professionals. They are presented in the columns of Figure 1. The most represented target groups were Companies and Enterprises 77% (30), Degree program students (Bachelor or Master's degree students) 59% (23), Government organizations 59% (23), Non-profit associations or similar 23% (9), General Public 18% (7) and Secondary level students 18% (7). The following groups were represented in the data by just one respondent: Training Service Providers, Systems Integrators, Cyber Professionals and Other. The top 20% of the cyber ranges supported four or more target groups.

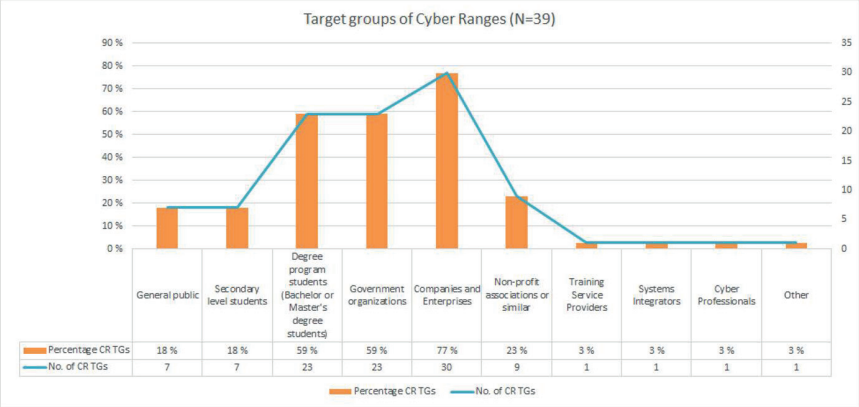


Figure 1: Distribution of target groups (N=39)

The number of target groups supported by cyber ranges is shown in Figure 2. Single Target Group was reported by 23% (9), two target groups by 28% (11), three target groups by 26% (10), four target groups by 13% (5), five target groups by 5% (2), and six target groups by 5% (2). Based on the survey data, a cyber range supports two (2.6) target groups on average.

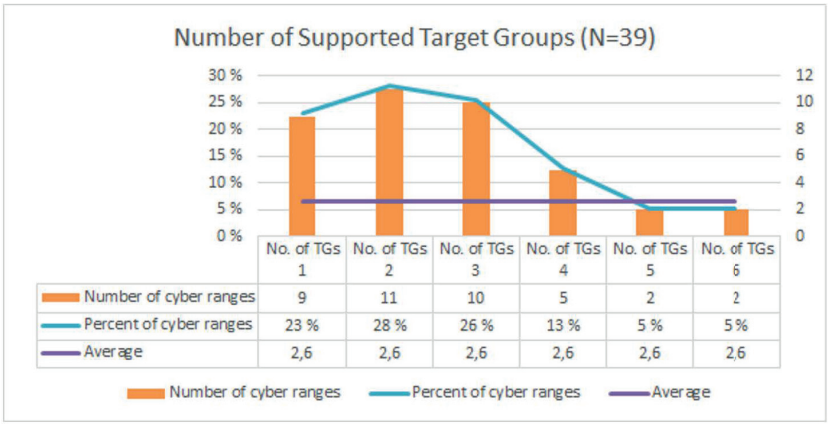


Figure 2: Number of supported target groups (N=39)

3.2 Cyber range use cases

A cyber range may be dedicated to a single use case, or it may support multiple use cases. The survey data contained 11 use cases, namely Security testing and certification, Security research & development, Competence Building, Security Education, Development of Cyber Capabilities, Development of Cyber Resilience, Competence Assessment, Recruitment, Cross-domain development environment (Digital dexterity), National and International Cybersecurity Competitions, and National and International Cybersecurity Exercises. The reported use cases were distributed (Figure 3) as Security testing and certification 44% (17), Security research & development 72% (28), Competence Building 62% (24), Security Education 82% (32), Development of Cyber Capabilities 51% (20), Development of Cyber Resilience 38% (15), Competence Assessment 36% (14),

Recruitment 13% (5), Cross-domain development environment (Digital dexterity) 13% (5), National and International Cybersecurity Competitions 26% (10), National and International Cybersecurity Exercises 44% (17).

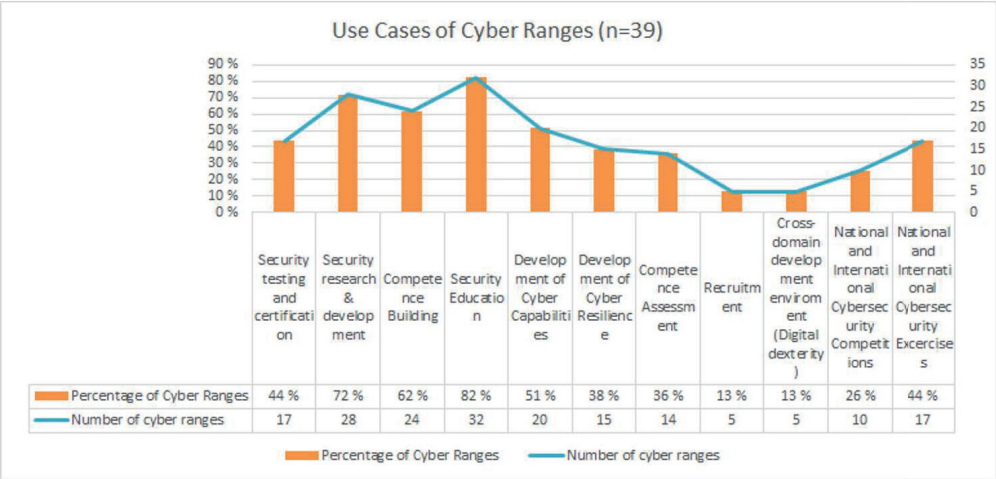


Figure 3: Distribution of use cases (N=39)

Figure 4 displays the number of the use cases (No. of UCs) supported by the cyber ranges. All eleven use cases were supported by 5% (2), ten use cases by 5% (2), nine use cases by 5% (2), eight use cases by 3% (1), seven use cases by 10% (4), six uses cases by 10% (4), five use cases by 10% (4), four use cases by 10% (4), three use cases by 13% (5), two use cases by 13% (5), one use case by 15% (6) cyber ranges as reported by the respondents. On average, a cyber range supports four (4.79) use cases. The top 20% of cyber ranges supported eight or more use cases.

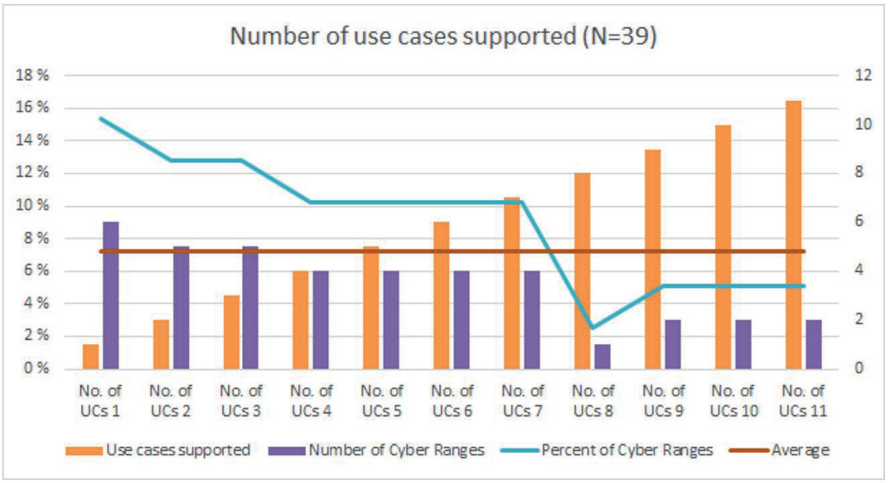


Figure 4: Number of use cases supported by cyber ranges (N=39)

3.3 Cyber range participant roles

Six user roles were listed: Director (Business, Director, Communication, etc.), Developer, Researcher, Security professional, Educator, and Other. The survey respondents reported to option "Other" with the following: Sysadmin, Network admin, Student, Job Applicants, Employees, Domain specialist. Two respondents responded "Different roles from organisations which are responsible for some parts of cyber incident response & handling (e.g. Public relations, Process owners, System owners, Technical specialists)" and "CISO, Incident managers, depending on the roles in organisations (e.g. IT admins)."

The number of participant roles is shown in Figure 6: one role 21% (8), two roles 23% (9), three roles 28% (11), four roles 13% (5), and five roles 13% (5). One respondent (3%) did not report the number of participant roles. On average, a cyber range supports two participant roles (2.66%). No cyber ranges were reported to support all roles, including the "Other" role.

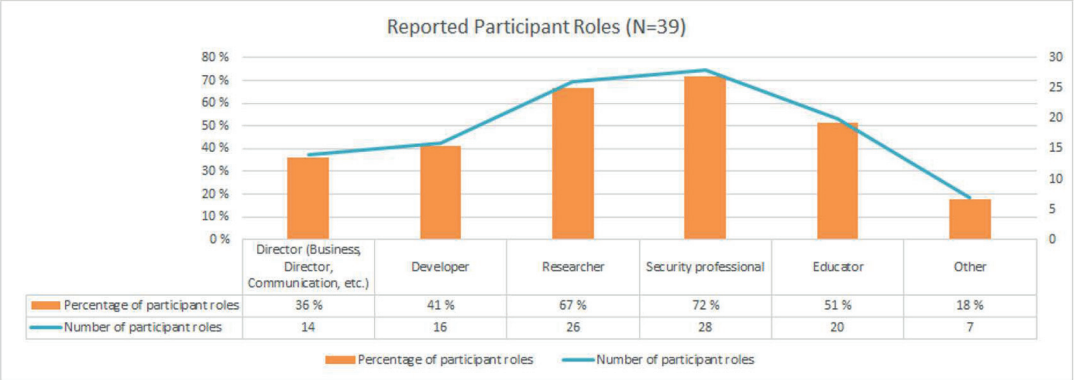


Figure 5: Distribution of participant roles

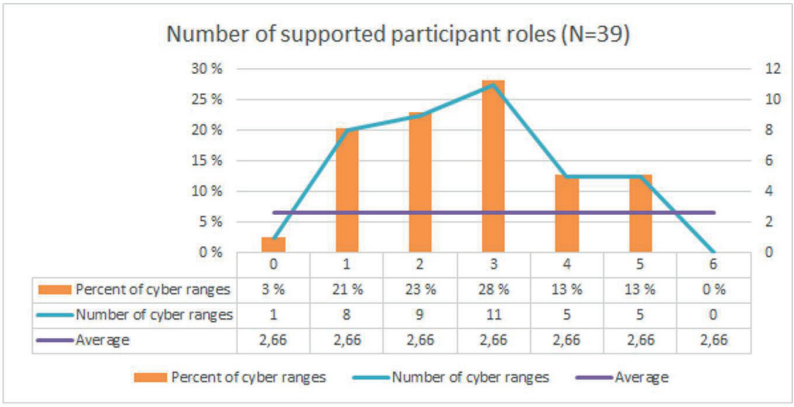


Figure 6: Number of participant roles supported (N=39)

3.4 Cross-tabulation of cyber range use cases and participant roles

Table 1 shows the cross-tabulation of filtered data, where target groups were Government organizations, Companies and Enterprises, or Non-profit associations or similar. It shows which use cases a cyber range supports, and the user roles supported. The table rows represent use cases and the columns the user roles. The number following a use case reports the total number of times the use case was reported: Security testing and certification (57), Security research & development (90), Competence Building (75), Security Education (85), Development of Cyber Capabilities (62), Development of Cyber Resilience (50), Competence Assessment (47), Recruitment (20), Cross-domain development environment (Digital dexterity) (21), National and International Cybersecurity Competitions (35), National and International Cybersecurity Exercises (54). In total, the user roles shown in the table were reported as follows: Director (Business, Director, Communication, etc.) 83 times, Developer 94 times, Researcher 145 times, Security professional 161 times, Educator 106 times, and Other User Roles seven times. In each use case the reported cyber ranges supported all the roles, except Other User Roles.

Table 1: Cross-tabulation of use cases with participant roles, filtered.

Use case	Director	Developer	Researcher	Security professional	Educator	Other User Roles	Total
Security testing and certification	8	10	14	14	11	0	**57**
Security research & development	11	15	22	20	15	7	**90**
Competence Building	9	12	18	22	14	0	**75**
Security Education	11	12	21	24	17	0	**85**
Development of Cyber Capabilities	10	10	15	17	10	0	**62**
Development of Cyber Resilience	8	8	11	14	9	0	**50**
Competence Assessment	6	7	11	14	9	0	**47**
Recruitment	3	3	5	5	4	0	**20**
Cross-domain development enviroment (Digital dexterity)	4	4	5	5	3	0	**21**
National and International Cybersecurity Competitions	4	5	10	10	6	0	**35**
National and International Cybersecurity Excercises	9	8	13	16	8	0	**54**
Total	**83**	**94**	**145**	**161**	**106**	**7**	**596**

4. Discussion

According to the research data, cyber ranges had various target groups (Figure 1), and the supported participant roles of cyber ranges were not limited to technically oriented user roles, but there were roles for e.g., directors (Figure 5). The cyber ranges supporting directors as a potential participant role, support a broader spectrum of use cases (Table 1). The data indicates that cyber ranges were used by both technical and non-technical user roles.

When an entity, e.g., an organisation, a company or an individual faces a cyber incident, it does not require only technical skills to understand, resolve and respond to the incident but also non-technical skills are required (Fingrid, 2017). An organisation may establish a Cyber Security Incident Response Team (CSIRT) that tries to respond to and resolve the attack. According to Onwubiko and Ouazzane (2020), CSIRTs should have the necessary expertise and support from the infrastructure and networking teams, systems administration and management teams, business continuity and disaster recovery teams, communications and press office, and designated senior management teams. In case of severe enough incident, senior management could provide decision-making and funding support; a cyber incident may require a dedicated cost-budget that only the senior management can allocate. The CSIRT example and exercising or training for incidents can be seen as preparing for a local and limited duration crisis. The work to recover from a cyber incident may last long, even several months, depending on the size of the organisation. In larger organisations, the CSIRT team contains these dedicated roles.

In conclusion, the key question of this article "Are cyber ranges just for technical people or do they actually provide vital tools for the organisation to prepare against a crisis?", we might say that based on our research results, cyber ranges enable the organisations to carry out more than just technical mitigation measures. However, this highly depends on the decisions made by the organisation itself on how well they take the different functionalities into use and make full use of the platform. Simply said, a cyber range acquired only for a specific technical purpose might be somewhat limited in terms of functionality. Since there are quite a few cyber range platforms available on the market with various features ranging from single technical point solutions to comprehensive cyber arenas including realistic simulation of business processes and technical systems, selecting the right tool for a specific organisation might require thorough examination of available options and possibly even external consultation.

The research results show that some cyber ranges support or have participated in national or international cybersecurity exercises. Such exercises, when exercising joint operations of civil government and authorities, or security authorities, require there to be non-technical participants, so that the areas of responsibilities as stated by national or international laws are followed.

Individuals, cyber professionals, government organisations, companies and enterprises, and degree program students use cyber ranges for competence building and development. The business features and domains as well as the technical features and functionalities they provide for users should be researched further. As the original survey was not specifically designed for the purpose of analysing the scope of educational cyber range use, there is a definite need for a new survey. The questions should be adjusted so that their scope focuses more on the previously studied subject and perhaps includes multiple different subjects. Future research might focus on the features, functionalities and properties of cyber ranges which have been reported to support non-technical roles for a better understanding of the potential use cases that they could participate for.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgments

This research was supported by the Cyber Security Network of Competence Centres for Europe (CyberSec4Europe) project of the Horizon 2020 SU-ICT-03-2018 program, and by the ERDF project "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

The authors would like to thank Ms. Tuula Kotikoski for proofreading the manuscript.

References

Bell S. and Oudshoorn M. (2018) "Meeting the Demand: Building a Cybersecurity Degree Program with Limited Resources," *2018 IEEE Frontiers in Education Conference (FIE)*, San Jose, CA, USA, 2018, pp. 1-7, DOI: 10.1109/FIE.2018.8659341.

CyberSec4Europe. (2020) "D7.1 Report on existing cyber ranges, requirements", [online], Cyber Security for Europe (CyberSec4Europe), https://cybersec4europe.eu/wp-content/uploads/2020/09/D7.1-Report-on-existing-cyber-ranges-and-requirement-specification-for-federated-cyber-ranges-v1.0_submitted.pdf

CyberSec4Europe. (2021) "CyberSec4Europe Hosting Flagship 1: An Online Cybersecurity Exercise", [online], Cyber Security for Europe (CyberSec4Europe), https://cybersec4europe.eu/cybersec4europe-hosting-flagship-1-an-online-cybersecurity-exercise/

ECSO. (2020) Understanding Cyber Ranges: From Hype to Reality. [Online]. Available at: https://ecs-org.eu/documents/publications/5fdb291cdf5e7.pdf, European Cyber Security Organisation (ECSO), Brussels, Belgium.

ENISA. (2020a) "ENISA Threat Landscape 2020 - Insider Threat". ISBN:978-92-9204-354-4. DOI:10.2824/552242

ENISA. (2020b) "ENISA Threat Landscape 2020 - Main incidents", [online], European Union Agency for Network and Information Security (ENISA), Science and Technology Park of Crete (ITE), Heraklion, Greece, Heraklion, Greece, https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

ENISA. (2020c) "ENISA Threat Landscape 2020 - The year in review", [online], European Union Agency for Network and Information Security (ENISA), Science and Technology Park of Crete (ITE), Heraklion, Greece, Heraklion, Greece, https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

FINGRID magazine. (2017) "Cyber security is ensured with genuine exercises, [online], Fingrid Oyj, https://www.fingridlehti.fi/en/cyber-security-ensured-genuine-exercises/

Finnish Ministry of Interior. (2015). "Firearms Act", [Online], https://www.finlex.fi/fi/laki/kaannokset/1998/en19980001.pdf.

EU2019.fi (2019) "Cyber Ranges Federation – Towards Better Cyber Capabilities Through Cooperation" [online], Finnish Presidency of the Council of the European Union (EU2019.fi), https://eu2019.fi/en/-/cyber-ranges-federation-yhteistyolla-kohti-parempaa-kyberkyvykkyytta

Fischer-Hübner S. et al. (2020) Quality Criteria for Cyber Security MOOCs. In: Drevin L., Von Solms S., Theocharidou M. (eds) Information Security Education. Information Security in Action. WISE 2020. IFIP Advances in Information and Communication Technology, vol 579. Springer, Cham. https://doi.org/10.1007/978-3-030-59291-2_4

Frank, M., Leitner, M. and Pahi, T. (2017) "Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education," 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Orlando, FL, 2017, pp. 38-46, DOI: 10.1109/DASC-PICom-DataCom-CyberSciTec.2017.23.

JYVSECTEC (2017) "JYVSECTEC success story", [online], Jyväskylä Security Technology (JYVSECTEC), https://jyvsectec.fi/2017/02/jyvsectec-success-story/

K. N. Sevis and E. Seker, "Cyber warfare: terms, issues, laws and controversies," 2016 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), London, 2016, pp. 1-9, DOI: 10.1109/CyberSecPODS.2016.7502348.

Karjalainen, M., Kokkonen T. and Puuska, S. (2019) "Pedagogical Aspects of Cyber Security Exercises", IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Stockholm, Sweden, pp 103–108. DOI: 10.1109/EuroSPW.2019.00018

Karjalainen, M. and Kokkonen, T. (2020a) "Comprehensive Cyber Arena; The Next Generation Cyber Range", 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, pp. 11–16. DOI: 10.1109/EuroSPW51379.2020.00011.

Karjalainen, M. and Kokkonen, T. (2020b) "Review of Pedagogical Principles of Cyber Security Exercises", Advances in Science, Technology and Engineering Systems Journal, Vol 5, No 5, pp 592–600. DOI: 10.25046/aj050572.

NATO. (2016) "NATO Cyber Defence" [Online]. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf

NATO CCDCOE. (2020) "Exercises", [Online]. Available at: https://ccdcoe.org/exercises/.

NTNU. 2018. Norwegian University of Science and Technology. "Norwegian Cyber Range". https://www.ntnu.no/ncr

Onwubiko C., Ouazzane, K. (2020) "SOTER: A Playbook for Cybersecurity Incident Management", IEEE Transactions on Engineering Management, DOI: 10.1109/TEM.2020.2979832.

Republic of Estonia Centre of Defence Investment. 2020. "Estonia Signs Contract to Develop Command Platform for NATO Cyber Range". [Online]. Available at: https://www.kaitseinvesteeringud.ee/en/estonia-signed-a-contract-for-the-development-of-a-command-platform-for-the-nato-cyber-range/

Russo, E., Costa, G, Armado, A. (2020) "Building next generation Cyber Ranges with CRACK", Computers & Security, Vol 95, pp. 101837. DOI: 10.1016/j.cose.2020.101837.

Singh S. K. and Rastogi N. (2018). "Role of Cyber Cell to Handle Cyber Crime within the Public and Private Sector: An Indian Case Study," 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, 2018, pp. 1-6, DOI: 10.1109/IoT-SIU.2018.8519884.

Saharinen K., Karjalainen M., and Kokkonen T. (2019) "A Design Model for a Degree Programme in Cyber Security". In Proceedings of the 2019 11th International Conference on Education Technology and Computers (ICETC 2019). Association for Computing Machinery, New York, NY, USA, 3–7. DOI: 10.1145/3369255.3369266

Secretariat of the Security Committee. (2019) "Turvallisuusviranomaiset kehittävät osaamistaan kansallisessa kyberturvallisuusharjoituksessa", [Online]. Available at: https://turvallisuuskomitea.fi/tiedote-turvallisuusviranomaiset-kehittavat-osaamistaan-kansallisessa-kyberturvallisuusharjoituksessa-kyha19-jamkissa-jatkossa-myos-terveydenhuollon-toimijat-mukaan-harjoituksiin/

Ukwandu, E., Ben Farah, M.E., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., Tachtatzis C., Bures M., Andonovic, I., Bellekens, X. (2020) "A Review of Cyber-Ranges and Test-Beds: Current and Future Trends", arXiv preprint arXiv:2010.06850.

Valtori. (2020) "Valtori's 2019 financial statements published", [Online]. Available at: https://valtori.fi/en/-/valtorin-tilinpaatos-2019-julkaistu?languageId=en_US

Vykopal, J., Ošlejšek, R., Čeleda, P., Vizváry, M., Tovarňák, D. (2017) "KYPO Cyber Range: Design and Use Cases", Proceedings of the 12th International Conference on Software Technologies - Volume 1: ICSOFT, SciTePress, Madrid, Spain, pp. 310-321. DOI: 10.5220/0006428203100321.

Yamin, M.M., Katt, B. and Gkioulos, V. (2020) "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture", Computers & Security, Vol 88, pp. 101636. DOI: 10.1016/j.cose.2019.101636.

PVI

PEDAGOGICAL AND SELF-REFLECTING APPROACH TO IMPROVING THE LEARNING WITHIN A CYBER EXERCISE

by

Anni Karinsalo, Karo Saharinen, Jani Paijanen and Jarno Salonen 2022

21th European Conference on Cyber Warfare and Security, 16th - 17th June 2022, Chester, UK.

DOI: https://doi.org/10.34190/eccws.21.1.221

Pedagogical and self-reflecting approach to improving the learning within a cyber exercise

Anni Karinsalo,[1] Karo Saharinen,[2] Jani Päijänen,[2] Jarno Salonen,[3]
[1] VTT Technical Research Centre of Finland, Oulu, Finland
[2] JAMK University of Applied Sciences, Jyväskylä, Finland
[3] VTT Technical Research Centre of Finland, Tampere, Finland
anni.karinsalo@vtt.fi
jani.paijanen@jamk.fi
karo.saharinen@jamk.fi
jarno.salonen@vtt.fi

Abstract: In the digitalized world, there is a growing need not only to improve one's cybersecurity skills and knowledge, but also to find ways to optimize the learning process, for example by motivating the learners or optimising the learning facilities, material and the learners for the process. Cyber exercises ran within cyber ranges/arenas (CR) are an efficient way for the exercise participants to improve their cybersecurity skills and knowledge level. The pedagogical way of orienteering the participant to a learning situation is to have a preliminary survey, which prepares the participant for the upcoming event, adds self-reflection, and may even provide feedback and background information for the educator about the upcoming event. The objective of the survey is to improve the quality of the exercise by knowing the interest areas, preferences and other useful information about the participants that is then be used optimise the exercise accordingly.

This study analyses the structure of one preliminary survey targeted for the cyber exercise event to be held in January 2022. The questions are justified according to existing frameworks. We have collected a set of structured questions presenting different topics related to the participants' professional background and expectations towards the exercise. In addition to the short-term goal of analysing the survey for one cyber exercise, this work benefits the long-term goal for improving the skills of cybersecurity professionals. Our further work will validate the results of our preliminary analysis and analyse its correspondence with the survey results, and the final analysis constructed after the cyber exercise.

Keywords:
Cyber range, Cyber exercise, Cybersecurity skills, Cybersecurity, Survey

1. Introduction

In the current research, there is an acknowledged need to improve the level of cybersecurity knowledge on European level. This includes both means of personal skill development for the cybersecurity professionals (European Commission. Joint Communication to the European Parliament and the Council, 2020), but also larger-scale, administrative policies such as developing a common European framework for monitoring and developing the skills of cybersecurity professionals (ENISA, 2019) (Nurse et al., 2021).

We perceive the motivating factors for this study from three dimensions. First, we want to extend the pedagogical knowledge of the learning process. The pedagogical aspect of cybersecurity learning has been studied for example in (Karjalainen, 2021) and (Le Compte, 2015). However, to the best of our knowledge, the concept of using a preliminary survey before the cyber exercise has not been employed in a very broad manner. Second, as we will be facilitating a cyber exercise ourselves, we study the ways to improve the cyber exercise practical arrangement with the pre-study from the organiser's perspective. Third, the knowledge we gain regarding learning within the cybersecurity exercise can affect other similar exercises. Thus, we hope our experience will add to the lessons-learned of such events, especially on European level, and where possible, also on the education framework development for security professionals.

The aim of this article is to describe the structure and benefits of, and theory behind the survey that is sent to the participants before the cyber exercise in January 2022. In this article, we argue, that by using a pre-survey to collect information about the participants' professional skills and areas of interest, and fine-tuning the exercise according to the responses, we can impact the development of the participants' professional skills as

well as enhance the learning experience during the cyber exercise or other cyber event. The benefits of this study relate to resolving the following research questions:

- How can we better understand the needs and interests of cyber exercise participants (that can also be considered as ”customers” in some sense) by using a pre-survey?
- What kind of questions should the pre-survey consist of?
- What kind of existing frameworks can we use to create our pre-survey?

The survey questions proposed in this article are tailored to the targeted exercise, namely Flagship #2, but we will generalise them in future research as well as provide the results from our pre-survey. We consider that this study lays groundwork for the benefits of increased learning about motivation of the participants, acquiring the necessary information for the cyber exercise, and increased general knowledge for the organisation of cyber exercises.

The article is structured as follows. In section two we provide the background to our research, namely describing the European and worldwide guidelines, taxonomies and other frameworks that we have used to create our pre-survey. In section three we introduce the pre-survey and justify the questions that we have decided to use in it. Finally, in section four we discuss the general justifications and lessons-learned for the construction of the study, before concluding the article in the last section.

2. Theory and Framework Background

2.1 Regulation and Theory

The European Higher Education Area (EHEA) was adopted in May 2005 and it specified three cycles of qualification to which national frameworks were encourage to be made compatible with (European Higher Education Area, 2005). The cycles of qualification were updated by 2008 in a recommendation of the European parliament and of the council in establishment of the European Qualifications Framework (EQF) for lifelong learning. This update gave way for an eight level of qualifications; each of which were described by Knowledge and Skills to create Competence. Within the recommendation was also the requirement of mapping National Qualifications Frameworks (NQF) to the EQF from the Member States of the European Union (European Commission. Directorate-General for Education and Culture, 2008). Just before the 10th year anniversary of the EQF, the Council of the European Union refreshed their recommendation. These recommendations were divided into 18 different topics, e.g. to have member states ensure their consistency of national frameworks with the EQF periodically. (Council of the European Union, 2017) Within the European Union this background of guiding frameworks and recommendations give a good background in individual competence building and have established a common terminology within the EU (Brockmann, Clarke and Winch, 2009).

Bloom *et al.* (1956) introduced in their book a taxonomy to *“help (curriculum builders) to specify objectives so that it becomes easier to plan learning experiences and prepare evaluation devices”*. This taxonomy declared six major classes: Knowledge, Comprehension, Application, Analysis, Synthesis and Evaluation. Even though the learner could perform the major classes in different order than introduced in the book; it is still used as a tool of evaluation. Bloom’s taxonomy has been revised by Anderson *et al.* (2001) to have a more dynamic conception of the classifications made earlier. Thus, the revised categories / cognitive processes are as follows; Remember, Understand, Apply, Analyze, Evaluate and Create. Curriculum developers use the taxonomy extensively in different universities.

2.2 Cybersecurity Frameworks

Cybersecurity, as a paradigm of computing, has been a continuous topic of framework definition in multiple countries and international organisations. Several guiding frameworks have been introduced at the end of the last decade, with continuous work being done at the start of this decade. This chapter introduces the main cybersecurity frameworks related to this research paper.

Background of the *NICE Framework* came from the Comprehensive National Cybersecurity Initiative where one of the objectives was to expand cybersecurity education (Rollins and Henning, 2009). This Initiative was further emphasized into the formation of a National Initiative for Cybersecurity Education or NICE (The White House, 2010). The first available version of the NICE framework was published in 2017 (Newhouse et al., 2017). The framework described the cybersecurity work through tasks assigned to different work roles. These tasks

required *Knowledge*, *Skills* and *Abilities* (KSA's) and the work roles themselves were defined into specialty areas and categories.

Association for Computing Machinery publishes their Curricula Recommendations on their web pages (Association for Computing Machinery, 2022). The overview report from 2005 on Curricula guidelines (CC2005 Task Force, 2005) had no section on cybersecurity. This was later published as "*Cybersecurity Curricula 2017"* guideline book in 2018 (Joint Task Force on Cybersecurity Education, 2018) next to the Computing Curricula recommendations of 2005. Finally in 2020 the updated work of ACM published the Computing Curricula 2020 (CC2020 Task Force, 2020) which declared cybersecurity as its own field of education.

In the European Union, several research and development projects had the goal of producing a cybersecurity framework to be used within the European Union. ECSO has published a European Cybersecurity Education and Training - Minimum Reference Curriculum (ECSO 2021) aimed at providing *"the guidelines relative to the competence & skills development framework along with pedagogical methodologies for the higher education programme requirements".* SPARTA -project published its deliverable on cybersecurity skills framework (Piesarskas *et al.*, 2020) with stating *"This document serves as a basis for setting in motion a process of development of a comprehensive European cybersecurity skills framework"*. The framework analysed that European Cybersecurity Taxonomy (European Commission. Joint Research Centre, 2019) to be coupled with the NICE Framework would be a good starting point for a more comprehensive framework for the EU. CyberSec4Europe -project published its own Design of Education and Professional Framework (Karinsalo and Halunen, 2021) which combined a small part of the NICE framework with the ACM Cybersecurity Curricula 2017 Knowledge Areas. Other notable framework is The Cyber Security Body of Knowledge (Rashid *et al.*, 2021) in the United Kingdom, however it is not used in this research paper.

2.2.1 Flagship #1 cyber exercise

Flagship #1 was an online-only cyber exercise, organised in January 2021. The exercise platform used was a cyber-arena, a large-scale cyber range, as a technical platform. Participants used the prepared environment to perform their tasks. Flagship #1 was a reactive cyber exercise, showcasing real-world skills needed in every organisation that uses ICT-services. The task was to detect and investigate a successful cyber-attack that the exercise organisation had previously faced. Once the attack was detected and deemed successful, the participants started following the prepared (cyber) incident management documents and procedures, alerting organisations' staff and stakeholders, and various authorities. Flagship #1 showcased that the organisation benefits from using the existing documentation and procedures in a cyber exercise. When a cyber incident happens, there is some knowledge on the expected behaviour to mitigate and respond to the incident.

During registration to the exercise, the participants completed a short self-assessment questionnaire on their skills and knowledge in cybersecurity and previous experience related to cyber-exercises. This self-assessment was the basis for the preliminary survey covered in this paper. After the exercise, a comprehensive self-assessment questionnaire in skills improvement was filled-out. The post-exercise questionnaire was based on NICE framework KSA's. (CyberSec4Europe, 2021)

2.2.2 Flagship #2 cyber exercise

The forthcoming two-day Flagship #2 exercise showcases a simulated successful cyber-attack targeting a critical infrastructure operator, a train operator using a (simulated) next-generation Rail Traffic Management System. In the scenario, trains have smart devices installed that include Trusted Platform Modules (TPMs). The (simulated) technology is dependent on various ICT-infrastructure services and functionalities located in the train and alongside the railway. Attacking against such technology stack requires besides malicious objectives, also technological skills to avoid or bypass the security controls in a train or infrastructure.

The objective of Flagship #2 is to showcase that analyzing and investigating a sophisticated attack against complex technology requires broad and deep understanding of the technology, and that a (simulated) company, whilst having competent cybersecurity employees may still lack the skills needed. Given the scenario is successful from this point of view, the exercise participants receive support from a (simulated) cybersecurity analyst company that they have hired. The analyst company has a vast amount of workforce that focuses on analysing and investigating complex cyber-attacks. Due to the aforementioned needs, we aim to impact the

development of the participants' professional skills as well as enhance the learning experience during the cyber exercise or other cyber event with our pre-survey.

2.3 Target groups

Flagship #2 exercise is targeted to the following target groups:

- Project group members
- Other personnel from project member organisations
- External stakeholders of the project (external cybersecurity analyst role)

In general, the exercise is targeted to any members of the aforementioned groups with interest towards attending the cyber exercise. In other words, one does not need to be a cybersecurity professional to participate even though professionals might benefit from the exercise more than non-professionals. The main difference to the previous Flagship #1 exercise is the inclusion of external cybersecurity analysts who participate in a separate capture-the-flag (CTF) exercise during Flagship #2 and analyse a simulated cyber-attack using real tools and applicable methodology in a dedicated environment. The cybersecurity analyst role has a prerequisite of having previous experience in using Linux command line tools and naturally the exercise benefits cybersecurity professionals more than non-professionals.

3. Survey Design

In this section, we analyse each of the survey questions and their theoretical background in order to justify their use. By "survey", we mean the preliminary survey (or pre-survey) which is targeted to the forthcoming Flagship #2 exercise participants.

3.1 Survey design and process

The survey in question is an online survey sent to the registered participants of the forthcoming cyber exercise and it collects information about their competence levels and preferences prior to the exercise. The survey consists of eleven questions with eight single-choice, two multiple-choice and one open question. All but the last question (#11) are mandatory in order to get responses to all survey questions. However, we have included a specific "I prefer not to disclose this information" response to questions #1-#5 that collect information concerning the educational background, knowledge/skill levels, participant job roles and the organisation sector in case the respondent is concerned about the responses. All the other questions are collecting information about areas of interest, preferred exercise roles and opinions about suitable exercise group sizes and session times and therefore they do not have the aforementioned response option. Since these extra response options do not provide additional value to this article, they are not included in the figures nor covered in the next sub-sections.

In addition to the survey questions covered in the following sub-sections, the survey also consists of an introductory/invitation text and a field to ask/verify the respondent email address. The email is used for connecting the right pre-survey with the post-survey that will be sent to the exercise participants after the event and used to match the expectations to the learning experience. Since these aforementioned survey parts do not have additional value to this article, we just mention them here.

3.2 Survey questions

The first survey question is shown in the figure below. The question is a single-choice one with four response options categorised according to the European Qualifications Framework (Council of the European Union, 2017). It also includes an "Other, please specify" option in case the respondent doesn't belong to any of the following groups or even has multiple degrees from different areas and would like to clarify.

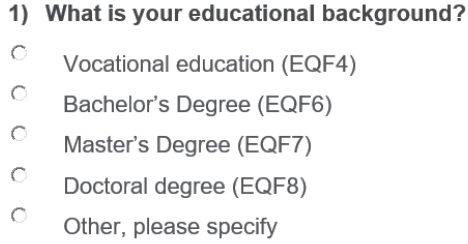


Figure 1. Survey question #1

The first survey question helps the exercise organisation to be more aware of the educational background and competence levels of the participants. With this gained awareness, the cybersecurity exercise could be adjusted or participant roles designed with more precision to match the capabilities of the participants.

The second survey question is shown below. The question is a single-choice one with 12 response options categorised according to the sectors specified in the European Cybersecurity Taxonomy (European Commission. Joint Research Centre, 2019). It also includes an "Other, please specify" option e.g. in case the respondent organisation doesn't belong or doesn't recognize him/herself to be in any of the groups.

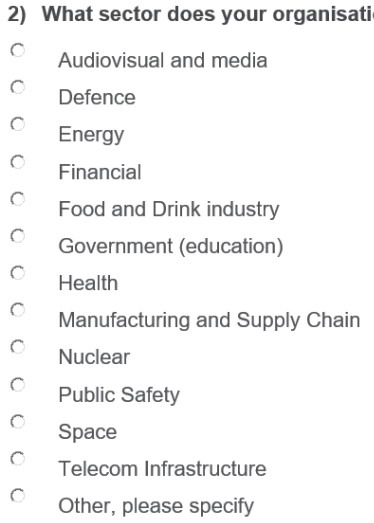


Figure 2. Survey question #2

Given the multipurpose cybersecurity exercises in development to day (Fischer-Hübner *et al.*, 2020) it would be of interest of the exercise conducting organization to get more familiar with the participants organization background. This gives way to customize the exercise towards a certain security of supply area.

The third survey question is shown below. The question is a single-choice one with three response options categorised according to Bloom's taxonomy (Bloom *et al.* (1956)). This gives a self-estimation of the participants' competence level in this particular area of expertise; of cybersecurity exercises in general.

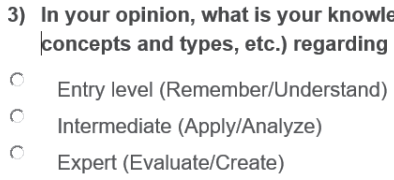


Figure 3. Survey question #3

The objective of this question is to categorise participants according to their knowledge level and then, based on the exercise type and objectives, organise exercise groups accordingly. Generally, the groups are formed evenly, i.e. each group has members from each skill level, which makes it possible for the expert level members to assist the entry and intermediate level members during the exercise. However, in some exercise types it is also possible to assign members of the same level into one group, which among others helps the facilitation of the group. In practice this could mean e.g. that the entry level groups receive more comprehensive explanation than others do.

The fourth survey question is shown. The question is a single-choice one with three response options categorised according to Bloom's taxonomy (Bloom *et al.,* 1956). As cybersecurity exercises usually are quite technical events, the participants are asked to self-evaluate their competence levels in technical skills.

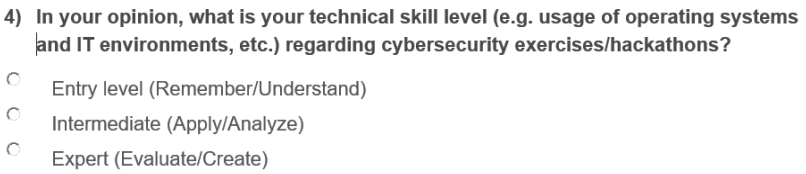


Figure 4. Survey question #4

This question is very similar to the previous one, but focuses on the technical skill level of the exercise participants instead of the overall knowhow of the exercise types and processes. The objective of this question is to categorise participants according to their technical skill level and then, based on the exercise type and objectives, organise the exercise groups accordingly. For example, if the exercise supports multiple simultaneous tasks at different levels, then groups could be formed according to the participants' knowledge level and they would complete different tasks or "missions" during the exercise. In case the exercise consists of tasks or "missions" that every group must complete in the same order, then the groups would most likely be formed in such a way that each group has members from each knowledge level.

In general, the advantage of having members of different technical skill level in one group may support the learning of those in the lower, i.e. entry and intermediate skill levels. However, there is a rather high probability that the members at expert level perform most of the exercise tasks, which may hinder the learning of the less advanced members. In most cases, it is the role of the group facilitator to monitor the progress and ensure that all members of the group understand the things done during the exercise despite their technical or other skill level.

The fifth survey question is shown below. The question is a single-choice one with seven response options categorised according to the sectors specified in the NIST - National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Newhouse *et al.*, 2017). It also includes an "Other, please specify" option e.g. in case the respondent job role doesn't belong to any of the aforementioned groups.

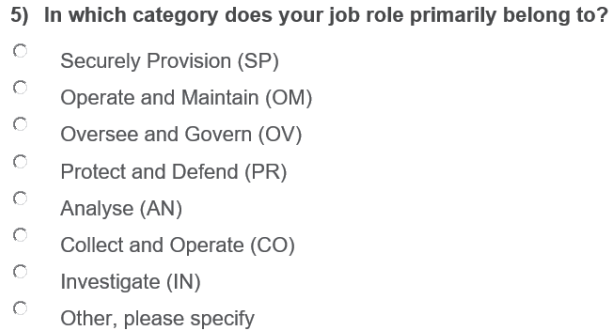


Figure 5. Survey question #5

The sixth survey question is shown below. The question is a multiple choice one with nine options that have been applied from the CyberSec4Europe deliverable "Design of Education and Professional Framework" (Karinsalo and Halunen, 2021). The respondents are instructed to choose from one to three options from the list.

6) **Flagship 2 has defined goals. However, if you could choose, which knowledge area development/improvement are you most interested in? Choose 1-3 options.**

- ☐ Data Security
- ☐ Software Security
- ☐ Component Security
- ☐ Connection Security
- ☐ System Security
- ☐ Human Security
- ☐ Organisational Security
- ☐ Societal Security
- ☐ Operate and maintain

Figure 6. Survey question #6

This question is very important one since it enables fine-grained exercise customisation according to the participants' areas of interest. In case the survey is conducted before or during the planning of the cyber exercise, it may enable quite radical customisation. However, as the question text in the previous figure specifies, the exercise may already have defined goals in which case the customisation could apply e.g. to spending more time in a desired type of session or include additional pieces of information to them in order to enhance the learning process. In case the exercise consists of different simultaneous tasks, then customisation could be done by grouping the members according to their desired interest areas and choosing suitable tasks for them.

The seventh survey question is shown below. The question is a single-choice one with seven response options categorised according to the sectors specified in the NIST - National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Newhouse et al., 2017). It also includes an "Other, please specify" option e.g. in case the respondent job role doesn't belong to any of the aforementioned groups.

7) **Which role do you want to primarily progress in the selected knowledge areas?**

- ○ Securely Provision (SP)
- ○ Operate and Maintain (OM)
- ○ Oversee and Govern (OV)
- ○ Protect and Defend (PR)
- ○ Analyse (AN)
- ○ Collect and Operate (CO)
- ○ Investigate (IN)
- ○ Other, please specify

Figure 7. Survey question #7

The objective of this question is to assign suitable roles for each cyber exercise participant and where possible, target some tasks in order to support specifically the learning of specific roles. As an example, the Flagship #2 exercise consists of a parallel capture-the-flag (CTF) type of cybersecurity analyst exercise that is directed specifically to people interested in that role.

The eighth survey question is shown below. The question is a single-choice one with four response options with the objective of collecting the respondent's opinion about their preference regarding the ideal number of participants for the exercise teams.

8) **In your opinion, what is the ideal number of participants for the exercise teams?**

- ○ 1-2
- ○ 3-4
- ○ 5-6
- ○ more than 6

Figure 8. Survey question #8

The objective of this question is to assign the participants in groups that are pleasing in terms of the number of members and therefore enhance participation, learning and elements like peer teaching. According to the research by e.g. Koolos et al. (2011), the group-size effect is observed in favour or working in smaller groups (subgroups), i.e. students prefer smaller assignments and smaller groups that enable peer teaching.

The ninth survey question is shown below. The question is a single-choice one with six response options ranging from zero to more than 90 minutes.

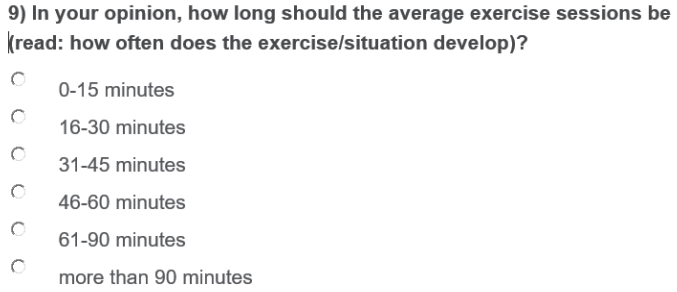


Figure 9. Survey question #9

The question relates to the intensity of learning events in the cybersecurity exercise. The effective training length is a topic researched in education e.g. by Ericsson (2006) and Bunce et al. (2010). Since Flagship #2 lasts for two days, the individual sessions are bound to be quite lengthy. However, we are searching for possibilities to adjust the exercise intensity at least to some extent based on the responses to this question.

The tenth survey question is shown below. The question is a multiple choice one with nine options that have been applied from the Cybersecurity Curricula 2017 (Newhouse *et al.*, 2017). The respondent is instructed to choose from one to three options from the list.

Figure 10. Survey question #10

Similarly to question six, this question enables customising the exercise contents in detail according to the responses. However since Flagship #2 exercise has already defined goals, customisation applies mainly e.g. to spending less time in the less desired knowledge areas or the related information can be provided as an extra.

The eleventh survey question is shown below. The question is an open one with the instructions to the respondent for giving any thoughts about the exercise or comments/greetings to the organisers.

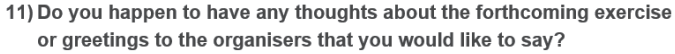


Figure 11. Survey question #11

The objective of this question is to allow participants express feelings and raise concerns about the forthcoming exercise, if any. The question is partially linked to the research by, e.g. Arbaugh and Benbunan-Fich (2007) that highlight the importance of participant interaction in online learning environments such as Flagship #2. In other words, the question also intends to motivate them by increasing their engagement to the exercise.

4. Discussion

In this study, we analysed how to use a pre-survey for understanding the needs and interests of the cyber exercise participants. We also analysed how to format the questions, and what frameworks to use when creating the survey. In this context, we constructed eleven questions using existing cybersecurity frameworks. We also provided related justifications based on the Flagship2 event requirements.

Regarding the general structuring of the survey, we concluded that since the audience consists of professionals and the event is voluntary for them (i.e. not a part of a student curriculum), the survey should not be too demanding or time-consuming. If the survey has too complex or too many questions, there is a risk that the respondents do not bother to answer. Thus, we optimized the questions to attain as much information as possible while trying to keep the number of the questions as low as possible. Regarding the question setting, we wanted to use the questions to improve the commitment of participants by increasing their motivation. Fishbach et al (2022) describe intrinsic (i.e. internally driven or rewarding) motivation to be "critical predictor of engagement". According to them, one approach for increasing intrinsic motivation is to factor "the positive experience while pursuing the activity, with choice." Questions formulated such as question 6, enabling participants feel they can affect or make choices of interest regarding the course content, potentially increase the intrinsic motivation of the participant towards the exercise. Further work will include analysing the pre-survey answers and reflecting them in the summary of the cyber exercise outcomes, lessons-learned and post-survey results.

5. Conclusions

This article presents the construction process and structure of a pre-survey targeted to the participants of a cyber exercise. We have constructed a survey consisting of eleven questions that are based on existing frameworks such as EQF, NICE, European and Cybersecurity Curricula. Based on our current analysis, the questions help us better understand the needs and interests of the Flagship #2 cyber exercise participants. The article also provides related justifications that are linked to the upcoming cyber exercise details.

References

Anderson, L. et al. (2001) A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives.

Arbaugh, J.B., Benbunan-Fich, R. (2007). The importance of participant interaction in online environments. Journal of Decision Support Systems, 43 (3), pp. 853-865. https://doi.org/10.1016/j.dss.2006.12.013.

Association for Computing Machinery (2022) Curricula Recommendations. Available at: https://www.acm.org/education/curricula-recommendations (Accessed: 10 January 2022).

Bloom, B.S. et al. (1956) Taxonomy of Educational Objectives - The Classification of Educational Goals. London: Longmans, Green and Co Ltd.

Brockmann, M., Clarke, L. and Winch, C. (2009) 'Competence and competency in the EQF and in European VET systems', Journal of European Industrial Training, 33, pp. 787–799. doi:10.1108/03090590910993634.

Bunce, D., Flens, E. and Neiles, K. (2010) How Long Can Students Pay Attention in Class? A Study of Student Attention Decline Using Clickers. Journal of Chemical Education 2010 87 (12), 1438-1443. doi: 10.1021/ed100409p.

CC2005 Task Force (2005) Computing Curricula 2005: The Overview Report. New York, NY, USA: Association for Computing Machinery. Available at: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2005-march06final.pdf (Accessed: 10 January 2022).

Council of the European Union (2017) Council Recommendation on European Qualifications Framework for lifelong learning. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017H0615(01)&from=EN (Accessed: 5 January 2022).

CyberSec4Europe. (2021) "CyberSec4Europe Hosting Flagship 1: An Online Cybersecurity Exercise", [online], Cyber Security for Europe (CyberSec4Europe), https://cybersec4europe.eu/cybersec4europe-hosting-flagship-1-an-online-cybersecurity-exercise/ (Accessed: 15 January 2022).

ECSO (2021) European Cybersecurity Education and Professional Training: Minimum Reference Curriculum SWG 5.2 I Education & Professional Training. https://ecs-org.eu/documents/publications/61967913d3f81.pdf (Accessed: 5 January 2022).

ENISA (2019) Cybersecurity skills development in the EU. https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union (Accessed: 15 January 2022).

European Commission. Joint Communication to the European Parliament and the Council (2020) The EU's Cybersecurity Strategy for the Digital Decade

European Commission. Joint Research Centre (2019) A proposal for a European cybersecurity taxonomy. LU: Publications Office. Available at: https://data.europa.eu/doi/10.2760/106002 (Accessed: 5 January 2022).

European Higher Education Area (2005) The Framework of Qualifications for the European Higher Education Area. Available at: http://www.ehea.info/media.ehea.info/file/WG_Frameworks_qualification/85/2/Framework_qualificationsforEHEA-May2005_587852.pdf (Accessed: 5 January 2022).

Ericsson, K.A. (2006) 'The Influence of Experience and Deliberate Practice on the Development of Superior Expert Performance', the Cambridge handbook of expertise and expert performance, p. 22.

Fischer-Hübner, S. et al. (2020) 'Quality Criteria for Cyber Security MOOCs', in Drevin, L., Von Solms, S., and Theocharidou, M. (eds) Information Security Education. Information Security in Action. Cham: Springer International Publishing (IFIP Advances in Information and Communication Technology), pp. 46–60. doi:10.1007/978-3-030-59291-2_4.

Fishbach, A. and Woolley, K. (2022). The Structure of Intrinsic Motivation. To be published in: Annual Review of Organizational Psychology and Organizational Behavior, Volume 9, number 1, doi:10.1146/annurev-orgpsych-012420-091122 (Accessed 17. January 2022)

Joint Task Force on Cybersecurity Education (2018) Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. New York, NY, USA: Association for Computing Machinery.

Newhouse, W. et al. (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. NIST SP 800-181. Gaithersburg, MD: National Institute of Standards and Technology, p. NIST SP 800-181. doi:10.6028/NIST.SP.800-181.

Karinsalo, A. and Halunen, K. (2021) 'Design of Education and Professional Framework'. CyberSec4Europe. Available at: https://cybersec4europe.eu/wp-content/uploads/2021/06/D6_3_Design-of-Education-and-Professional-Frame-work_Final.pdf. (Accessed: 14 January 2022).

Karjalainen, M. (2021). Pedagogical Basis of Live Cybersecurity Exercises. https://jyx.jyu.fi/handle/123456789/76371 (Accessed: 12 January 2022).

Kooloos, J.G.M. *et al.* (2011) 'Collaborative group work: Effects of group size and assignment structure on learning gain, student satisfaction and perceived participation', *Medical Teacher*, 33(12), pp. 983–988. doi:10.3109/0142159X.2011.588733.

Le Compte, A., Elizondo, D. and Watson, T. "A renewed approach to serious games for cyber security," 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, 2015, pp. 203-216, doi: 10.1109/CYCON.2015.7158478.

Nurse, J. R. C. and Adamos, K. and Grammatopoulos, A. and Di Franco, F. (2021) Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education. European Union Agency for Cybersecurity (ENISA). Available at: https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education/@@download/fullReport (Accessed: 5 January 2022).

Piesarskas, E. et al. (2020) 'Cybersecurity skills framework'. Available at: https://sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf (Accessed: 10 January 2022).

Rashid, A. et al. (2021) 'The Cyber Security Body of Knowledge'. Available at: https://www.cybok.org/ (Accessed: 15 January 2022).

Rollins, J. and Henning, A.C. (2009) Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations, UNT Digital Library. Library of Congress. Congressional Research Service. Available at: https://digital.library.unt.edu/ark:/67531/metadc743582/ (Accessed: 10 January 2022).

The White House (2010) Advancing Our Interests: Actions in Support of the President's National Security Strategy, whitehouse.gov. Available at: https://obamawhitehouse.archives.gov/the-press-office/advancing-our-interests-actions-support-presidents-national-security-strategy (Accessed: 10 January 2022).

PVII

RESEARCHING GRADUATED CYBER SECURITY STUDENTS – REFLECTING EMPLOYMENT AND JOB RESPONSIBILITIES THROUGH NICE FRAMEWORK

by

Karo Saharinen, Jarmo Viinikanoja and Jouni Huotari 2022

21th European Conference on Cyber Warfare and Security, 16th - 17th June 2022, Chester, UK.

DOI: https://doi.org/10.34190/eccws.21.1.201

Researching Graduated Cyber Security Students – Reflecting Employment and Job Responsibilities through NICE framework

Karo Saharinen, Jarmo Viinikanoja, Jouni Huotari
JAMK University of Applied Sciences, Jyväskylä, Finland
karo.saharinen@jamk.fi
jarmo.viinikanoja@jamk.fi
jouni.huotari@jamk.fi

Abstract: Most research and development on Cyber Security education is currently focusing on what should be taught, how much, and where within the degree programmes. Different Cyber Security frameworks are currently evolving to include Cyber Security education parallel to older paradigms of Computing Education, existing alongside with such as "*Information Technology*" and "*Software Engineering*". Different Cyber Security specialisations or even whole degree programmes have started within universities before the frameworks have been defined into standardised degree structures. This is mainly the result of a dire industry need of well-educated cyber security personnel, a phenomenon affecting the industry globally.

Our research concentrates on Finnish alumni students who have already graduated from a bachelor's degree programme in Information Technology with a specialisation in Cyber Security in Finland. Within our gathered research data, we analysed what is the industry sector where their current job resides, and what are the cyber security responsibilities in their current work. The questionnaire also contained an after-reflection section where the graduated students could choose what they would study were they about to start and plan their studies again.

The results verify that Cyber Security is still the most favoured specialisation within the former Cyber Security alumni students. Slight variation is evident from the data, which in the authors' perspective, verifies the multifaceted nature of Cyber Security. When analysing alumni students' job responsibilities, the main category of work resides in the "*Protect and Defend*" category of the NICE Framework, which in the terms of the conference, relates to Critical Infrastructure Protection being the main subject of employment for fresh graduates.

These results give insight to other education organisations on how to develop their curricula to further emphasise the employment of students or to offer modules which are of interest for newly employed Cyber Security professionals. In addition, it gives an insight of industry demand for freshly graduated students within the target group.

Keywords: Cyber Security, Degree Programme, Cybersecurity skills

1. Introduction

Cyber Security capability building is a world-wide phenomenon where different nations are either gathering or developing tools, training people (Catota et al, 2019) and perfecting their processes to an extent that some might even call a cyber arms race (Limnéll, 2016). This paper concentrates on researching the training of cyber security professionals through the education systems of a country. An undertaking which is simultaneously answering to an evident workforce need of a functioning industry (Jaurimaa et al, 2020) and the national cyber resilience levels of a country (Whyte, 2020). Both of which are targeted by threats coming from the cyber domain affecting e.g. the critical infrastructure of a country or the information security of a nation.

To answer this need of cyber security professionals, degree programmes fully dedicated to Cyber Security are being established in the Higher Education institutions of different countries. European Union Agency for Cybersecurity (ENISA) established Cybersecurity Higher Education Database (CyberHEAD) to map these degree programmes (Zan De & Di Franco, 2019). Criteria for degree programme approval were:

- 25 percent of *cyber security topics* for bachelor's degrees
- 40 percent of *cyber security topics* for master's degrees
- and research on *cyber security topics* for PhD students

At the time of writing this paper, there are 139 programmes in 25 countries that are approved in CyberHEAD (ENISA, 2021). Within these 139 programmes the word cyber security appeared in the title of 13 out of 23 bachelor's degrees, 56 out of 105 master's degrees and in none of the three PhD programmes (and 0 out of 8 specialiation postgraduate courses). This emphasises that almost half of the degrees are titled and focused on other areas of Computing. However, they contain the percentage required in *cyber security topics* to be a part of CyberHEAD.

2. Literature review

As described by the introduction chapter, the *cyber security topics* in use at CyberHEAD were defined by ENISA (Zan De & Di Franco, 2019) to be aligned with Joint Task Force on Cybersecurity Education called CSEC2017 (Associate for Computing Machinery, 2017), which is published by the Association for Computing Machinery (ACM) in their collection of curricula recommendations (Associate for Computing Machinery, n.d.). These recommendations were published to emphasise Cyber Security as a paradigm of Global Computing Education. An aspect which was lacking in the ACM Curricula Recommendations of 2005 (Shackelford et al, 2005). ACM recently published their Curricula Recommendations 2020 (CC2020 Task Force, 2020), which stabilised the presence of Cybersecurity as a full paradigm of computing next to older topics such as *"Information Technology*" and *"Software Engineering"* to name a few.

Alongside these developments the National Institute of Science and Technology (NIST) released National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework in 2017 (Newhouse et al, 2017), which described the knowledge, skills and tasks in different categories and workroles within Cyber Security. The framework aspired to partner academia, private and public sector to provide comprehensive material to improve workforce development in education and training within the United States of America. In the UK, as put forth by the UK Cyber Security Strategy (United Kingdom, 2016), The Cyber Security Body of Knowledge was released in 2019 by version 1.0 (Rashid et al, 2019) and 2021 with version 1.1.0 (Rashid et al, 2021) respectively. It is a simplification if stated that both are quite similar in their agendas and goals.

Similar projects were conducted in the European Union in two different research and development projects; SPARTA and Cyber Security for Europe (CS4E). SPARTA released their "*Cybersecurity skills framework"* in 2020 (Piesarskas et al, 2020), but based a part of their work on the NICE framework. A very similar undertaking was developed under the Cyber Security for Europe (CS4E) project in Work Package 6 with a topic of Cybersecurity Skills & Capability Building. The work package released a Deliverable on "*Design of Education and Professional Framework*" in 2021 (Karinsalo et al, 2021).

Many skills framework documents were motivated by the worldwide need of Cybersecurity Workforce. This topic was declared as follows: *"The cybersecurity skills shortage and gap are well-documented issues that are currently having an impact on national labour markets worldwide*", a direct quote from a publication of ENISA released on 24th of November 2021 titled "Addresing Skills Shortage and Gap Through Higher Education" (Nurse et al, 2021), released just prior to writing this research paper. This shortage was referenced by seven different sources, divided regionally here to be from European Union, UK, North America, Central and South America, Asia and Australia. This emphasises the fact that there is a world wide need of Cyber Security Professionals. Even the newly published cyber security strategy of the European Union (European Comission, 2020) states this lack of professionals, but with fewer references. These parallelly generated frameworks, curriculum guides, and different publications prove an evident background and need of establishing cyber security focused education.

Finland published its first Cyber Security Strategy on 24 January 2013 as a government resolution (The Security Committee of Finland, 2013). The strategy declared different goals and operation models to meet the challenges of the cyber domain and ensure the fuctionality of the cyber domain. The first version of the strategy contained a sentence declaring *"The study of basic cyber security skills must be included at all levels of education"*. This was further enforced in the updated strategy (The Security Committee of Finland, 2019) that all cyber and information and communications technology (ICT) related training/degree programmes will be strengthened.

The first Finnish strategy can be seen as a clear point in time when Higher Education institutions in Finland began to start degree programmes purely dedicated to cyber security. JAMK University of Applied Sciences (JAMK) and University of Jyväskylä (JYU) both launched a master's degree programme on purely cyber security in 2013 (JAMK University of Applied Sciences, 2013) (University of Jyväskylä, 2013). JAMK also started a bachelor's degree with a cyber security specialisation in 2015 (JAMK University of Applied Sciences, 2015). Afterwards many other Universities of Applied Sciences and Universities in Finland followed with their own offering of Cyber Security, be it degree-oriented curricula (South-Eastern Finland University of Applied Sciences, 2021) or just specialisation studies for life-long learning with no official degree completion (Metropolia University of Applied Sciences, 2021). This timeline of frameworks and degree oriented higher education is further visualised in the Figure 1.

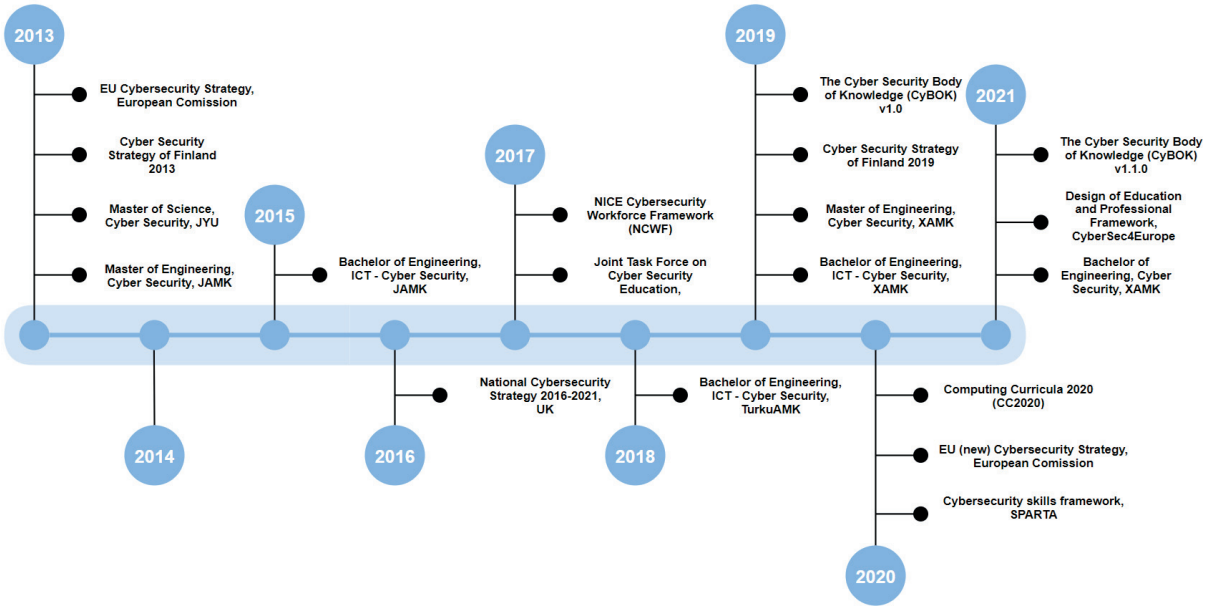


Figure 1: Timeline of cyber security frameworks, Finnish cyber security strategies and degree programmes

3. Survey Research on Graduated Students

This research was scoped to concern graduated bachelor's degree students of JAMK University of Applied Sciences with a cyber security specialisation in their degree. The degree programme was started in 2015 and has a recommended length of 4 years (240 ECTS). Thus, the first students to graduate according to the recommended timetable should have been around 2019. Noteworthy is that these students were the first graduates within Finland to have a cyber security focus in their bachelor's degree.

The research was designed to directly involve the university in contacting the students, however it proved to be a troublesome task. Cyber Security students, by the nature of their studies presumably, had marked that their contact information should not be used for research purposes, nor should they be contacted later by the university. Thus, the research permission process of the university granted no results for student contact information.

This result of the permission process forced the researchers of this paper to contact the students through different social media platforms; asking the students publicly to inform of their willingness for the research by contacting the researchers personally. Luckily few active students could be found which then forwarded the request to attend the research to more specific and limited messaging groups of the students. To increase the reliability of the research, one aspect was that the questionnaire was handed only to graduated students who had directly contacted the researchers and been identified as former students. This resulted in 19 respondents out of 68 graduated, thus sample size from the total possible participants was 27.94%.

The research method used was a survey containing mostly quantitative measurements of the participants. Research ethics were used design the questionnaire in a way that would give the researchers the necessary

information, and then the replies were generalised (e.g., specific company to be “private/public company”) so that no singular student could be identifiable from the data.

As the literature review stated, there are multiple frameworks possible of data categorisation/analyzation. In this research the NICE Framework was chosen to categorise and analyse the work roles of researched participants. The Framework has descriptive terminology on each work responsibility assigned to each work role. Because of this, the NICE framework was something that the students were requested to examine, if they had doubt in selecting what work role described their profession the best.

4. Survey Results and Analysis

This chapter divides into two different sections; place of employment answers the research question “Where are graduated students employed?” and type of work answering, “What kind of work responsibilities do the students have?”.

4.1 Place of Employment

First question concerned the student’s starting year and graduation year to get a glimpse of the length of their studies. This is visualised in the Figure 2 in which the darker color shows the total count of started degree studies of each year and the lighter color represents the total count of graduations of each year within our sample group.

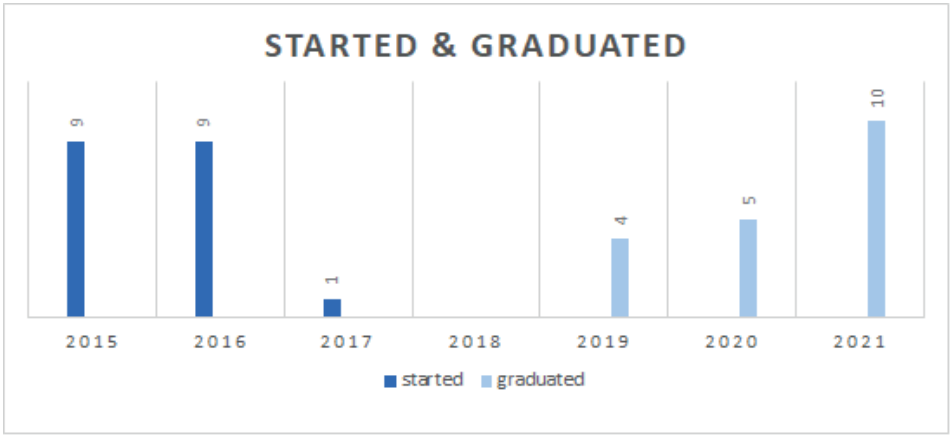


Figure 2: Starting year compared to graduation year

It is evident that even though almost half of the respondents started their studies in 2015, still many graduated behind schedule in 2020 and 2021. The authors interpret this could be the result of e.g. fast employment during studies as ICT degrees do not need to be finished to start working in the industry which results to delaying the graduation of a student. Although other reasons might be as plausible as proved by other research (Willoughby et al, 2021). Unfortunately, within our research this reason of delay was not a separate question.

One of the main research objectives was to find out where the bachelor’s degree students get employed, which industry sector and company size. These are apparent in the data gathered and visualised in the Figure 3.

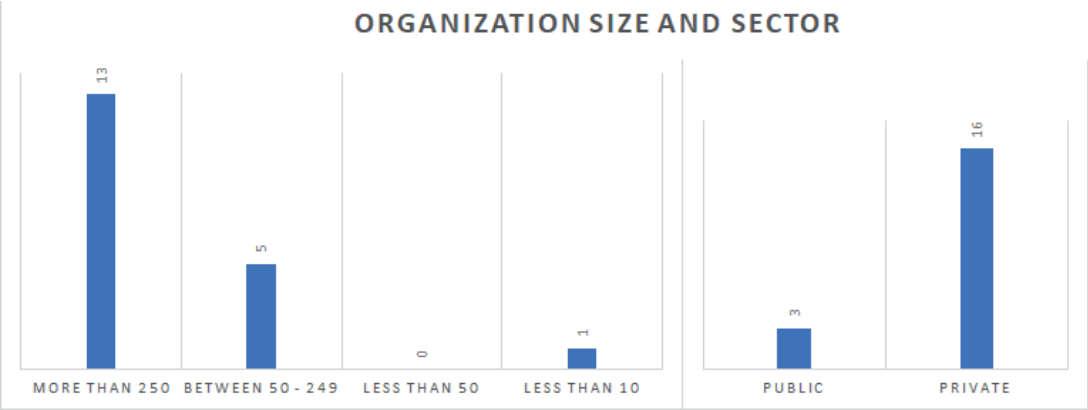


Figure 3: Organisation size and sector

Within these results, neither the employment sector nor company size surprised the authors. In Finland, the growing cyber security sector seems to follow the same footsteps as the global phenomenon. The European Cyber Security Strategy (European Comission, 2020) states that *"Over two-thirds of companies, in particular Small to Medium Enterprises (SMEs) are considered 'novices' in cyber security…"*. This stated need for protection can be witnessed from the service offering of private cyber security companies in Finland. These provided services need workforce behind them and thus, graduated bachelor's degree students get employed.

Given the employment, these companies can be dissected further based on their industry sector. A proposal for a European Cybersecurity Taxonomy (Nai Fovino et al, 2019) declared industry sectors which were utilised in the data categorisation of this research. Students' employment information was translated into these sectors as represented by figure 4.

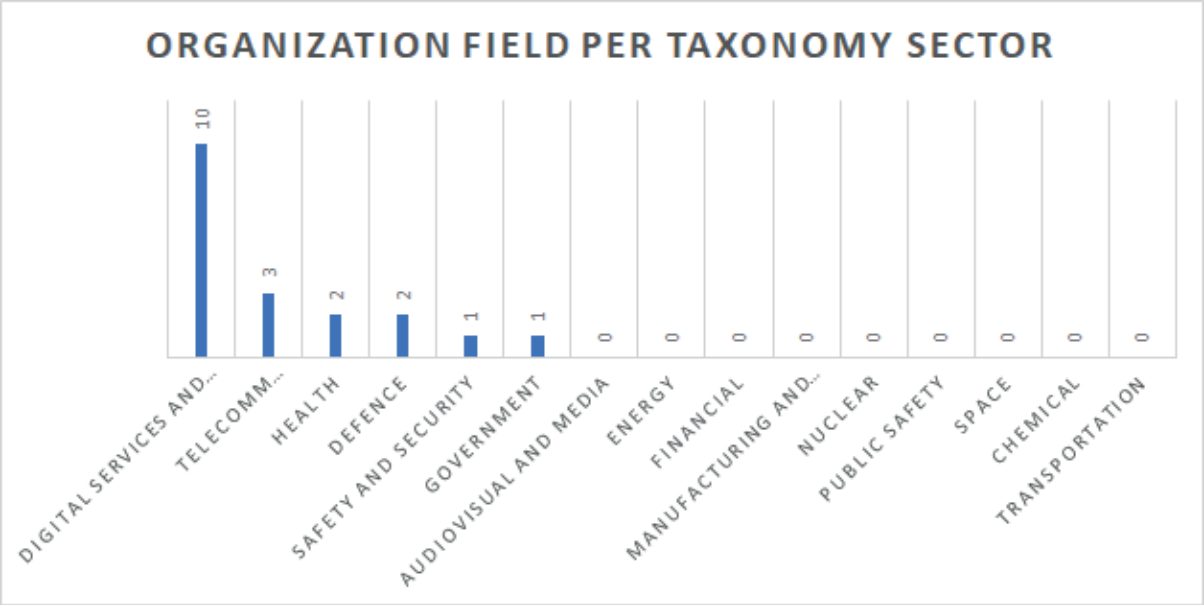


Figure 4: Employment sector of students based on A proposal for a European Cybersecurity Taxonomy

Out of these sectors, the business to business (B2B) companies were most apparent. Most of them categorising under the "*Digital services and platforms"* sector of the taxonomy. "*Telecomm infrastructure*" had significant Internet Service Providers (ISPs) of Finland recruiting some students, but for reliability sake it is worth metioning that some of the "*digital services and platforms*" were subsidiary organisations of the previously mentioned ISPs. Thus, based on analysis interpretation of the organisations, these two were the largest employers. "*Health"* and "*Defence"* sectors have employed two students both with "*Defence"* being the majority of public organisation employers. *"Government"* and *"Safety and Security"* sectors followed, but there are no results of other sectors within this survey scope.

4.2 Type of Work

As for the following results, we asked the students to place emphasis on the question of "what work role of the NICE framework describe their work the most?". As the quantitative grading scheme, we asked them to place the work roles in 1st to 5th order where the 1st being the most descriptive work role for their current work and 2nd being the second most descriptive work role etc. Figure 5 shows a graph of the whole data.

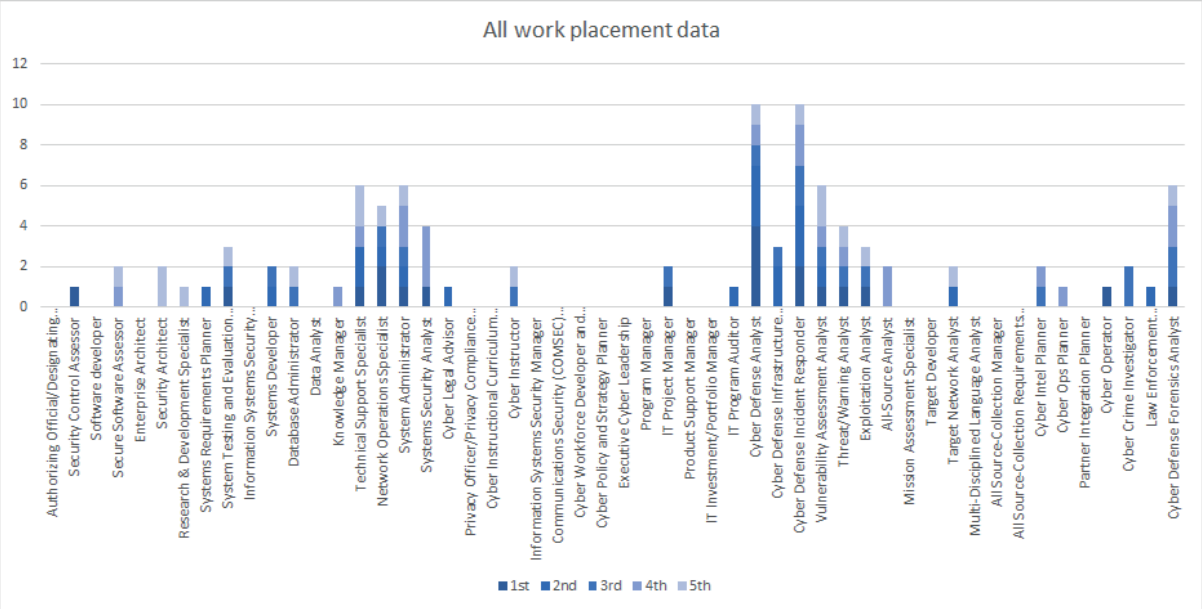


Figure 5: Top NICE categories based on what best fit their work

As there are 52 work roles described by the NICE Framework, Figure 5 is quite extensive or even hard to differentiate, but clear emphasises can already be observed from the visualization. To illustrate the work responsibilities more informatively, we used the frameworks categories to further delve into the data and order it from the most hit category (up top) and the least hit category (on bottom) as visualised in the Figure 6.

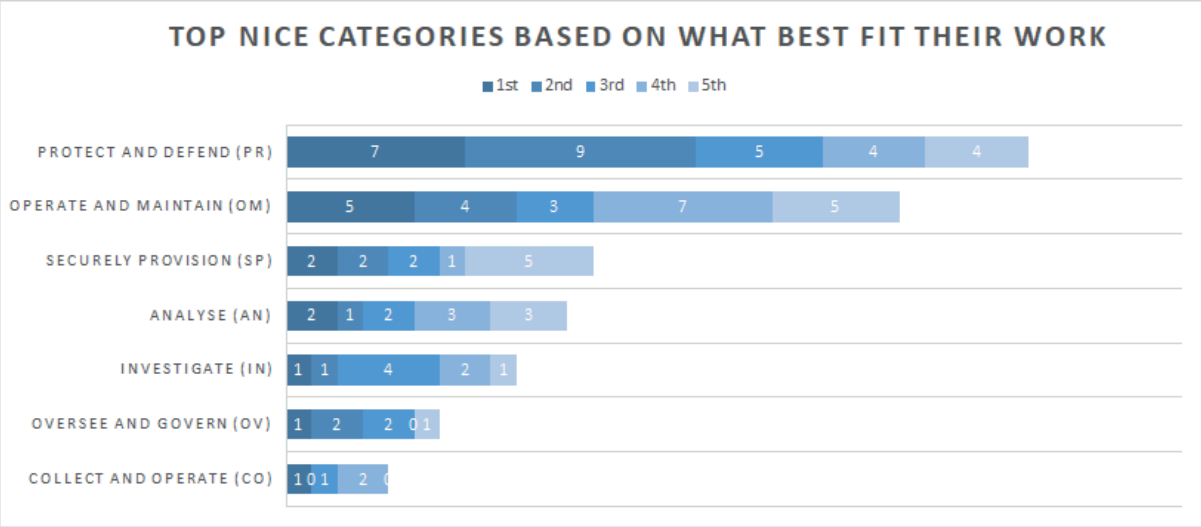


Figure 6: Top NICE categories based on what best fit their work

With this analysis of the data one can see that the bachelor's degree students are clearly employed in the "*Protect and Defend*" and "*Operate and Maintain*" categories with "*Securely Provision*" category closely behind them. "*Investigate*" and "*Analyse*" are categories that closely tie in with one another, thus they are quite similarly represented in the data. "*Oversee and Govern*" is quite administrative or managerial category with executive work roles; thus, the authors are not surprised that the bachelor's degree students do not work in

that category immediately at the end of their studies. "*Collect and Operate"* category has described as intelligence gathering and offensive operations performed within the cyber domain, and as such it was the lowest category to receive answers.

To get a better view of the most frequent work roles we filtered 3rd to 5th selections from the data (still visible in figure 5) to get an understanding of what are the primary work roles of the respondents. This visualization can be seen in figure 7.

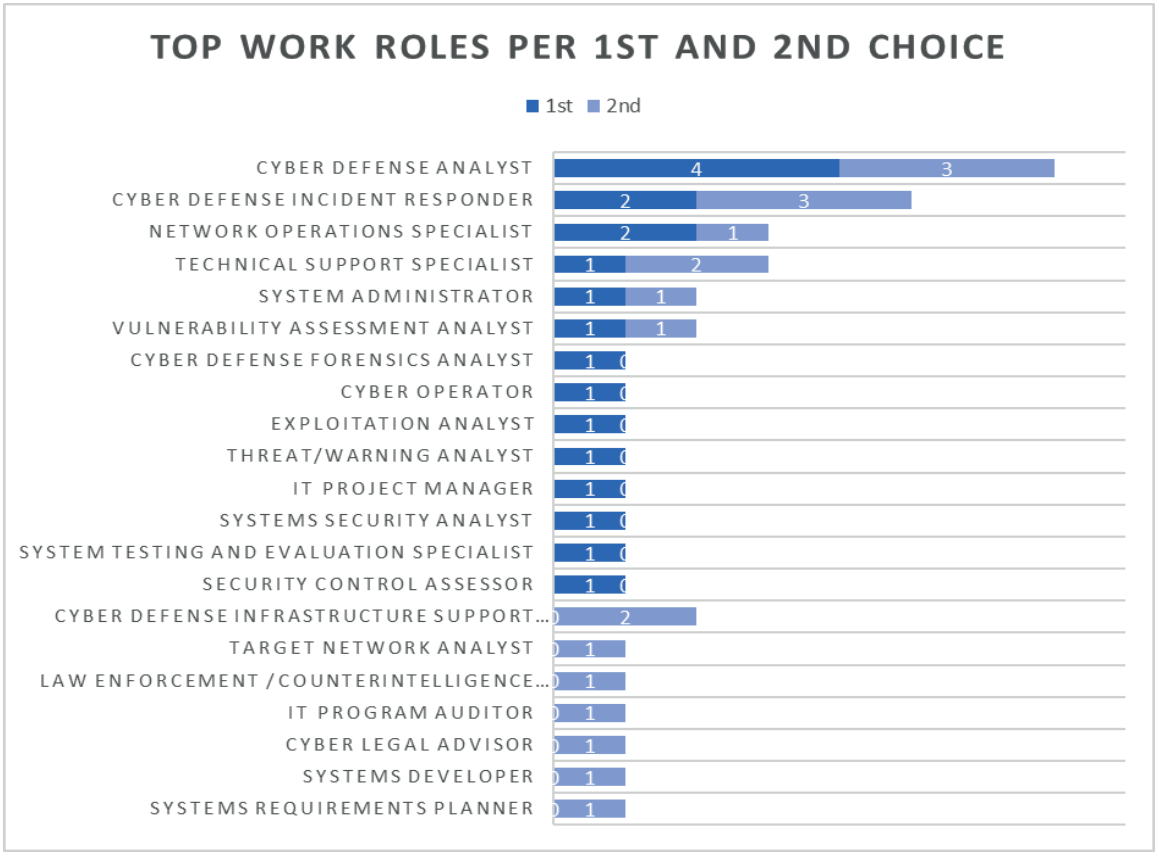


Figure 7: Top NICE categories based on what best fit their work

Almost all the data was either in "*Cyber Defense Analyst"* or "*Cyber Defense Incident Responder"* work roles with both belonging to "*Protect and Defend*" category. The authors would assume these two work roles of NICE Framework to be essential parts of the current establishment of Security Operations Centres (SOCs) within Finland (Carson, 2014), a growing private and public sector functionality within the field of Cyber Security (Jauhiainen, 2021). The newly graduated would most probably be workforce to create, upkeep or provide this service.

4.3 Cyber Security Specialisation in Retrospective

At the end of the survey, the hindsight of the students is asked; "How would you choose your specialisation modules nowadays, with all the knowledge of your current work occupation and your hindsight of the studies". The student could choose two 30 ECTS modules but not the same module twice.

Noteworthy is that the module selection is available at the University of Applied Sciences they graduated from, but from a newly updated curriculum (JAMK University of Applied Sciences, 2021). The students were asked to familiarise themselves with the updated curriculum and then make their module selections. One central theme of the curriculum is to divide the modules into the *"DevSecOps"* ideology (Sánchez-Gordón & Colomo-Palacios, 2020) within ICT; the acronym standing for *"Dev"* being developers, *"Sec"* meaning (cyber) security and *"Ops"* as Operations. Results from the student answers are visualised in the Figure 8.

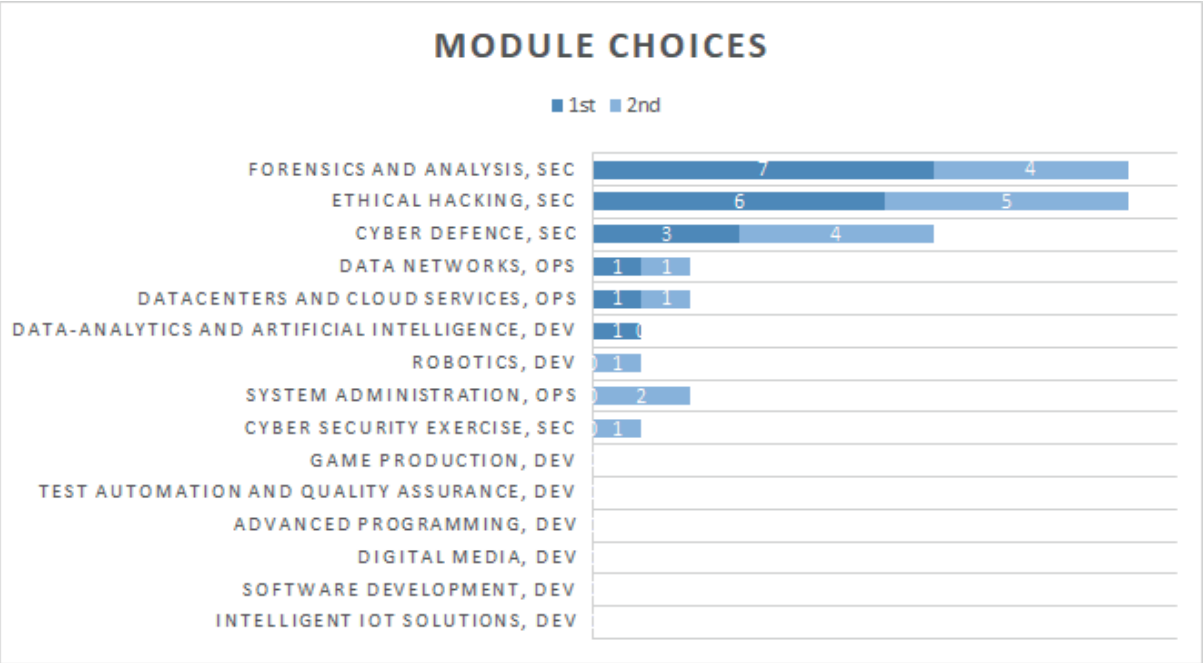


Figure 8: Specialisation modules of the bachelor's degree

An encouraging result from the survey data is that the module choices would still focus on Cyber Security. These top three modules are considered by the ICT degree programme coordinators to be a part of Cyber Security specialisation. The following two choices *"Data Networks"* and *"Datacentres and Cloud Services"* are more in the Operations section of the curriculum but noticeably related to some students' current work. This ties well with the results in Figure 6 as *"Operate and Maintain"* category was the second most descriptive category of their work.

One misstep of the authors was that we did not ask the alumni students about what modules they already had studied. Without this information it is impossible trace back Figure 8 data as being a new selection of the participants or did they just confirm that they would choose the same module they did once again, supposing they were freshly started students. Still, it would indicate the trend, that they wish to further emphasise their studies in Cyber Security. And as an education organisation it would give a confirmation to the university that these specialisation studies should be offered to the industry as a part of life-long learning.

5. Conclusion

Given the results and analysis, one can conclude that the cyber security students graduate and get employed to "*Protect and Defend"* the Critical Infrastructure through ISPs and work with the safety of "*Digital Services and Platforms"* in Finland. Our research data can be interpreted to prove that students are employed to be ensuring the functionality of the Finnish Cyber Domain as the Cyber Security Strategy of Finland stated.

Through our research the education organizers (at JAMK) can now have a better understanding of the work placements of their former students in the field of Cyber Security. Adjustments of the curriculum can be based on researched data. By researching the education landscape (Saharinen et al, 2020), industry need (Jaurimaa et al, 2020) and student employment and satisfaction data the degree programme coordinators can verify their curricula to be up to date, have an ongoing discussion with the industry and provide current students of the degree programme information about their module choices.

The timeline of the different, parallel cyber security frameworks gives a view of the evolving atmosphere around cyber security education. Different frameworks have varying amount of scientific research behind them, and this is typically stated in publication of the framework. The authors of this paper would like to conclude that all additions are of course an enrichment of the field, but for an education organisation; it would be preferrable to establish a basis of education on one of the frameworks (Saharinen et al, 2019) and proceed with the chosen framework consistently throughout the curriculum.

6. Discussion

The lifespan of a bachelor's degrees varies from three to four years in the Finnish education system (Ministery of Education and Culture - Finland, 2021). Given the degree completion length of the participating students in the research, there are six different cyber security frameworks published as visualized in Figure 1. The authors would assume that many of these Finnish cyber security degree programmes were started purely to respond to an industry need, however, also to meet this governmental resolution in Finland. Their formation might have come from an earlier information security orientation degree background, rather than a guiding cyber security framework or a governmental guidance, enforcing a clear degree structure and content. Thus, education organizations are trying to hit a moving target with their module and course structures within their curricula, that should be publicly available as mandated by the ECTS Users' Guide (European Comission, 2015).

Finland has a national graduands feedback questionnaire system (Rectors' Conference of Finnish Universities of Applied Science, 2021) in place; however, the questionnaire is generalised to cover all education fields in the Universities of Applied Sciences. Although it gives useful data to the educating organisations, it rarely has relevant data on a certain degree field. The data is aggregated to Finland's Ministry of Education specific "Fields of Steering" and thus it does not even mention a specialisation of the degree, such as Cyber Security in ICT. Our research in this paper could and should be replicated to various universities to gain a better understanding of the graduands of cyber security.

Acknowledgements

This work has been done in Jyväskylä University of Applied Sciences (JAMK) which is participating in LIPPA - project – Quality to ICT Education from Industry and Education collaboration (project code S22466) funded by European Social Fund.

The authors would like to thank Tuula Kotikoski for her contribution in proofreading the English language on the paper.

References

Associate for Computing Machinery. (2017) *Cybersecurity Curricula 2017 - Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity.* New York: Associate for Computing Machinery.
Associate for Computing Machinery, n.d. *Curricula Recommendations.* [online] https://www.acm.org/education/curricula-recommendations
Carson, Z. (2014) *Ten Strategies of a World-Class Cybersecurity Operations Center.* s.l.:The MITRE Corporation.
CC2020 Task Force, 2020. *Computing Curricula 2020: Paradigms for Global Computing Education.* s.l.:Association for Computing Machinery.
Catota, F.E., Morgan, M.G. and Sicker, D.C. (2019) Cybersecurity education in a developing nation: the Ecuadorian environment, *Journal of Cybersecurity*, 5(1), p. tyz001. doi:10.1093/cybsec/tyz001.
ENISA (2021) *CYBERHEAD - Cybersecurity Higher Education Database.* [online] https://www.enisa.europa.eu/topics/cybersecurity-education/education-map
European Comission, 2015. *ECTS Users' Guide.* [online] https://ec.europa.eu/assets/eac/education/ects/users-guide/docs/ects-users-guide_en.pdf
European Comission, (2020) *The EU's Cybersecurity Strategy for the Digital Decade.* [online] Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
JAMK University of Applied Sciences. (2013) *Cyber Security, Master of Engineering.* [online] https://www.jamk.fi/en/Education/Technology-and-Transport/Cyber-Security-Masters-Degree/
JAMK University of Applied Sciences. (2015) *Bachelor of Engineering, Information and Communications Technology.* [online] https://www.jamk.fi/en/Education/Technology-and-Transport/information-and-communication-technology-bachelor-of-engineering/
JAMK University of Applied Sciences. (2021) *Bachelor's Degree Programme in Information and Communications Technology.* [online] https://opetussuunnitelmat.peppi.jamk.fi/en/48/en/5290/TTV2021SS/year/2021
Jauhiainen, J. (2021) *List of SOC service providers.* [online] https://csoc.fi/
Jaurimaa, J., Saharinen, K. and Kotikoski, S. (2021) Critical Infrastructure Protection: Employer Expectations for Cyber Security Education in Finland, in *Proceedings of the 2021 20th European Conference on Cyber Warfare*

and Security. *European Conference on Cyber Warfare and Security*, United Kingdoms: Academic Conferences International Limited. doi:10.34190/EWS.21.015.
Karinsalo, A. et al. (2021) [online] Available at: https://cybersec4europe.eu/wp-content/uploads/2021/06/D6_3_Design-of-Education-and-Professional-Frame-work_Final.pdf
Limnéll, J. (2016) The cyber arms race is accelerating – what are the consequences?, *Journal of Cyber Policy*, 1(1), pp. 50–60. doi:10.1080/23738871.2016.1158304.
Metropolia University of Applied Sciences (2021) *Cyber Security specialization studies.* [online] https://www.metropolia.fi/fi/opiskelu-metropoliassa/osaamisen-taydentaminen/erikoistumiskoulutukset/kyberturvallisuus
Ministery of Education and Culture - Finland (2021) *Finnish Education System.* [online] https://okm.fi/en/education-system
Nai Fovino, I. et al. (2019) *A Proposal for a European Cybersecurity Taxonomy.* [online] https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf
Newhouse et al. (2017) *National.* s.l.:National Institute of Science and Technology.
Nurse, J. R. et al. (2021) [online] https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education/@@download/fullReport
Piesarskas, E. et al. (2020) [online] https://sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf
Rashid, A. et al. (2019) *The Cyber Security Body of Knowledge.* [online] https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf
Rashid, A. et al. (2021) *The Cyber Security Body of Knowledge.* [online] https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf
Rectors' Conference of Finnish Universities of Applied Science, 2021. *University of Applied Sciences Graduand Feedback Questionnaire.* [online] https://avop.fi/en
Saharinen, K., Backlund, J. & Nevala, J. (2020) *Assessing Cyber Security Education through NICE Cybersecurity Workforce Framework.* New York, NY, USA, Association for Computing Machinery, p. 172–176.
Saharinen, K., Karjalainen, M. & Kokkonen, T. (2019) *A Design Model for a Degree Programme in Cyber Security.* New York, NY, USA, Association for Computing Machinery, p. 3–7.
Sánchez-Gordón, M. & Colomo-Palacios, R. (2020) *Security as Culture: A Systematic Literature Review of DevSecOps.* New York, NY, USA, Association for Computing Machinery, p. 266–269.
Shackelford, R. et al. (2005) In: *Computing Curricula 2015.* s.l.:The Association for Computing Machinery (ACM); The Association for Information Systems (AIS); The Computer Society (IEEE-CS).
South-Eastern Finland University of Applied Sciences (2021) *Bachelor of Engineering, cyber security.* [online] https://www.xamk.fi/koulutukset/insinoori-amk-kyberturvallisuus/
The Security Committee of Finland (2013) *Finland's Cyber security Strategy.* [online] https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
The Security Committee of Finland, 2019. *Finland's Cyber security Strategy 2019.* [online] https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf
United Kingdom (2016) *National Cyber Security Strategy 2016-2021.* [online] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
University of Jyväskylä (2013) *Cyber Security, Master of Philosophy.* [online] https://www.jyu.fi/it/fi/opiskelu/maisteriohjelmat/kyberturvallisuus
Whyte, C. (2020) Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare, *Journal of Cybersecurity*, 6(1), p. tyaa013. doi:10.1093/cybsec/tyaa013.
Willoughby, T. et al. (2021) A Long-Term Study of What Best Predicts Graduating From University Versus Leaving Prior to Graduation, Journal of College Student Retention: Research, Theory & Practice. doi: 10.1177/1521025120987993.
Zan De, T. & Di Franco, F. (2019) *Cybersecurity Skills Development in the EU.* [online] https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/@@download/fullReport

PVIII

ANALYSING FINNISH CYBERSECURITY THESIS TOPICS USING TAXONOMIC FRAMEWORKS

by

Joonatan Ovaska, Karo Saharinen and Tuomo Sipola 2022

2022 IEEE International Conference on Cyber Science and Technology Congress (CyberSciTech).

DOI: https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927808

Analysing Finnish Cybersecurity Thesis Topics Using Taxonomic Frameworks

Joonatan Ovaska
Institute of Information Technology
Jamk University of Applied Sciences
Jyväskylä, Finland
joonatan.ovaska@jamk.fi

Karo Saharinen
Institute of Information Technology
Jamk University of Applied Sciences
Jyväskylä, Finland
karo.saharinen@jamk.fi

Tuomo Sipola
Institute of Information Technology
Jamk University of Applied Sciences
Jyväskylä, Finland
tuomo.sipola@jamk.fi

***Abstract*—This paper presents an analysis of Bachelor's and Master's cybersecurity theses in Jyväskylä, Finland. The theses were gathered from publicly available publishing platforms of Finnish universities and were analysed using the NICE Cybersecurity Workforce Framework (NCWF) categories and European Cyber Security Organization's (ECSO) The European Cybersecurity Taxonomy. The aim of this research was to find whether there clearly were emphasis on certain framework categories or work roles. Similarly, industry sectors about which cybersecurity theses were done were of interest. The results can be used by education providers to align and plan their education based on regional needs, and cybersecurity students, before starting their thesis project, can use this information to deliberate suitable work sectors in which theses are lacking. As our research results point out, there is a clear emphasis on certain NICE categories and work roles that are more common within the dataset. However, it is prudent to take into account the scope of the dataset, which was specific to one region in Finland. While this research presents findings about this one region, researchers from around the world can consider using the same research methods on a similar datasets gathered from their respective regions.**

***Index Terms*—Cybersecurity, Education, Thesis, NICE Framework**

I. Introduction

A. Cybersecurity as a Field of Education

Already in 2018, a study in the field of cybersecurity education reviewed and analysed 21 cybersecurity master's programmes with a content, structure, requirements, duration, etc. [1]. A UK case study about cybersecurity education and accreditation analysed this subject in the scope of UK, which was compared to the US [2].

The security committee of Finland was established in 2012 and released a program for the implementation of the national cybersecurity strategy [3] in March 2013. One point of the implementation was to establish cybersecurity education on all levels of the Finnish educational system. Both organisations at the higher education institution (HEI) level in Jyväskylä, Jamk University of Applied Sciences (JAMK) and University of Jyväskylä (JYU), started their master's degrees in cybersecurity around 2013 [4], [5]. JAMK established a bachelor's degree in 2015. Within the decade more and more HEIs in Finland started to establish courses or full degrees in cybersecurity as Lehto and Niemelä point out [6].

B. Government Decrees on the Universities

The HEIs are regulated by Government Decree on Universities of Applied Sciences [7] and Decree on Universities [8], [9]. The mission of the scientific universities of Finland, by law, is to freely further scientific research, provide scientific education and civilise artistically and *interact with the society* . The mission of the universities of applied sciences, by law, is to *practice research, development, innovation and artistic actions to improve working life and regional development* [7].

Ministry of Education and Culture in Finland has written down that studies must have certain structure which includes a thesis project [7]. Each programme leading either to a Bachelor's degree or Master's degree must have a thesis, this also applies to the field of all universities. Theses for this analysis are gathered from programmes in this category and only from publicly available sources. Bachelor's theses are worth of 15 European Credit Transfer and Accumulation System (ECTS) credits and Master's theses from both JAMK and JYU are worth of 30 (ECTS) [10].

C. Our contribution

This research categorizes the thesis topics from two Finnish universities according to taxonomic frameworks. This is done to map the topics to industry and workforce needs and gain insight into how well the educational outcomes correspond to the frameworks. This is a rarely studied topic, especially within the context of the Finnish educational system.

II. Literature and Frameworks

A. Degree Levels

For measuring the degree levels of the analysed theses, we can use European Qualifications Framework (EQF) and International Standard Classification of Education (ISCED) for a similar International level system. Leveling system for (EQF) goes from level 1 up to level 8 and (ISCED) from level 0 up to level 8, where level 8 is concidered to be highest level. Level 8 would map to Ph.D. studies while the lowest level 1 is concidered as just only a basic general knowledge. In this paper we concentrate on levels 6 & 7.

Learning outcomes can be mapped as Bachelor's degree for level 6 (EQF) and Master's degree for level 7 (EQF and

ISCED) [11] [12], for older ISCED 1997 model the corresponding leveling would be 5A-medium and 5A-long/very long programmes.

B. NICE Framework

National Initiative for Cybersecurity Education (NICE) describes the Workforce Framework for Cybersecurity (NICE Framework or NCWF). The main idea is to map certain skills and knowledge into a task. The most common use case of the NICE Framework is to assign those into a Work Role. [13] The work roles and building blocks are illustrated in Figure 1.

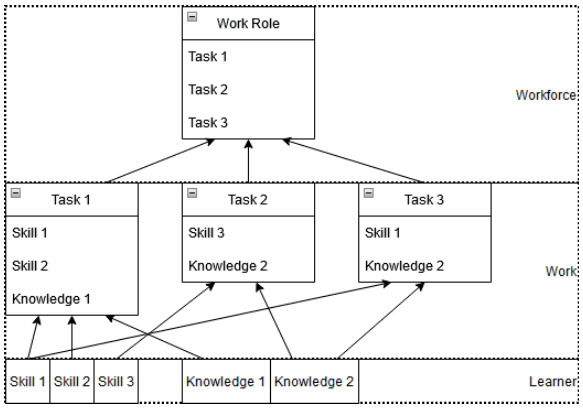


Fig. 1. Work roles' relationship to building blocks.

As the Framework evolved and got more attention, the National Institute of Standards and Technology (NIST) has updated the Framework and mapped work roles into 7 categories. Each of these categories is composed of Specialty Areas that contain one or more work roles. The work roles contain KSAs and Tasks, see Figure 2 and list below. [13]

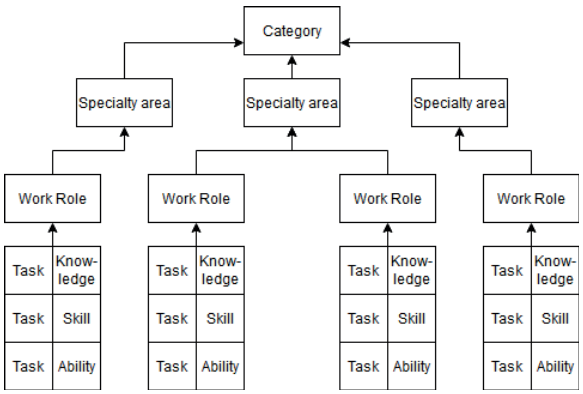


Fig. 2. Relationships among NICE framework components.

- Securely Provision (SP)
  Build secure, conceptualized, procures, designs information technology (IT) systems. Includes specialty areas such as *Technology R&D, Risk Management, Systems Architecture, etc.*
- Operate and Maintain (OM)
  Provides the support, maintance and administration for efficient and effective information technology (IT) system performance and security. Includes specialty areas such as *Network Services, Data Administration, Systems Administration, etc.*
- Oversee and Govern (OV)
  Provides direction, leadership, management or development and advocacy for organisation effective conduct cybersecurity work. Includes specialty areas such as *Strategic Planning and Policy, Legal Advice and Advocacy, Training, Education and Awareness, etc.*
- Protect and Defend (PR)
  Analyses, mitigates and identifies threats to internal information technology (IT) systems and/or networks. Includes specialty areas such as *Vulnerability Assessment and Management, Cybersecurity Defence Infrastructure Support, Cybersecurity Defence Analysis, etc.*
- Analyze (AN)
  Performs specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence. Includes specialty areas such as *Threat Analysis, All-Source Analysis, Exploitation Analysis, etc.*
- Collect and Operate (CO)
  Provides specialized deception and collection and denial of cybersecurity information that may be used to develop intelligence. Includes specialty areas *Cyber Operational Planning, Cyber Operations, Collection Operations*
- Investigate (IN)
  Investigates cybersecurity crimes and/or events related to information technology (IT) systems, digital evidence, and networks. Includes specialty areas *Cyber Investigation, Digital Forensics*

Work roles are not listed here, but a few examples are given as examples to get the idea what is the meaning of a work role: "Security Architect", "System Administrator", "Exploitation Analyst", "Cyber Crime Investigator". A single Work Role (e.g., Software Developer) could cover multiple actual job titles (e.g., software engineer, coder, application developer). A combination of roles could also be used to form a job describtion.

There are no definitions for proficiency levels (e.g., Basic, Intermediate, Advanced) in the NICE Framework. Proficiency levels and attributes describing how a learner performs Tasks, are covered by other models and resources.

NICE Framework has the following parts:

- 7 Cyber Security Workforce Categories,
- 33 Specialty Areas,
- 52 Work Roles.

Framework itself provides freedom of either using existing work roles or creating a new work roles, but this analysis is limited to use only existing work roles within the framework.

Mapping NICE Framework with EQF table can be used to generate a design model for a degree programme within field of cybersecurity. [14]

C. The European Cybersecurity Taxonomy

The European Cybersecurity Taxonomy has been reformed to complete more aspects and details than competing similar Frameworks such as NICE Framework. It covers the most sources compared to other Frameworks as contributions to Cybersecurity Taxonomy. [15]

The goal of the taxonomy is to support the mapping of the European cybersecurity competencies available. However, the taxonomy is not meant for cybersecurity products, services or processes, including operational activities.

Cybersecurity is a complex and multifaceted discipline, which leads to the need to cluster it meaningfully. The taxonomy is structured as a multi-dimensional representation of the core and traditional research domains. At the same time, it tries to take into account impacted sectors and application.

This taxonomy is proposed as three-dimensional taxonomy:

- **Research domains** represent areas of knowledge, inluding human, legal, ethical and technological aspects.
- **Sectors** for scenarios, such as energy, transport or financial sector.
- **Tehnologies and Use Cases** are the technological enablers to enchance the development of the sectors.

European cybersecurity taxonomy can be mapped to 15 Cybersecurity Domains which each have respective subdomains (e.g., Domain Cryptology has total of 14 subdomains such as “Asymmetric cryptography”, “Symmetric cryptography”, “Hash functions”, “Random number generation”, etc.). Here’s full list of main domains:

- Assurance, Audit, and Certification
- Cryptology (Cryptography and Cryptanalysis)
- Data Security and Privacy
- Education and Training
- Human Aspects
- Identity Management
- Incident Handling and Digital Forensics
- Legal Aspects
- Network and Distributed Systems
- Security Management and Governance
- Security Measurements
- Software and Hardware Security Engineering
- Steganography, Steganalysis and Watermarking
- Theoretical Foundations
- Trust Management and Accountability

The European cybersecurity taxonomy maps also different sectors which are described further in the documentation. (e.g., Defence described as “This sector embraces the activities and infrastructure required for protecting citizen, including the use of aeronautics, space, electronices, land or telecommunication systems”.) There are total of 15 sectors, but we are listing only those which had hits within this research:

- Audiovisual and media
- Defence
- Digital Services and Platforms
- Energy
- Financial
- Food and drink
- Government
- Health
- Manufacturing and Supply Chain
- Telecomm Infrastructure

Technologies and Use Cases Dimensions relates to these topics in the dimensions. Many sectors use these technologies, as there are total of 23 listed items, but we are listing only sectors which had at least one hit within this research:

- Artificial intelligence
- Big Data
- Blockchain and Distributed Ledger Technology (DLT)
- Cloud, Edge and Virtualisation
- Critical Infrastructure Protection (CIP)
- Disaster resilience and crisis management
- Fight against crime and terrorism
- Border and external security
- Local/wide area observation and surveillance
- Hardware technology (RFID, chips, sensors, networking, etc.
- Information Systems
- Internet of Things, embedded systems, pervasive systems
- Mobile Devices
- Operating Systems
- Vehicular Systems (e.g. autonomous vehicles)

III. Dataset, Scoping & Research Method

For the research scope the authors targeted theses done in Central Finland that were publicly available/released over several years which proved to be an big enough dataset to reflect findings. Regional developer scoping was chosen, Jyväskylä is a major player in Finland when it comes to cybersecurity training and education [16] [17]. In Jyväskylä there are 2 Universities which provide cybersecurity education: University of Jyväskylä and Jamk University of Applied Sciences. University of Jyväskylä provides Master’s students more theorical approach for cybersecurity. Jamk University of Applied Sciences has ICT engineering programs for both Bachelor’s and Master’s class Applied Sciences for cybersecurity [18].

Theses done for Jamk University of Applied Sciences can be found publicly from theseus [19] site. For University of Jyväskylä theses called pro-gradu, can be found from their system called JYX [20], where these theses are also publicly available. Both of these publishing databases have extensive search functionalities implemented, however they differ in terms of search functionality and filtering methods, because they are structured differently. Some of the theses contained appendixes or even whole main thesis as restricted access or hidden based on the Act of the Openness of Government Activities which allows Universities of Applied Sciences and University of Jyväskylä to have thesis which may contain hidden appendixes due research permission for confidential data [21]. Those which has not been scoped out has been determined by the abstract and topic of the thesis.

Theseus is a service for Universities of Applied Sciences for storing and sharing published theses. JYX is a digital archive which collect and display parts of JYX materials including theses from (JYU).

Used research method is mixed methods, quantity of the total scope is 173 theses, which has been qualified to match against the described Frameworks and analysed afterwards. Dataset from JAMK is from 2013 to 2020 and the dataset from JYU from 2018 to 2020. The reasoning for the scope is that this dataset was pregathered for investigation, only some theses were dropped from that dataset for not hitting the scope of cybersecurity field (e.g. Cybersecurity was only mentioned as a future research, while not being part of thesis itself). The counted total of 173 theses does not include these mentioned unscoped theses.

Most of the theses dataset could have been mapped very differently during the mapping phase these theses are tried to tied only to the category which it fits the most or is the main part of that specific thesis. Same applies for each other mapping done for work role and industry sectors also, when not specified on the orderer side.

IV. Analysis

A. NICE Categories

Based on all the collected theses by the dataset, within Figure 3 we can see the distribution of theses in NICE categories.

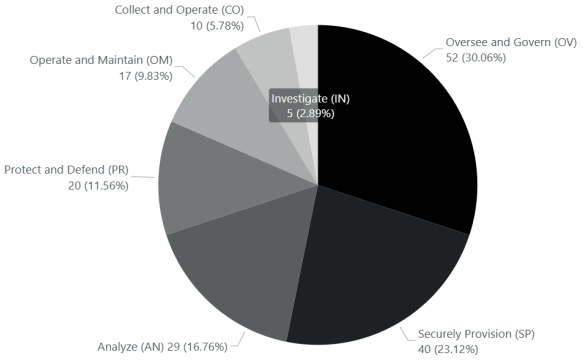


Fig. 3. Theses per NICE category.

Mapping of the we can see that over half of the mapped theses were done for “Oversee and Govern” and “Securely Provision” while categories “Investigate” and “Collect and Operate” were total of less than 10% of the works.

The authors also wanted to compare the differences on each levels of education and education organisation. Thus, we also mapped the weights of each category based on those attributes. This is visualized in Figure 4.

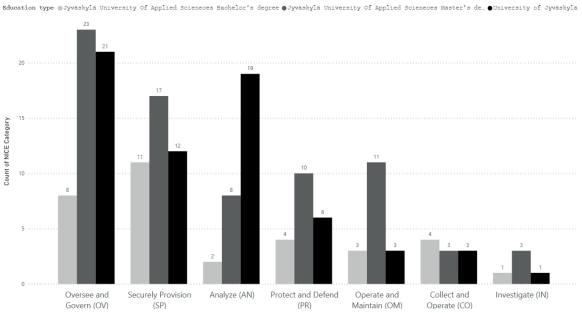


Fig. 4. Mapped categories by education type.

In Figure 5 we can see the detailed precentages of category mappings between target universities to highlight the differences and mission between the education types as described by chapter I-B. These precentages are compared towards the total number of theses in the corresponding university.

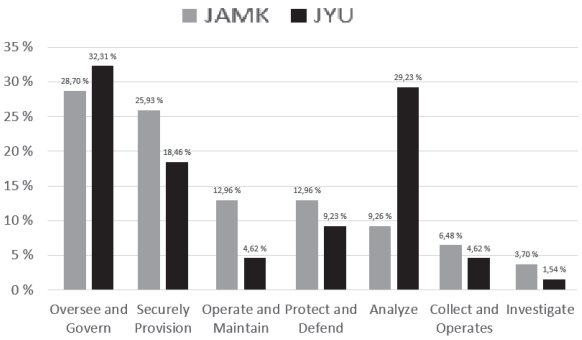


Fig. 5. Mapped categories by education type, total.

In table I we can see the more detailed amounts and precentages of these category mappings between each education type, these precentages are compared to total number of theses.

TABLE I
Categories Mapping Table

Categories	Bachelor’s (JAMK)	Master’s (JAMK)	Master’s (JYU)	Total
Oversee and Govern (OV)	8 (24.24%)	23 (30.67%)	21 (32.31%)	52 (30.06%)
Securely Provision (SP)	11 (33.33%)	17 (22.26%)	12 (18.46%)	40 (23.12%)
Analyze (AN)	2 (6.06%)	8 (10.67%)	19 (29.23%)	29 (16.76%)
Protect and Defend (PR)	4 (12.12%)	10 (13.33%)	6 (9.23%)	20 (11.56%)
Operate and Maintain (OM)	3 (9.09%)	11 (14.67%)	3 (4.62%)	17 (9.83%)
Collect and Operate (CO)	4 (12.12%)	3 (4%)	3 (4.62%)	10 (5.78%)
Investigate (IN)	1 (3.03%)	3 (4%)	1 (1.54%)	5 (2.89%)
Total	33 (19.08%)	75 (43.35%)	65 (37.57%)	173 (100%)

B. NICE Work Roles

One objective was to map each thesis towards a work role of the framework that was exactly or close to that thesis topic. Total of 37 work roles were present within the analysis. However, only top 15 had five or more hits each. There was also many work roles with only one hit. Here is the top 15 listed provided with the count of mapped roles:

1) Threat/Warning Analyst, 19
2) Reasearch & Development Specialist, 18
3) Cyber Policy and Strategy Planner, 15
4) Vulnerability Assessment Analyst, 11
5) Privacy Officer/Privacy Compliance Manager, 8
6) Cyber Instructor, 7
7) Cyber Legal Advisor, 6
7) Security Architect, 6
9) Cyber Crime Investigator, 5
9) Cyber Instructional Curriculum Developer, 5
9) Cyber Workforce Developer and Manager, 5
9) Network Operations Specialist,5
9) Security Control Assessor, 5
9) System Requirements Planner, 5
9) Systems Security Analyst, 5

These top 15 work roles cover 72.25% of all works. Remaining 27.75% were distributed between other work roles. For mapping each of these top 15 work roles for each education type we can get graph to show us the results as visualized by Figure 6.

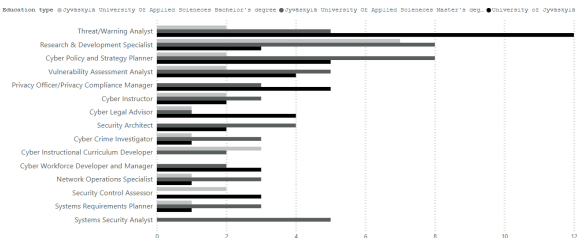


Fig. 6. Mapped work roles by education type.

As the figure shows there is much alteration between education types when mapping into work roles.

C. European Taxonomy, Industry Sectors

Theses done within University of Applied Sciences most of the time have a thesis orderer within the description page and in Scientific Universities this orderer might appear in the contents of the thesis. Given the theses where the orderer appeared, the NICE category thesis can be mapped to an industry sector e.g. telecomm company as an order would map it into "Telecomm Infrasturcture" and most of the institution orders are mapped into "Government".

Theses from University of Jyväskylä are mostly research based, there will be more of mapping with the feeling which industry would be the most relevant for the thesis, while most works would of course map to multiple sectors.

These sectors can indicate where cybersecurity play roles in current life span, obviously the most common sectors are the sectory which are heavily related to information communications technologies and government. Sector mapping listed here:

- **Government** 74, 44.31%
- **Digital Services and Platforms** 58, 34.73%
- **Telecomm Infrastructure** 17, 10.08%
- **Defence** 6, 3.59%
- **Health** 4, 2.4%
- **Financial** 3, 1.8%
- **Energy** 2, 1.2%
- **Audiovisual and media** 1, 0.6%
- **Food and drink** 1, 0.6%
- **Manufactruing Supply Chain** 1, 0.6%

Sectors can be also mapped to NICE categories as shown on the Figure 7. For the minor sectors most commonly the work was done in "Securely Provision", while the "Oversee and Govern" was on top of the more common sectors.

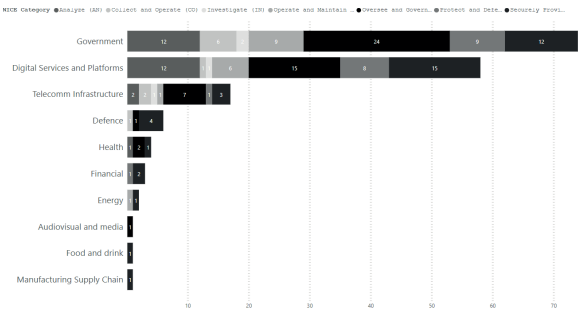


Fig. 7. European Taxonomy sectors mapped to NICE categories.

Theses around very high level of concepts or not a clear way nor order to define sector remained unmapped or has been mapped to most applyable sector.

D. Other Analysis

Used frameworks could lead for more potential findings using different correlations with different options of European Cybersecurity Taxonomy domains, industries or sectors. Instead of mapping to NICE category and NICE work roles, we could map and see how they map into European Taxonomy and compare that result between two different frameworks or just to find the domains under different taxonomy.

V. Discussion

Before making any conclusions the first observation is that neither of these chosen frameworks suits perfectly to this type of analysis. Within the dataset there was a minimal number of theses which suited to just one category of the NICE framework or just one specialty area nor one work role, as already mentioned also in the original NIST documentation.

Comparing to the European Taxonomy proposal, there are more domains in use, however in the opinion of the authors they also overlap, maybe even more than NICE categories do,

therefore the NICE categories was chosen as the main target for this study. Also the European Taxonomy offers much in names of technology and sectors, while those sectors might be quite far from the main area of cybersecurity, there could be a connection that those sectors might prefer to purchase these cybersecurity services from another company. This connection is hard to detect as typically theses were done to companies providing these *digital services and platforms* and thus were the assigned orderer of the thesis.

Frameworks are relevant to categorise different fields together and to analyse certain trends that could be emphasised and communicated to interested parties. In case of the work roles, it gives an idea what to study in order to get the work that learner is interested of, however at the same time it is quite common that students should acquire multiple skillsets in many different work roles. There are not many employers, in Finland, that can have a cybersecurity teams big enough to include each of these work roles within one company.

A. Cybersecurity as a Field

In modern world there is no sector or field that could be totally unplugged or irrelevant to the Internet which leads to the point that in every field there is a need for at least some cybersecurity. More and more devices from IoT and any other embedded system will be connected to Internet if not already. Even the industrial factories where the common ideology has been that each of the factory controlling device is plugged offline there is always a part when someone with a lack of understanding or just by accident could attach this unit to public Internet. Sometimes it could be a worker who wants to work from home fex. Covid-19 issues or maybe a business fusion with another company which has joined to the same area network.

While cybersecurity as a field is growing fast, in terms of student theses and research, this growth is not apparent in all industry sectors. However, the trend can be seen from the researched dataset already, cybersecurity is not anymore just for the most obvious sectors as in ICT, government, digital platforms, cloud computing, but it is for all.

VI. Conclusion

A. Effects of the Education Level

Since the theses were pointing to EQF levels 6 & 7, there is an effect that can be seen from the results and should be noted when making conclusions. For example basic cybersecurity work incident responder role didn't get a single match in this analysis, while it might be a common work role in the industry for lower level of education (EQF levels 4 & 5). Meanwhile, there wer many theses which related to incident response as a concept, but the thesis had more of a planning or developing nature, therefore there a different work role was selected.

Not only the level of education is pushing these results to aim higher or more advanced levels, but also the workload of the thesis project. EQF level 6 studies has approximately 400 hours workload and EQF level 7 studies has approximately 800 hours of workload for thesis project of chosen research study that could be pure research or combination of doing implementation for chosen topic. This will effect the targeted work role as the workload is not too small the project is often pushed towards the mapping of higher hierarchy workforce.

B. Differences Between the Universities

For the chosen fields and subjects there could be seen trends between the two universities. JAMK students more often related their work, that could be at least somewhat correlated, to provided courses. Meanwhile, JYU theses more often included analytical research than implementations.

As Figure 5 shows JAMK theses are more often towards categories "Securely Provision", "Operate and Maintain", "Protect and Defend", while JYU theses maps more often towards "Oversee and Govern" and "Analyze".

C. NICE Categories

While the dataset has least amount of data from Bachelor's degree theses they still pointed out to be much more focused on implementations by having a comperable high amount of works for "Securely Provision" and "Protect and Defend", also the third biggest total category analyze had only 2 works from Bachelor's level, mean while it was huge in (JYU) Master's theses, while not the first one, which was Oversee and Govern, which is somewhat same nature with the analysis category.

Investigate category has only 3 work roles and 2 specialty areas in it, and that could be also seen from these works that it's more rare to thesis land in this area, also there could be much of work loads which is not a good idea to give for a thesis project, being criminal investigation etc. Meanwhile there is definately work roles that exists in the real world, while it is clear that theses aren't done within these lines of work based on our research data.

The most mapped category, "Oversee and Govern", suits probably the best to these levels of research, I wouldn't say that there is not that much of work roles in work life as there was mapped theses for that category. Meanwhile there definately is work roles, it might not just be as big of a field that these statistics are providing.

D. NICE Work Roles

Surprisingly, there was one work role that stood clearly, with four (4) as clear leaders. "Threat/Warning analyst" was clearly the most mapped work role, while also "Research & Development Specialist" was the 2nd most mapped work role in this analysis. "Cyber Policy and Strategy Planner" and "Vulnerability Assessment Analyst" were both mapped over 10 times. Theses from JYU were clearly most mapped to "Threat/Warning Analyst", while Bachelor's theses' most common mapping was "Research & Development Specialist". Other top 4 work roles were quite even among different education types. Something to mention outside the top 4 is that all 5 works mapped to "Systems Security Analyst" were exclusively from the University of Applied Sciences Master's thesis.

Another interesting finding was that while University of Jyväskylä concentrated more on works around research fields,

there were no mappings for "Cyber Instructional Curriculum Developer" work role. However, this might reflect the fact that these theses were extracted from the IT field including Cybersecurity as a search parameter and those works might be done for different fields of studies, e.g., Teacher Education.

E. European Taxonomy Industry Sectors

European Taxonomy Industry Sectors had hits only for about half of the industries. Meanwhile, multiple sectors had one hit in the complete dataset. In the rare cases they were mostly "Securely Provision" hits, which are more often implementation or system requirement based hits. If we would look the non-top 3 hits without "Securely Provision" works included, the amount of works and industries would cut lower than 50%.

The methodology in the University of Applied Sciences on thesis projects encourages to find a commissioner for the thesis, therefore the mappings to rare industries were because of these commissioners. The other two industries that gained considerable amount of theses were from Health and Financials in the data from University of Jyväskylä. Health as an industry and as a regional determiner play a big role when looking at the location of Jyväskylä in Central Finland. There is a new hospital built recently and opened in early 2021 [22] [23]. These theses were done before that time, but could be related to that project.

F. Other Observations

NICE Framework is suitable for obtaining data when asking where the work is and what kind of work orders have been given. Also, the courses and the nature of studies played a role in the thesis categories. This dataset scope can be used for regional education development while it also gives an example for future research and possibilities in other geographic locations.

While the framework makes this mapping possible, there is room for subjective evaluation: another person could map some of the works differently by weighting the main topic differently, while it could be technically possible to map same works with multiple attributes. The authors considered the possibility, but concluded to go with only one category per thesis. More advanced mathematical analysis methods could be used to investigate the dataset. However, the authors could draw up relevant conclusions with the analysis methods used in this paper.

G. Future Research

This data could be used to improve regional focus of education. This could be achieved by developing courses towards the work roles, categories and industries that were found during this work. These findings can also be used internationally to reflect the current state and to compare to other regions or perform similar research as an inspiration. With this dataset there are possibilities to look at other aspects concerning the topic or carry out research around European Taxonomy Domains mapping analysis.

ACKNOWLEDGMENT

This research was supported by European Social Fund 2021–2023 as part of the LIPPA research and development project which is supporting smooth transitions from ICT studies to work life [24].

REFERENCES

[1] K. Cabaj, D. Domingos, Z. Kotulski, and A. Respício, "Cybersecurity education: Evolution of the discipline and analysis of master programs," *Computers & Security*, vol. 75, pp. 24–35, 2018.

[2] T. Crick, J. H. Davenport, A. Irons, and T. Prickett, "A uk case study on cybersecurity education and accreditation," in *2019 IEEE Frontiers in Education Conference (FIE)*, 2019, pp. 1–9.

[3] The Security Committee, "Implementation programme for Finland's cyber security strategy," pp. 47–48, 2014, (in Finnish), retrieved May 21, 2022. [Online]. Available: https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Kyberturvallisuusstrategian-toimeenpano-ohjelma.pdf

[4] University of Jyväskylä, "MSc cyber security," n.d., retrieved June 3, 2022. [Online]. Available: https://www.jyu.fi/it/fi/opiskelu/maisteriohjelmat/kyberturvallisuus/masters-degree-programme-in-cyber-security

[5] JAMK University of Applied Sciences, "Educate yourself to be a cyber security professional," n.d., retrieved May 31, 2022. [Online]. Available: https://www.jamk.fi/en/Apply-to-Jamk/masters-degree/educate-yourself-to-be-a-cyber-security-professional

[6] M. Lehto and J. Niemelä, *Kyberalan tutkimus ja koulutus Suomessa 2019*, ser. Informaatioteknologian tiedekunnan julkaisuja, P. Neittaanmäki, Ed. Jyväskylä: University of Jyväskylä, 2019, no. 83/2019, retrieved May 30, 2022. [Online]. Available: https://www.jyu.fi/it/fi/tutkimus/julkaisut/it-julkaisut/kyberalan_koulutus_suomessa_verkkoversio.pdf

[7] Ministry of Education and Culture, "Government decree on universities of applied sciences," 2014, retrieved May 21, 2022. [Online]. Available: https://finlex.fi/en/laki/kaannokset/2014/en20141129.pdf

[8] "Valtioneuvoston asetus yliopistojen tutkinnoista," 2004, 794/2004, retrieved May 30, 2022. [Online]. Available: https://www.finlex.fi/fi/laki/alkup/2004/20040794#Pidp446675200

[9] "Yliopistolaki," 2004, 24.7.2009/558, retrieved May 30, 2022. [Online]. Available: https://www.finlex.fi/fi/laki/ajantasa/2009/20090558

[10] E. Commission, "Ects users' guide 2015," p. 11, 2015, retrieved May 25, 2022. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/da7467e6-8450-11e5-b8b7-01aa75ed71a1

[11] European Commission, "European qualifications framework," 2017, retrieved May 25, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017H0615(01)&qid=1552997420044&from=EN

[12] UNESCO Institute of Statistics, "International standard classification of education isced 2011," 2011, retrieved May 25, 2022. [Online]. Available: https://web.archive.org/web/20170106011231/https://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

[13] National Institute of Standards and Technology, "Workforce framtework for cybersecurity (NICE framework)," 2020, retrieved May 25, 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

[14] K. Saharinen, M. Karjalainen, and T. Kokkonen, "A design model for a degree programme in cyber security," in *Proceedings of the 2019 11th International Conference on Education Technology and Computers*, ser. ICETC 2019, 2019, pp. 3–7.

[15] European Commission, "A proposal for a european cybersecurity taxonomy," 2019, retrieved May 26, 2022. [Online]. Available: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

[16] R. M. Savola, "Current level of cybersecurity competence and future development: case Finland," in *Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings*, ser. ECSA '17, 2017, pp. 121–124.

[17] M. Lehto, "Cyber security competencies: cyber security education and research in finnish universities," in *Proceedings of the 14th European Conference on Cyber Warfare & Security*, ser. ECCWS 2015, 2015, pp. 179–188. [Online]. Available: http://urn.fi/URN:NBN:fi:jyu-201507092560

[18] Ministry of Education and Culture, “Agreements with universities of applied sciences,” n.d., (in Finnish), retrieved May 31, 2022. [Online]. Available: https://okm.fi/ammattikorkeakoulut-sopimukset

[19] Arene ry, “Database for theses from universities of applied sciences in finland,” n.d., retrieved May 31, 2022. [Online]. Available: https://www.theseus.fi/

[20] University of Jyväskylä, “Jyväskylä university digital repository,” n.d., retrieved May 31, 2022. [Online]. Available: https://jyx.jyu.fi/?locale-attribute=en

[21] Ministry of Jucstice, “Act on the openness of government activities,” 2015, 621/1999, amendments to 907/2015 included, retrieved May 31, 2022. [Online]. Available: https://www.finlex.fi/en/laki/kaannokset/1999/en19990621_20150907.pdf

[22] Keski-Suomen sairaanhoitopiiri, “Move to new hopital was success,” 2021, retrieved May 31, 2022. [Online]. Available: https://www.sairaalanova.fi/fi-FI/Ajankohtaista/Muutto_Sairaala_Novaan_sujui_erinomaises(62659)

[23] ——, “Organising and producting health and social services in central finland 2021-2023,” 2021, retrieved May 31, 2022. [Online]. Available: https://www.sairaalanova.fi/fi-FI/Sairaanhoitopiiri/Terveydenhuoltolain_mukainen_jarjestamis(62970)

[24] Ministry of Employment and the Economy, “LIPPA quality for ICT studies from the working life interface,” 2021, retrieved May 31, 2022. [Online]. Available: https://www.eura2014.fi/rrtiepa/projekti.php?projektikoodi=S22466

PIX

ANALYSING CYBERSECURITY EDUCATION IN DEGREE PROGRAMMES OF FINNISH UNIVERSITIES

by

Karo Saharinen, Vesa Leino, Tero Kokkonen, Tuomo Sipola and Timo Hämäläinen 2022

Journal of Information and Computer Security, Accepted with Revisions.

URL: https://www.emeraldgrouppublishing.com/journal/ics

Analysing Cybersecurity Education in Degree Programmes of Finnish Universities

Karo Saharinen[1], Vesa Leino[1], Tero Kokkonen[1], Tuomo Sipola[1], and Timo Hämäläinen[2]

[1]Jamk University of Applied Sciences
[2]University of Jyväskylä
email: karo.saharinen@jamk.fi, vesa.leino@gmail.com, tero.kokkonen@jamk.fi, tuomo.sipola@jamk.fi, timo.t.hamalainen@jyu.fi

Abstract

Finland's Cyber Security Strategy has called for the strengthening of cybersecurity education within all levels of the education system. This paper analyses this strengthening through quantitative measure-ment of degree programmes of the Finnish Higher Education. The scope is set to Bachelor's and Master's Degrees related to the field of of Information and Communications Technology in Finland. The gathered dataset of curricula between 2018 and 2020 was harmonised and reflected through a cybersecurity frame-work, which describes the workforce of cybersecurity. These cybersecurity frameworks are an ongoing research and development topic as described in the theory section. The analysis of the gathered data brought up evidently that certain categories of the framework were heavily emphasised and that there was a proven difference between the focus of the Master's and Bachelor's degrees. It was reassuring that to a certain extent purely cybersecurity related courses were also present in the compulsory parts of the degrees. Based on our data, some categories of the cybersecurity framework were neglected based by course offerings. This does not mean they might be smaller topics within the other courses, however they did not have a course of their own. The conclusion is that the education system of Finland, within the scope of the research, is educating the field of cybersecurity adequately and provides courses in it within the specialty or elective studies. Certain sections of the cybersecurity framework evidently have room for additional education offering. Based on our research and the open dataset, other educators can reflect their own curricula through the same means for a more adapt approach in cybersecurity education in a degree programme.

Keywords: Cybersecurity, Education, Degree Programme, Cybersecurity Workforce

1 Introduction

Given the frequent cybersecurity incidents and threats facing the world, one might assume the education sector is hastily reacting to the current development of the field by increasing cybersecurity education throughout its information and communications technology (ICT) curricula's. For example, the European Cyber Security Organisation, ECSO, has announced the requirement for cybersecurity education and professional training (European Cyber Security Organisation, 2017). ECSO has also announced estimation by Frost & Sullivan about 1.8 million cybersecurity professionals workforce deficit by 2022 (European Cyber Security Organisation, 2018). This lack of competent workforce is the concern of many different publications (European Union Agency for Cybersecurity, 2021; European Comission, 2020; McHenry et al., 2021).

In Finland, the Prime Minster's Office published a research by Lehto et al. (2018) on how cybersecurity should be organized and lead within Finland. To enforce the strategic leadership of cybersecurity, the research paper recommended, among other things, to establish a national cybersecurity director in Finland. This director was appointed in 2020[1] into the Ministry of Traffic and Communications. In 2021, this director was the sole writer of the updated Cyber Security Development Programme (Paananen, 2021) in which the first theme and chapter based on creating world class competence and directing enough resources for education of cybersecurity.

At the end of 2021 the Minister of Education and Culture declared 2300 additional study places within the higher education of Finland (Ministry of Education and Culture, 2021b). These study places were distributed to different fields of education in both Higher Education Institutions of Finland; the Universities and the Universities of Applied Sciences (Ministry of Education and Culture, 2021a; Ministry of Education and Culture, 2021c). This declaration did not exactly target cybersecurity education, however 424 places were directed to the field of ICT. This follows the Higher Education and Research Vision 2030 workgroup proposal (Ministry of Education and Culture, 2017) and the current Government Programme of Finland (Finnish Government, 2019); to increase the amount of citizens with a higher education up to 50 percent of the population (at least a bachelor's degree).

The Ministry of Education and Culture steers the higher education institutions of Finland through agreements[2] established per institution. These agreements are publicly available on the webpages of the Ministry and are currently set to last from 2021 through 2024. The agreements are formed through the following structure:

- Strategic goals, choices and profiles
- Core areas and newly emerging scientific fields
- Degree objectives (or completed degree goals)
- Following of results and funding

When searched through all of the agreements, cybersecurity could be found in only one University of Applied Sciences Agreement and in none of the agreements between the Ministry and Universities of Finland. This does not mean that cybersecurity is not taught or a subject within these universities, but clearly it has not risen as a significant field amongst other fields of education, research and development.

This is intresting as the Finnish Cyber Security Strategy has demanded since 2013, that cybersecurity education should be established and implemented on all levels of education in Finland (Secretariat of the Security Committee, 2013). The updated 2019 version of the strategy (Secretariat of the Security Committee, 2019) continues on the same path with the following statement:

> "Training programmes related to cyber and information security, software and application development, information networks and telecommunications in vocational education, universities of applied sciences and universities will be strengthened."

There is not much publically available data on how this strengthening has occurred in Finland and what results it has yielded nor is it visible in any of the prementioned agreements. Different cybersecurity strategic papers and development programs have been written, however actual open data on how they have succeeded has not been made easily available. A report by Lehto et al. (2017) mostly mentions the education sector of other countries to have degree programmes of their own dedicated solely for cybersecurity.

Outside of Finland the cybersecurity education has been studied through e.g. interviews (Catota, Morgan, and Sicker, 2019), literature reviews of cybersecurity education oriented papers (Švábenský, Vykopal, and Čeleda, 2020) and where the education field should head towards in 2030 (Parrish et al., 2018). After researching 1174 papers Švábenský, Vykopal, and Čeleda (2020) concluded that:

[1] https://www.lvm.fi/-/national-cyber-security-director-appointed-1033628
[2] https://okm.fi/en/steering-financing-and-agreements

> A typical SIGCSE/ITiCSE cybersecurity education paper deals with topics such as secure software development, network security, cyber attacks, cryptography, or privacy. It describes a course, hands-on exercise, or a tool applied in teaching practice, in the context of a North American university. It usually reports data and teaching experience from a period of one semester, with a population of several dozens of undergraduate students.

Based on this, there was a clear lack in international research papers on researching the whole higher education curricula structure of a nation. A report in Finland by Lehto, Niemelä, and Vähäkainu (2019) took the aspect of going through these Finnish curricula, however it only lists the available course names and codes in different educational organisations in Finland. The report does not take into account, if the courses are in any way mandatory; they just exist within the curricula and have cybersecurity (or the name can be interpreted to be related to cybersecurity) written in the course name. No apparent structure of course categorisation into cybersecurity is apparent in the report.

Based on this background, our leading research questions are as follows:

- How has the cybersecurity education actually been implemented in curricula's of different, organisationally independent and geographically distributed universities of Finland?
- How are the courses distributed by Core, Specialty and Elective studies?
- What is the quantitative precentage of cybersecurity education within the degree programmes based on the number of ECTS credits?

To answer these questions, the authors approached the issue by measuring quantitatively the amount of cybersecurity related studies on course catalogues of Finnish Universities. The scope is set to be Bachelor's and Master's Degrees respectively. As cybersecurity is mainly considered a technical field, our research targeted degree programmes categorised into the field of Information and Communications Technology (Statistics Finland, 2022; UNESCO Institute for Statistics, 2015). These are typically present and taught in organisational units related to technology or business, but sometimes can be found in defence related education.

2 Higher Education in Europe

European Qualifications Framework (EQF) sets out the levels of education (Council of the European Union, 2017). These levels are recommended to be be targeted by the qualifications granted within the member states of the European Union. The EQF also encompasses previous work carried out in e.g. The Framework for Qualification of the European Higher Education (Bologna Working Group, 2005) (QF-EHEA). The eight level framework presented in table 1.

Table 1: Education levels within the European Qualifications Framework

EQF	**QF-EHEA**	**Degree**[1]
Level 1		Basic Education
Level 2		Basic Education
Level 3		Basic Education
Level 4		Matriculation and Vocational qualifications
Level 5		Specialist vocational qualifications
Level 6	Cycle 1	Bachelor's Degree
Level 7	Cycle 2	Master's Degree
Level 8	Cycle 3	Licentiate and Doctoral Degrees

[1] Slight generalisation made by the authors and not an all encompassing list

The aforementioned frameworks create a reference point in the European Union that is used to prepare, compare and finally publish National Qualification Frameworks (NQF). One example of this would be the Finnish National Qualifications Framework (The Finnish National Agency for Education and Ministry of Education and Culture, 2018).

European Credit Transfer and Accumulation System (ECTS) is a generally agreed specification (European Comission, 2022) of student workload required to reach defined learning outcomes. It promises to make studies and courses more translucent for student mobility and exchange between degree programmes, which contributes to an increase in student exchanges between the member states of the European Union.

The ECTS Users' Guide (European Commission, 2017) is a tool for education organisations for having clear guidelines on how to use ECTS in their degree programmes. In our research the supporting documentation as referred to in the handbook is examined more in detail, especially the course catalogue.

The ECTS Users' Guide encourages all universities to publish up-to-date course catalogues of their degree programmes to enhance student mobility and give visibility to the educational structures. The guide gives free decision upon the format of the course catalogue, however our study concentrates on gathering and normalising this course catalogue data from all Finnish universities to gain a more in-depth view of the current state of cybersecurity education.

Concerning the templates of the course catalogues, as advised in the ECTS Guide, the most important fields of this research were:

- **Information on programmes:** Length of programme, number of credits, level of qualification according to the NQF and EQF
- **Information on individual educational components:** number of ECTS credits allocated, title, type (compulsory/optional[3])

Finnish Education has been regarded as a success by international estimates e.g. Organisation for Economic Co-operation and Development - Programme for International Student Assessment (OECD PISA). The reasons for Finland's success are being analysed up to this day by e.g. Välijärvi et al. (2002) and Simola et al. (2017). It is a subject that has facinated researchers of other countries aspiring towards the same phenomenon e.g. Üstün and Eryilmaz (2018) and Altaf, Shehzad, and Akhtar (2020). Finnish higher education has two placements in the top 250 university lists[4] at the time of writing this paper, however still the higher education perceived to be of high quality based on the forementioned Finnish education reputation alone.

The following figure 1 presents the complete diagram of the education system in Finland as published by the Ministry of Education and Culture of Finland[5] highlighting the focus of this research paper.

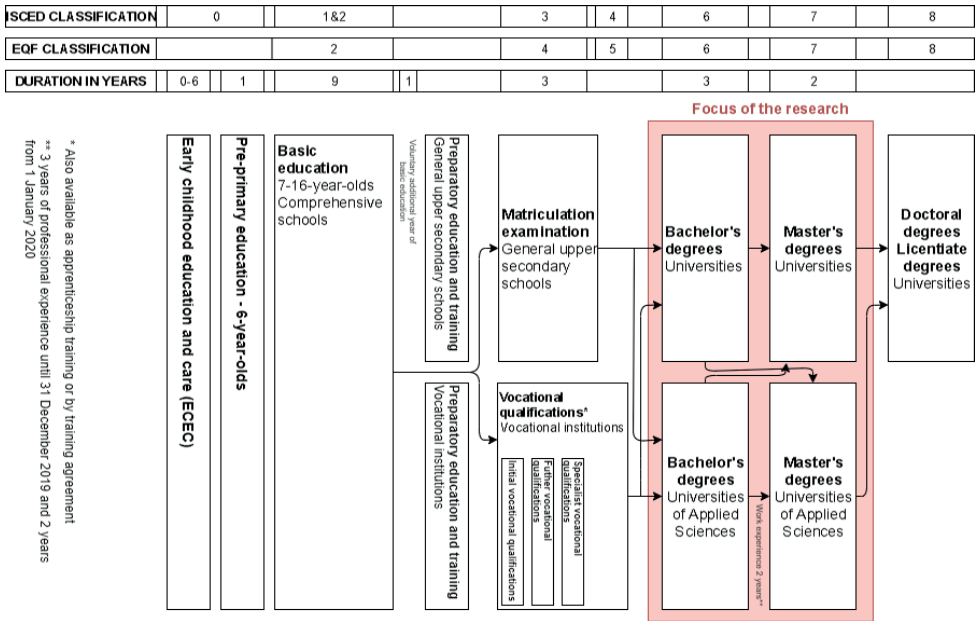


Figure 1: The Finnish Education System and this research context

As illustrated in Figure 1, the universities in Finland are divided into two categories: *Universities* and *Universities of Applied Sciences*. Both have their own guiding Acts[6][7] in the Finnish Law giving statements on their mission, autonomy and their responsibilities in education and research. Given the above, the higher education sector in Finland consists of 13 Universities and 23 Universities of Applied Sciences as stated by the Ministry of Education in Finland. The Universities are listed in the Table 2.

[3]The terms Core, Specialty and Elective are used throughout the paper in synonym to ECTS Guide terminology
[4]https://www.timeshighereducation.com/
[5]https://minedu.fi/en/education-system
[6]https://www.finlex.fi/fi/laki/kaannokset/2009/en20090558.pdf
[7]https://finlex.fi/fi/laki/kaannokset/2014/en20140932_20160563.pdf

Table 2: List of Universities in Finland

Universities	Universities of Applied Sciences
Aalto University	Arcada University of Applied Sciences
University of Helsinki	Centria University of Applied Sciences
University of Eastern Finland	Diaconia University of Applied Sciences
University of Jyväskylä	Haaga-Helia University of Applied Sciences
University of Lapland	Humak University of Applied Sciences
LUT University	Häme University of Applied Sciences
University of Oulu	JAMK University of Applied Sciences
Hanken School of Economics	South-Eastern Finland University of Applied Sciences
University of the Arts Helsinki	Kajaani University of Applied Sciences
Tampere University	Karelia University of Applied Sciences
University of Turku	LAB University of Applied Sciences
University of Vaasa	Lapland University of Applied Sciences
Åbo Akademi University	Laurea University of Applied Sciences
National Defence University	Metropolia University of Applied Sciences
	Oulu University of Applied Sciences
	Satakunta University of Applied Sciences
	Savonia University of Applied Sciences
	Seinäjoki University of Applied Sciences
	Tampere University of Applied Sciences
	Turku University of Applied Sciences
	Vaasa University of Applied Sciences
	Novia University of Applied Sciences
	Åland University of Applied Sciences
	Police University College

This research does not include universities that are purely dedicated to social work, arts or business. These universities are listed as follows: *Diaconia University of Applied Sciences*, *Humak University of Applied Sciences*, *Hanken School of Economics* and *University of the Arts Helsinki*.

3 Cybersecurity Frameworks

Cybersecurity field has developed in the past few years actively by different frameworks. The frameworks have different perspectives and contexts of the industry as described by Azmi, Tibben, and Win (2018). The frameworks of interest in this paper are describing the assets of people working within the field. This gives a good comparison point for educators on how to construct their courses and finally degrees to fulfil different work roles in the framework. Saharinen, Karjalainen, and Kokkonen (2019) describe on how these frameworks could be utilised to design cybersecurity curricula.

3.1 Workforce Framework for Cybersecurity in the United States

One example of a framework is the Workforce Framework for Cybersecurity (or NICE Framework) which was first published in 2017 by Newhouse et al. (2017) and updated in 2020 by Petersen et al. (2020). The framework was developed throughout a decade of development[8] and research accompanying it such as Jones, Namin, and Armstrong (2018) and Armstrong et al. (2020).

The framework consists of Categories under which cybersecurity Specialty Areas reside, which are then occupied by different Work Roles. These categories are useful for sectioning the cybersecurity workforce; however, they were deprecated in the first revision of the framework to improve agility of the framework. The authors of this article feel it is a step backwards, thus in this research paper, the categorisation is still utilised. Same is evident on different websites provided to enhance the usage of the NICE framework[9].

3.2 European Cybersecurity Skills Framework

In addition, European Union has several cybersecurity research and development projects such as Cyber Security Network of Competence Centres for Europe (CyberSec4Europe)[10], Cyber Security Competence for Research and Innovation (CONCORDIA)[11] and Strategic Programs for Advanced Research and Technology in Europe (SPARTA)[12] which in some work packages dedicated to the subject of cybersecurity skills and certification. SPARTA in particular published a deliverable of the project called Cybersecurity skills framework written by Hajný et al. (2020). The deliverable has a section describing preliminary work of the NICE framework (without revision 1 changes) and other approaches such as Nai Fovino et al. (2018) which resulted in A Proposal for a European Cybersecurity Taxonomy Nai Fovino et al. (2019). SPARTA utilised these frameworks to map the preliminary European Cybersecurity Skills Framework, but state in their conclusion that an exhaustive list is still left to be completed (see Hajný et al., 2020, p. 61). SPARTA's work resulted into an ad-hoc workgroup being established in 2020 under The European Union Agency for Cybersecurity (ENISA) and starting work in 2021.

With the framework field in active development the authors decided to use the categorisation of the NICE framework for this research, which can be further down the line merged with the upcoming European Cybersecurity

[8]https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/history
[9]https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework
[10]https://cybersec4europe.eu/
[11]https://www.concordia-h2020.eu/
[12]https://www.sparta.eu/

Skills Framework, assuming the basis of its creation stays the same. These seven workforce categories that are described in Table 3.

Table 3: NICE framework Categories (Newhouse et al., 2017)

Workforce category	**Description**
Securely Provision (SP)	Conceptualizes, designs, procures and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyses, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information.

4 Data gathering, normalisation and analysis methodology

To quantitatively approach the situation within the population group (degree programmes) of the study, the authors faced the problem of gathering the most up-to-date curricula present on the websites of Finnish Universities. As stated earlier in Section 2 in the ECTS Users' Guide, the publishing method varied significantly as for how the education organisations offer the curricula data publicly. In Finland, the data could be stored and published in a web-system like Peppi[13] or plainly just PDF- linked[14] to the public website of the higher education organisation.

This process is presented in Figure 2.

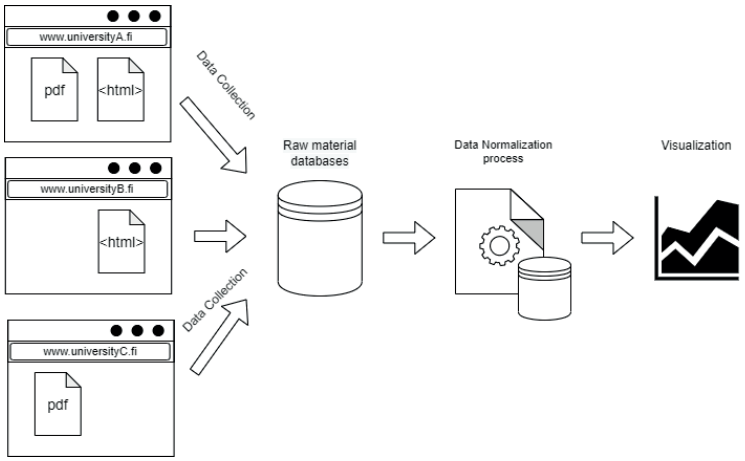


Figure 2: Research flowchart

The sampled course catalogues in this research were published between 2018 to 2020, and typically related to the field of ICT. The two year variation was caused by each educating organisation having their own cycle for updating the curricula; thus, the latest version of the curricula was used for each organisation and degree. The total amount of the degree programmes collected is presented in Table 5 and the variation of degrees descibed in Table 4.

[13]https://opetussuunnitelmat.peppi.jamk.fi/en/49/en
[14]https://www.jyu.fi/ops/fi/it/tietotekniikan-kandidaattiohjelma

Table 4: List of different Degrees/qualifications in data collection

University	Qualification, English	Qualification, Finnish	ECTS
Applied Sciences	Bachelor of Business Administration	Tradenomi (AMK)	210 cr
Applied Sciences	Master of Business Administration	Tradenomi (YAMK)	90 cr
Applied Sciences	Bachelor of Engineering	Insinööri (AMK)	240 cr
Applied Sciences	Master of Engineering	Insinööri (YAMK)	60 cr
Applied Sciences	Bachelor of Police Services	Poliisi (AMK)	180 cr
Applied Sciences	Master of Police Services	Poliisi (YAMK)	120 cr
University	Bachelor of Engineering	Tekniikan Kandidaatti	180 cr
University	Bachelor of Science	Luonnontieteiden Kandidaatti	180 cr
University	Master of Engineering	Diplomi-Insinööri	120 cr
University	Master of Science	Luonnontieteiden Maisteri	120 cr
University	Bachelor of Military Sciences	Sotatieteiden Kanditaatti	120 cr
Universtiy	Master of Military Sciences	Sotatieteiden Maisteri	180 cr

The observation sets (based on university type/degree level) provided a very wide spread of different degree programmes. To get an perspective on the different credit lenghts, levels and organisations within the research, the total amounts of sampled degree programmes are presented in Table 5.

Table 5: Amount of sampled degree programmes

Degree programmes	60 cr	90 cr	120 cr	180 cr	210 cr	240 cr
University of Applied Sciences, Bachelor's degree	-	-	-	1	19	27
University of Applied Sciences, Master's degree	13	11	1	-	-	-
University, Bachelor's degree	-	-	-	23	-	-
University, Master's degree	-	-	37	-	-	-

4.1 Source data reliability

Authors have collected the material, with as minimal change as possible, from the different University publishing systems. Authors trust that the material collected from these sources, are authentic, reliable and follow the guidelines and frameworks described earlier.

4.2 Data cleaning and normalisation

To be able to reliable use data and to minimize the imperfections, following procedures were used.

The data was cleaned by removing unnecessary information from the curricula data, this included course and module descriptions, and possible extra information not required in this analysis. Normalisation, to research relevant data variables, was done by dividing course name, descriptions, ECTS credit numbers and course-code to individual columns. If a specific course had a ECTS credits declared as an range, for example, from one to five credits, the number was rounded upwards. If the curricula included multiple mandatory language courses, e.g. for students with Swedish or Finnish as mother tongue, only Finnish was left to ensure that the number of ECTS credits from mandatory courses stays under the required total number of credits of the degree programme.

After the normalisation, a field was defined per course to present if the course belongs to Core, Specialty or Elective studies. Core studies are mandatory studies, included in curricula. Specialty studies are studies, that concentrate on specific area, e.g. programming or cybersecurity. If the degree programme includes more than one specialty studies, student typically has to choose one of these specialty studies as their field of expertise. Elective studies are studies that are completely free to choose from the university whole course catalogue. To further improve accuracy of the data, the calculated total number of ECTS-credits from mandatory courses, was compared to the number of credits in degree programme; if the number was higher, the particular curriculum was revised to find anomalies.

To verify that the assumptions were correct the dataset was compared to the originally published curricula. The presentation of the courses and working out which of them are Core, Specialty or Elective can be sometimes quite vague and gives room for interpretation[15].

[15]This should be noted as reliability problem of actual student understanding of the curricula and this interpretation problem is also partly reflected in the reliability of our dataset (Leino and Saharinen, 2021).

4.3 Data variables

Mapping NICE category to course names was one of the main goals of the data normalisation. The mapping was enhanced by a word list derived from all the course names. This word list helped to recognize different derivations and grammatical cases within the course names, including words in singular and plural forms, or in different inflected forms, in English or Finnish language, e.g. network and networks or “verkko” and “verkot”. This word list was then compared to specialty area and work role descriptions of the NICE framework to verify that the assumptions made by the authors were correct. The produced word lists were later merged to be used as attribute hits (in the results chapter).

In categorisation one interpretation point is that in the NICE framework, category descriptions classify workforce in a cyber-related manner, as seen in Oversee and Govern (OV) categorisation: ”Provides leadership, management, direction, or development and advocacy so the organisation may effectively conduct cybersecurity work”. As this study is not specified to concern only cybersecurity related degree programmes, the attributes were defined by more generalised way, for example all leadership and management related courses in curricula, were categorised to Oversee and Govern category regardless of whether they concern specific management types, e.g., business management or human resources management. If a singular course related to more than two NICE categories, it was revised and least suitable categories were removed, so that only two categories were left.

Finally, the courses specifically targeted at cybersecurity were also tagged from the data as ”purely cybersecurity related” courses, i.e., the course name was exactly cybersecurity or somehow related to it e.g., information security, security, hacking, penetration. After adding the forementioned mappings to the data, the full dataset was reviewed to find obvious anomalies; these anomalies would be e.g., categorising courses like Patient Safety (Finnish: Potilasturvallisuus) to cybersecurity. These anomalies were removed from the calculations by deleting the attribute attachment.

The observation sets were analysed by calculating several key frequency values per curriculum. These values included total number of Core, Specialty and Elective studies per curriculum and how those total amounts had NICE category distribution and purely cyber related courses within them. These values (or descriptive statistics) were used to calculate the average values that are presented in the results chapter. Used formulas can be found in the open dataset (Leino and Saharinen, 2021) of the research.

4.4 Visualisation

The data charts were visualised using the following principles: orange colours are used in bachelor’s degree programmes and blue colours are used in master’s degree programmes, to visualize the differences between degree programmes. Rasterisation was used to seperate the Universities of Applied Sciences from the Universities.

5 Results

5.1 Attribute hits within the Curricula

The inspection of the research results starts with looking at the top attributes hitting each NICE category as a total sum number in Figure 3. The development of society is heavily emphasising programming, which is very present in the course catalogues with most hits and categorised in the NICE framework under *Securely Provision*. Following close behind is the attribute words, *Management*, *Analytics*, *Network* and *System*, which are all distribute in the categories under different work roles.

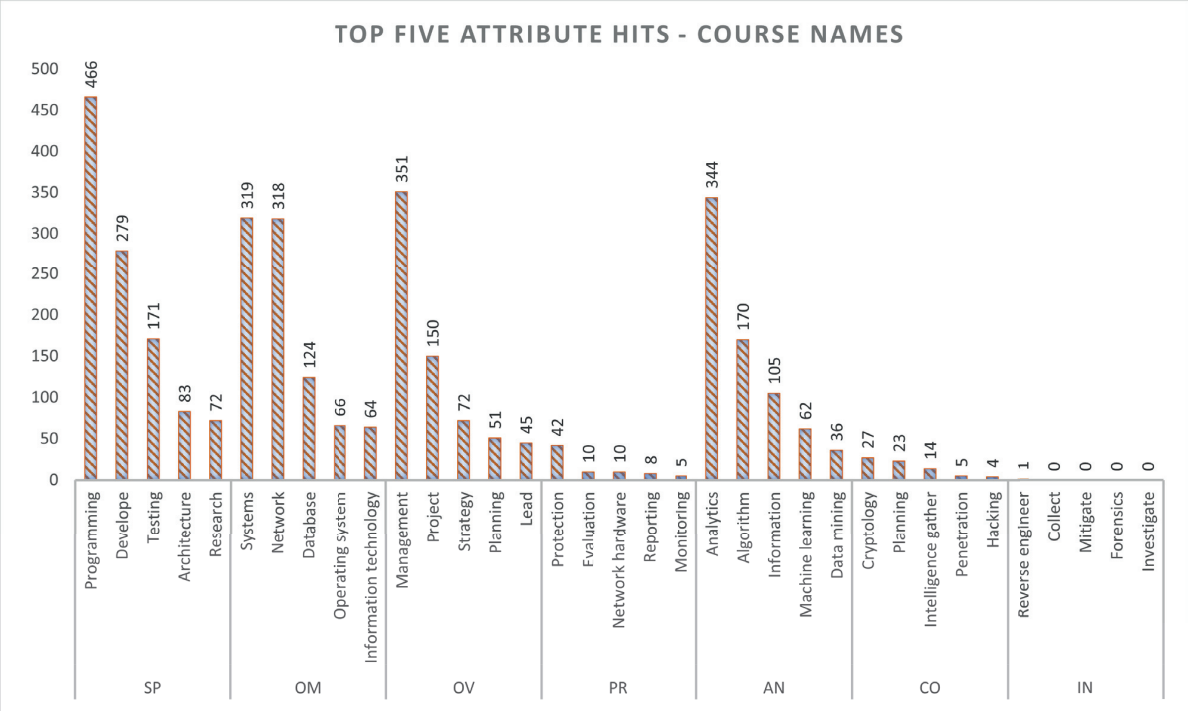


Figure 3: Attribute hits in course names

Later on, it is important to note that the figure 3 does not take into account whether or not the courses are core, speciality or elective studies. They are just present in the course catalogue listings. Looking at this graph, the trend still is that the top five attribute hits amount to the following statistics.

Table 6: Total attribute hits in course names per category

Category	**Total hits**	**Percentage**
Securely Provision (SP)	1071	30.63%
Operate and Maintain (OM)	891	25.48%
Analyze (AN)	717	20.50%
Oversee and Govern (OV)	669	19.13%
Protect and Defend (PR)	75	2.14%
Collect and Operate (CO)	73	2.09%
Investigate (IN)	1	0.03%

The ECTS Users' Guide mandates that the course structure should be modular. In our collections we also analysed the attribute correlation between module names and attributes. This slightly changes the order of the categories as seen in Figure 4, however the same phenomenon is still evident.

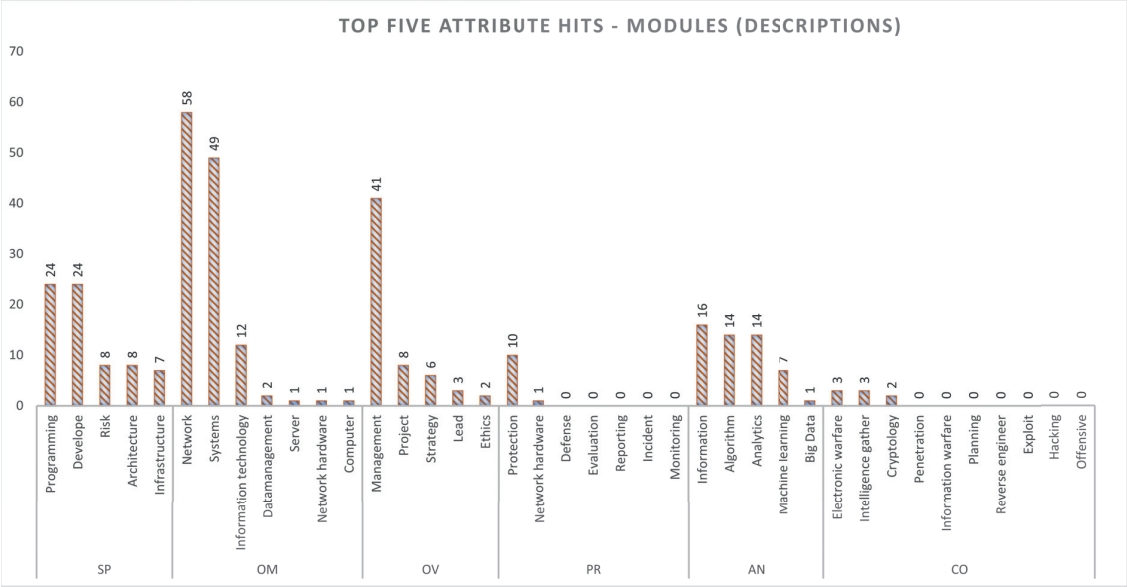


Figure 4: Attribute hits in Modules Descriptions

Top four categories are still the same as in attribute hits with course names. There are just minor placement changes within the percentage weights of modules. *Securely Provision* dropped to second place with *Operate and Maintain* taking the lead.

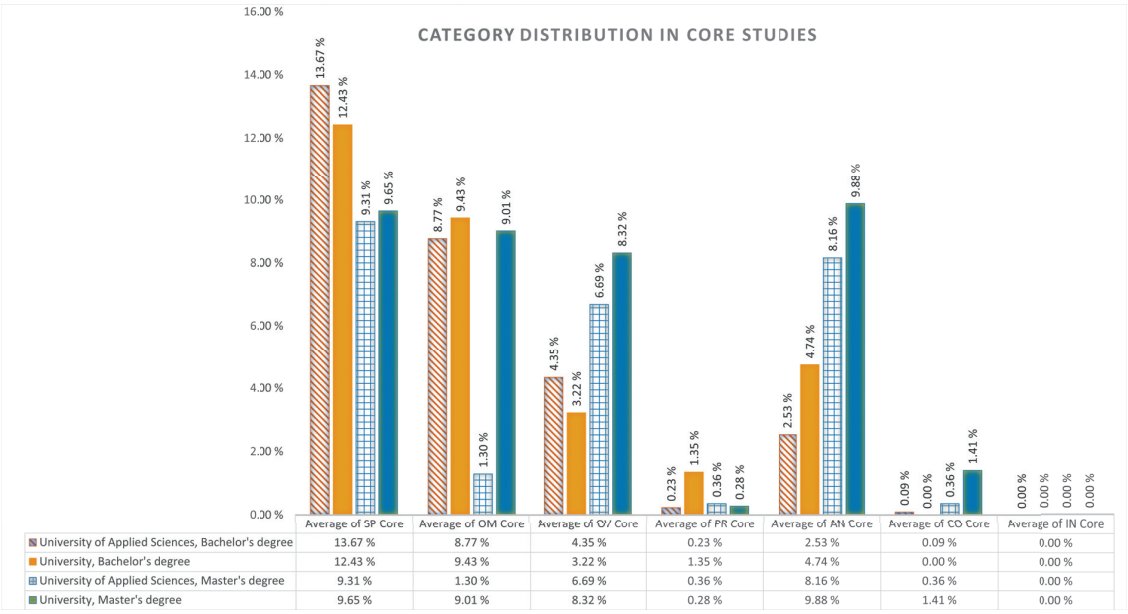
Table 7: Total attribute hits in module names per category

Category	**Total hits**	**Percentage**
Operate and Maintain (OM)	124	38.04%
Securely Provision (SP)	71	21.78%
Oversee and Govern (OV)	60	18.40%
Analyze (AN)	52	15.95%
Protect and Defend (PR)	11	3.37%
Collect and Operate (CO)	8	2.45%
Investigate (IN)	0	0.00%

Oversee and Govern took the third position, which was conluded to be caused by the module names mainly in the Master's Degree programmes. Illustrative is that *Protect and Defend*, with *Collect and Operate* have hits in modules (e.g. Data-analytics), however *Investigate* is completely missing.

5.2 NICE Category Distribution in Core Studies

The forementioned attribute calculations were purely statistical, however the following category distributions were gone through based on the type of studies: Core/Compulsory, Specialty and Elective. These category distributions are first looked from the perspective of Core studies (or compulsory studies). What courses are actually mandatory for completion of a degree programme and where do these mandatory courses align per category and degree programme? This is answered by Figure 5.



	Average of SP Core	Average of OM Core	Average of OV Core	Average of PR Core	Average of MN Core	Average of CO Core	Average of IN Core
University of Applied Sciences, Bachelor's degree	13.67 %	8.77 %	4.35 %	0.23 %	2.53 %	0.09 %	0.00 %
University, Bachelor's degree	12.43 %	9.43 %	3.22 %	1.35 %	4.74 %	0.00 %	0.00 %
University of Applied Sciences, Master's degree	9.31 %	1.30 %	6.69 %	0.36 %	8.16 %	0.36 %	0.00 %
University, Master's degree	9.65 %	9.01 %	8.32 %	0.28 %	9.88 %	1.41 %	0.00 %

Figure 5: Category Distribution in Core Studies

The figure 5 visualises the calculated average percentage of Core studies courses for each NICE category. Without looking at EQF level of the degree programmes, a clear weighting can be seen for *Securely Provision* and *Operate and Maintain* categories. *Oversee and Govern* with *Analyze* following closely behind. Other categories have very small percentages in comparison.

Interesting to see in the figure is that Bachelor's Degrees clearly focus on *Securely Provision* and *Operate and Maintain*, with a minor focus on *Oversee and Govern* and *Analyze*.

Given the percentages this would mean that in the Bachelor's Degrees there are approximately[16].

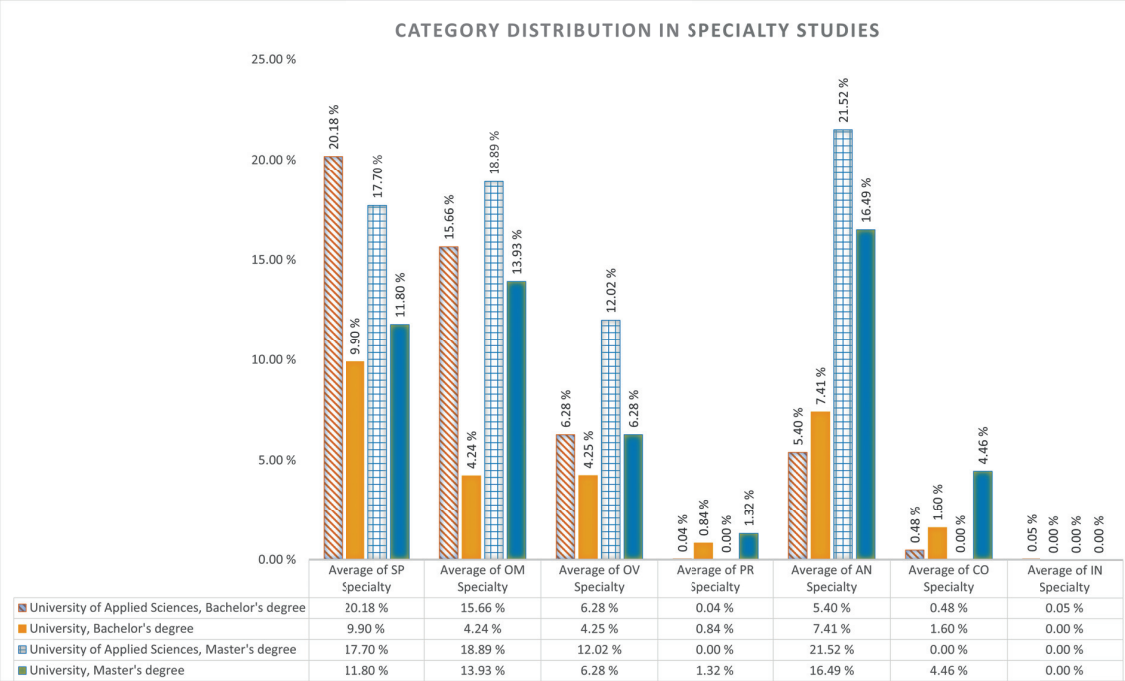
- 10 - 15 ECTS dedicated for *Securely Provision*
- 10 ECTS for *Operate and Maintain*
- five ECTS for *Oversee and Govern*

The core studies in Master's Degrees are more evenly distributed within the categories. It is worth mentioning that the rising status of *Oversee and Govern* and the decline (or total collapse in Universities of Applied Sciences, Master's Degrees) of *Operate and Maintain*, which is to be expected on the level of education in Master's Degree. Typically, the ability to make management level decisions is based on analysing the situation, thus *Analyze* is also emphasised more in the Master's Degree. In comparison, there is small difference variation between Universities of Applied Sciences and the regular Universities in the Core studies of Master's Degrees.

5.3 NICE Category Distribution in Speciality Studies

Speciality studies are typically courses (or whole modules) that the students choose and the variety of categorisation is well represented in the Figure 6.

[16]depends on the length of the bachelor's degree, thus an generalisation/approximated value



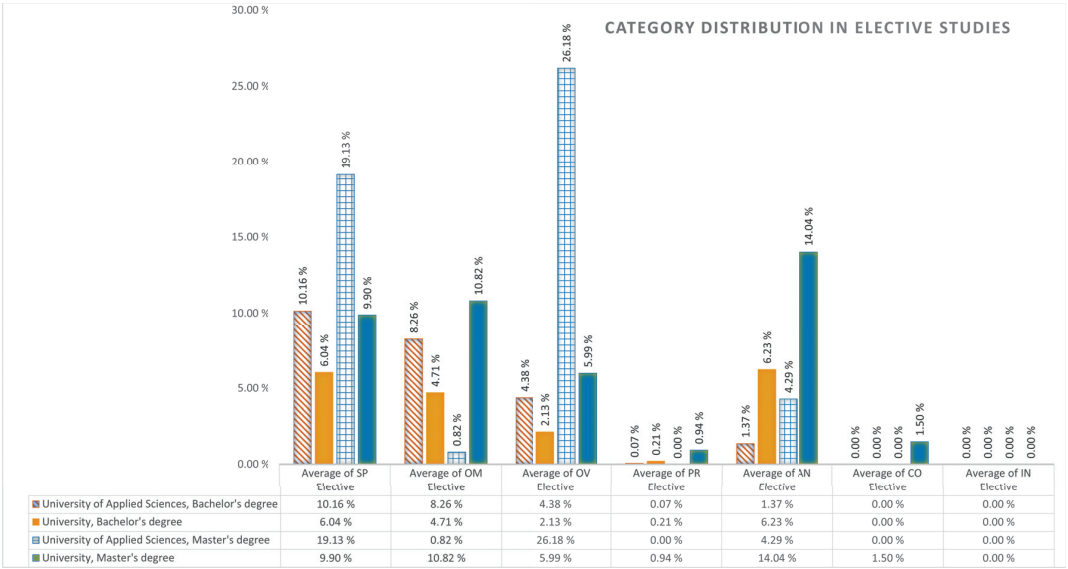
	Average of SP Specialty	Average of OM Specialty	Average of OV Specialty	Average of PR Specialty	Average of AN Specialty	Average of CO Specialty	Average of IN Specialty
University of Applied Sciences, Bachelor's degree	20.18 %	15.66 %	6.28 %	0.04 %	5.40 %	0.48 %	0.05 %
University, Bachelor's degree	9.90 %	4.24 %	4.25 %	0.84 %	7.41 %	1.60 %	0.00 %
University of Applied Sciences, Master's degree	17.70 %	18.89 %	12.02 %	0.00 %	21.52 %	0.00 %	0.00 %
University, Master's degree	11.80 %	13.93 %	6.28 %	1.32 %	16.49 %	4.46 %	0.00 %

Figure 6: Category Distribution in Specialty Studies

Based on our data, it is delighful to note that the students can choose from a variety of studies from varying categories. Althought, the small percentages that are assigned to *Protect and Defend*, *Collect and Operate* and *Investigations* raise a slight hesitation: They were low in the core studies presented in Figure 5, however one would assume they would have had higher percentage in the speciality studies offerings.

5.4 NICE Category Distribution in Elective Studies

The elective studies are just listed on the course catalogues. Even thought the students might be able to choose from all the studies of the University at hand, it still raises the point that published course catalogues typically prefer the courses listed to be chosen[17]. The distribution is visualised in Figure 7.



	Average of SP Elective	Average of OM Elective	Average of OV Elective	Average of PR Elective	Average of AN Elective	Average of CO Elective	Average of IN Elective
University of Applied Sciences, Bachelor's degree	10.16 %	8.26 %	4.38 %	0.07 %	1.37 %	0.00 %	0.00 %
University, Bachelor's degree	6.04 %	4.71 %	2.13 %	0.21 %	6.23 %	0.00 %	0.00 %
University of Applied Sciences, Master's degree	19.13 %	0.82 %	26.18 %	0.00 %	4.29 %	0.00 %	0.00 %
University, Master's degree	9.90 %	10.82 %	5.99 %	0.94 %	14.04 %	1.50 %	0.00 %

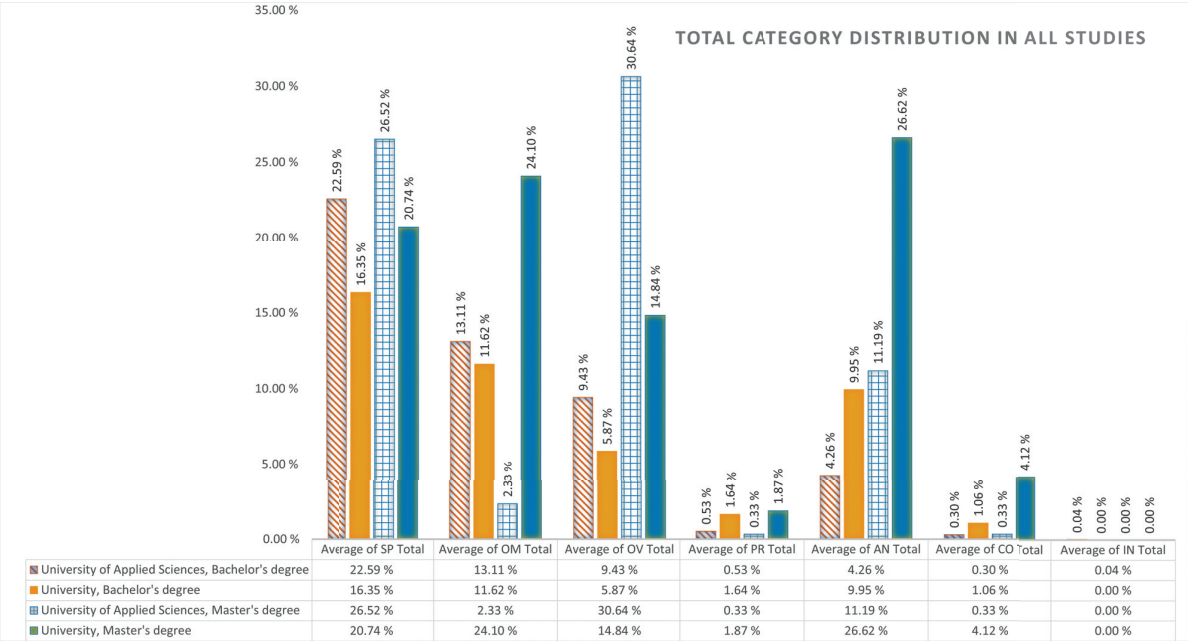
Figure 7: Category Distribution in Elective Studies

[17] XAMK University of Applied Sciences listed all the courses within their offering as elective as seen in https://opinto-opas.xamk.fi/index.php/en/28/en/123044/ITMI21SP/year/2021

In elective studies we can see three categories rising above all others. *Securely Provision* and *Oversee and Govern* categories in Master's Degrees programme in Universities of Applied Sciences. In the Figure 7,we can detect slight problems relating to presentation of the curricula and categorisation of the courses, as elective studies can be basically from the regulation based ten ECTS to a very varied amount of ECTS just listed in the course catalogues. This causes the calculated averages having to be interpreted by the reader as more of an trend rather than actual hard quantitative percentage.

5.5 Total NICE Category Distribution in All Studies

After the dissection of categories within different kinds of studies, we approach the subject of category distribution in all of the different studies a student can go through in the Finnish higher education system. This distribution is illustrated in Figure 8.



	Average of SP Total	Average of OM Total	Average of OV Total	Average of PR Total	Average of AN Total	Average of CO Total	Average of IN Total
University of Applied Sciences, Bachelor's degree	22.59 %	13.11 %	9.43 %	0.53 %	4.26 %	0.30 %	0.04 %
University, Bachelor's degree	16.35 %	11.62 %	5.87 %	1.64 %	9.95 %	1.06 %	0.00 %
University of Applied Sciences, Master's degree	26.52 %	2.33 %	30.64 %	0.33 %	11.19 %	0.33 %	0.00 %
University, Master's degree	20.74 %	24.10 %	14.84 %	1.87 %	26.62 %	4.12 %	0.00 %

Figure 8: Total Category Distribution in All Studies

As for the Bachelor's degrees, the graphs are quite similar between categories. A notable difference is observed in *Analyze*, as the scientific universities being concentrated on research methods, the category is more emphasised to reflect this. This strategic mission of Universities of Applied Sciences then can be seen as an slight advantage in *Securely Provision* and *Operate and Maintain* weightings.

As for the Master's Degrees, the graphs show the same unification, however *Analyze* is even more weighed in the science universities. *Operate and Maintain* is lower in the Master's Degree programmes of Universities of Applied Sciences, however this is mainly because the course selection is wider on the bachelor's degree. *Oversee and Govern* is clearly emphasized high in the Master's Degrees at Universities of Applied Sciences. This might be explained by the two-year work experience requirement (see figure 1) between Bachelor and Master's degrees in the Universities of Applied Sciences track resulting in course election focusing on work coordination on a supervisor/foreman level of the industry. Thus, Management and such attributes hit this category, and this is also reflected in the course categorisation.

5.6 Purely Cybersecurity focused courses in Core Studies

Finally, we come to the courses that are completely focused on cybersecurity. In our data gathering we wanted to visualise to what extent cybersecurity is mandatory for the students of the Finnish higher education system within our research scope. This is illustrated in Figure 9.

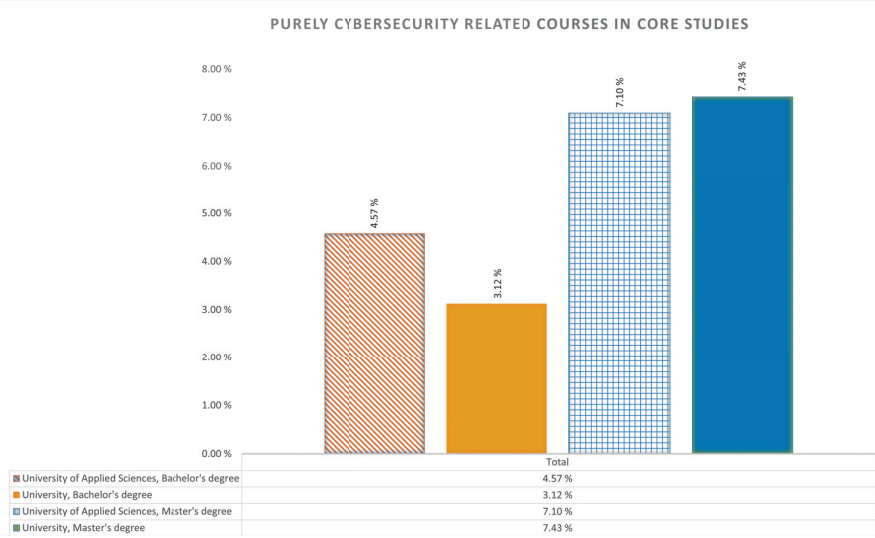


Figure 9: Purely Cybersecurity Related Courses in Core Studies

What is reassuring is that cybersecurity is currently somehow, on average, present in the degree programme structures. It might not be a part of every degree, however as a general weighting within our research scope, one can come to the following conclusion.

In the University of Applied Sciences Bachelor's Degrees education the percentage would result in about three to five ECTS credits being spent on the field of cybersecurity. In the University Bachelor's Degrees the same would be around two to four ECTS credits (as 180 ECTS credits in the degree results in smaller amounts of ECTS credits). As for the Master's Degree education, the percentages are almost similar. Being from 60 ECTS credits to 120 ECTS credits this would result in five to ten ECTS credits purely dedicated for cybersecurity.

6 Conclusions

6.1 Policy Guidance of Cybersecurity Education in Finland

Through the research of different curricula of Finland, even with the chosen delineation. It was quite apparent that cybersecurity clearly structures itself within the field of ICT as a meta-discipline. Thus, the granted study places by the ministry trickle into cybersecurity as seen in the quantitative data. How many actually then choose the field of cybersecurity in specialty or elective studies is information only within the student management software of each higher education institution and in the transcript of records of each individual student.

Around 2015 the degree programmes of Finland were harmonized to follow the ISCED categorization (UNESCO Institute for Statistics, 2015) more precisely. This integrated the very specific curricula into much broader degrees, such as ICT. From the degree data it is quite apparent, that this unification of degree programmes is quite variously interpreted by the Higher Education Institutions of Finland. Some ICT degrees having more specific details after them or even completely removed the mention of ICT altogether in marketing, eventhought the actual degree granted still is Bachelor's Degree in ICT.

The fastest way to enforce cybersecurity workforce through degree oriented education would be to increase the student intake of the pre-existing cybersecurity curricula in Finland such as (in alphabetical order):

- JAMK University of Applied Sciences: Master's Degree in Information Technology, Cyber Security
- Laurea University of Applied Sciences, Business Information Technology, Cyber Security
- South-Eastern University of Applied Sciences: Master's Degree in Cyber Security and Bachelor's Degree in Cyber Security
- Turku University of Applied Sciences: Bachelor's Degree in ICT, Data Networks and Cybersecurity
- University of Jyväskylä: Master's Degree in Cyber Security

Other way would be to encourage the establishment of cybersecurity degree programmes into other universities. This method, however, would contradict the profiling of Universities demanded in the agreements with the Ministry. Based on all the background information and curricula data, it is really vague to draw a clear line from policy guidance on a strategic level to an actual implementation of a degree in cybersecurity.

6.2 Quantitative Research of the Cybersecurity Education in Finland

When analyzing the the gathered curricula data in a systematic way with a cybersecurity framework, it is evident that the cybersecurity education is being offered within the higher education institutions of Finland. Curricula have either courses completely dedicated for cybersecurity and compulsory for participation, or somehow elective and categorizable to a cybersecurity framework. This proven educational capability can be tied into the general aspect of a nations cybersecurity capacity building (Creese et al., 2021; Makridis and Smeets, 2019).

The most important finding is that on average, there are at least some ECTS credits allocated for cybersecurity, in the core/compulsory studies of the degree programmes. This amounts to the result that the authors are not so concerned about what is currently available, but what is missing. The framework categories of *Investigate*, *Protect and Defend* and *Collect and Operate* are seemed to be of very little emphasis based on our data.

Protect and Defend is an important category for handling cybersecurity incidents. This is a day-to-day job within the field of cybersecurity; how to act when an incident has happened. Clearly the higher education does not currently respond to this need currently in their course catalogues, which is even more worrisome as the first topic of Finnish Cyber Security Strategy 2019 has a section of *"protection of the cyber environment without borders"* in its title. Some examples of this category would be the courses such as *Cyber Security Exercise*, which is currently offered in JAMK University of Applied Sciences, and *Cybersecurity Attack and its Defence* in University of Jyväskylä.

Investigate categorisation is a notable feat after an incident has happened. There are very few course offerings for e.g. criminal investigation of cybersecurity related incidents. This aspect of cybersecurity might be neglegted as the responsibility for it is typically left for a governmental authority such as the police. As we looked through the Police University of Applied Sciences, this field was not present in their curriculum, leaving it as a complete blank spot in the education system of Finland.

Finally, we are coming to the *Collect and Operate* category. Data Collection is a part of Cyber Threat Intelligence (CTI) gathering from the cyber domain; something that ENISA is actively campaigning as a research topic in its publishment for research topics in 2021 (European Union Agency for Cybersecurity, 2020). The *Operate* section of the category is a quite offensive cybersecurity section of the NICE framework, in which we find that the higher education system of Finland is not extensively focusing on the offensive capability of the cybersecurity field. It has a few hits in the different curricula such as in cryptology, penetration and hacking attributes of the course names. However, the amounts are minuscule compared to other educated capabilities.

All of the forementioned fields, based on on research, might be in need of an specialty or elective module, which could be a way to differentiate from the crowd.

6.3 Future Research

The course catalogues used in this research were gathered in order to most up-to-date information from the university publishing systems. This does not leave any insight on how this situation has developed over the years since the first Cyber Security Strategy of Finland in 2013 nor can it predict how the different emphases will develope in the upcoming decades. These could be answered by gathering a time series data of course catalogues from the universities. Typically in Finland, the course catalogue goes through major overhauls in three to five years on the Bachelor's Degree and from two to four years on the Master's Degree. This of course depends on the direction the Ministry of Education and Culture is giving the higher education based on its strategy and visions.

With a time series of the course catalogues the trend of cybersecurity education strengthening could be proved. This development could be researched for any subject and field, not just cybersecurity. It would also mandate a more precise developement of national attributes and categorisations, rather than complying to a few, industry segment specific frameworks in particular. The authors feel that the development of e.g. data-analytics education also overlap with the cybersecurity *Analyze* category and would rather complement both. Thus, the trend research of education curricula would respond to the status and development trend of both education fields.

Even though the education course catalogues might give one view of the situation, it is completely a different approach to think of what the students have chosen in their studies. All the Universities publish what they have to offer; however, there is no (public) data on what have the students actually have chosen to be a part of their degree. This leaves a decreased visibility in e.g., speciality studies; even though cybersecurity is offered, it does not mean that any students have actually taken the module or courses.

By looking at the actual course data of graduated students, one could start to draw a dataset of what has actually been produced by the education organisations. This of course is a hard subject to tackle, as often these choices are bound to grades given and are a sensitive matter for each student in question. Strict ethical approach would be required of gatherings of such data.

Be it any hypothesis, research question or dataset; the publishment methods of this data should be improved based on our research experience alone. It is a sad sight to see how the data structures of the curricula are so separate from one another that it is almost impossible to gather data effectively and continuously. Nontheless, all the data

and variables that are based on funding the education are well gathered and continuously visualised in Finland[18], however it does not offer much to the degree/course development and quality improvement of the given education field, what ever it might be.

7 Author contributions statement

K.S. had the research idea/subject and V.L. did the data gathering. K.S. and V.L. analysed the results with K.S. writing the manuscript. V.L. contributed in drawing the tables, visualisations, along with some chapter writing relating to those topics. T.K. contributed for the conseptualisation and writing of text with contributing as the research supervisor and reviewer. T.S. and T.H. reviewed and submitted corrections to the text.

8 Acknowledgments

This work was supported by Jyväskylä University of Applied Science (JAMK) which is participating the Cyber Security Network of Competence Centres for Europe (CyberSec4Europe) project [19] of the Horizon 2020 SU-ICT-03-2018 program. CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929

The authors would like to thank Ms. Tuula Kotikoski for proofreading the manuscript.

References

Altaf, Sobia, Abid Shehzad, and Aneela Akhtar. "Finnish Education System and its Triumph in Pisa: Lessons to Learn for Pakistan". In: *Global Regional Review* V (Mar. 2020), pp. 479–487. DOI: 10.31703/grr.2020(V-I).51.

Armstrong, Miriam E. et al. "Knowledge, Skills, and Abilities for Specialized Curricula in Cyber Defense: Results from Interviews with Cyber Professionals". In: *ACM Trans. Comput. Educ.* 20.4 (Nov. 2020). DOI: 10.1145/3421254. URL: https://doi.org/10.1145/3421254.

Azmi, Riza, William Tibben, and Khin Than Win. "Review of cybersecurity frameworks: context and shared concepts". In: *Journal of Cyber Policy* 3.2 (2018), pp. 258–283. DOI: 10.1080/23738871.2018.1520271. eprint: https://doi.org/10.1080/23738871.2018.1520271. URL: https://doi.org/10.1080/23738871.2018.1520271.

Bologna Working Group. "A Framework for Qualifications of the European Higher Education Area". In: Bologna Working Group Report on Qualifications Frameworks (Copenhagen, Danish Ministry of Science, Technology and Innovation), 2005.

Catota, Frankie E, M Granger Morgan, and Douglas C Sicker. "Cybersecurity education in a developing nation: the Ecuadorian environment". In: *Journal of Cybersecurity* 5.1 (Mar. 2019). tyz001. ISSN: 2057-2085. DOI: 10.1093/cybsec/tyz001. eprint: https://academic.oup.com/cybersecurity/article-pdf/5/1/tyz001/28086821/tyz001.pdf. URL: https://doi.org/10.1093/cybsec/tyz001.

Council of the European Union. "Council Recommendation on the European Qualifications Framework for lifelong learning". In: Official Journal of the European Union, 2017. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017H0615(01).

Creese, S. et al. "Cybersecurity capacity-building: cross-national benefits and international divides". In: *Journal of Cyber Policy* 6.2 (2021), pp. 214–235. DOI: 10.1080/23738871.2021.1979617. eprint: https://doi.org/10.1080/23738871.2021.1979617. URL: https://doi.org/10.1080/23738871.2021.1979617.

European Comission. *European Credit Transfer and Accumulation System (ECTS)*. 2022. URL: https://ec.europa.eu/education/resources-and-tools/european-credit-transfer-and-accumulation-system-ects_en (visited on 03/31/2022).

— *The EU's Cybersecurity Strategy for the Digital Decade*. 2020. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (visited on 04/07/2022).

European Commission. *ECTS Users' Guide 2015*. Publications Office, 2017. ISBN: 978-92-79-43559-1. DOI: doi/10.2766/87592.

European Cyber Security Organisation. *POSITION PAPER, Gaps in European Cyber Education and Professional Training*. 2017. URL: https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf.

— *WG5 ANALYSIS, Information and Cyber Security Professional Certification*. 2018. URL: https://ecs-org.eu/documents/publications/60101ad752a50.pdf.

[18] https://vipunen.fi/en-gb/university-education

[19] https://cybersec4europe.eu/about/

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

— "ENISA Threat Landscape 2020 - Research topics". In: European Union Agency for Cybersecurity, 2020. ISBN: 978-92-9204-354-4. DOI: 10.2824/552242. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-research-topics/at_download/fullReport.

Finnish Government. *Programme of Prime Minister Sanna Marin's Government*. en. Dec. 2019. URL: https://julkaisut.valtioneuvosto.fi/handle/10024/161935 (visited on 04/01/2022).

Hajný, Jan et al. *Cybersecurity skills framework*. SPARTA project, 2020.

Jones, Keith S., Akbar Siami Namin, and Miriam E. Armstrong. "The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals". In: *ACM Trans. Comput. Educ.* 18.3 (Aug. 2018). DOI: 10.1145/3152893. URL: https://doi.org/10.1145/3152893.

Lehto, Martti, Jukka Niemelä, and Petri Vähäkainu. *Cybersecurity research and education in Finland 2019*. 2019. URL: https://www.jyu.fi/it/fi/tutkimus/julkaisut/it-julkaisut/kyberalan_koulutus_suomessa_verkkoversio.pdf.

Lehto, Martti et al. *Finland's cyber security: the present state, vision and the actions needed to achieve the vision*. Feb. 2017. URL: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160233/Suomen_kyberturvallisuuden_nykytila%2c__tavoitetila_ja.pdf.

Lehto, Martti et al. "Strategic management of cyber security in Finland". In: Prime Minister's Office, 2018. ISBN: 978-952-287-532-7. URL: https://tietokayttoon.fi/documents/10616/6354562/28-2018-Kyberturvallisuuden+strateginen+johtaminen..pdf/efea3c33-3c74-4cf6-b237-d49b4f10ab83/28-2018-Kyberturvallisuuden+strateginen+johtaminen..pdf (visited on 03/31/2022).

Leino, Vesa and Karo Saharinen. *[dataset]* Open Data set of the research*. 2021. URL: https://gitlab.labranet.jamk.fi/cs4e/analysing-cyber-security-education-in-degree-programmes-of-finnish-universities (visited on 04/08/2021).

Makridis, Christos Andreas and Max Smeets. "Determinants of cyber readiness". In: *Journal of Cyber Policy* 4.1 (2019), pp. 72–89. DOI: 10.1080/23738871.2019.1604781. eprint: https://doi.org/10.1080/23738871.2019.1604781. URL: https://doi.org/10.1080/23738871.2019.1604781.

McHenry, Darragh et al. *Cyber security skills in the UK labour market 2021*. 2021. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1042429/Cyber_skills_in_the_labour_market_report_v6_.pdf (visited on 04/07/2022).

Ministry of Education and Culture. *Ammattikorkeakouluille myönnetyt uudet lisäpaikat vuodelle 2022*. fi. Dec. 2021. URL: https://okm.fi/documents/1410845/4392480/AMK-uudet+lis%C3%A4paikat+2022.pdf/7a9befe4-8019-135c-fbb1-381094f5d67f/AMK-uudet+lis%C3%A4paikat+2022.pdf?t=1639985949325.

— *Korkeakoulujen aloituspaikkoja lisätään vuodelle 2022 noin 2 300:lla - OKM*. fi-FI. Dec. 2021. URL: https://okm.fi/-/korkeakoulujen-aloituspaikkoja-lisataan-vuodelle-2022-noin-2-300-lla (visited on 04/01/2022).

— *Korkeakoulutus ja tutkimus 2030-luvulle; Taustamuistio korkeakoulutuksen ja tutkimuksen 2030 visiotyölle*. fi. Oct. 2017. URL: https://julkaisut.valtioneuvosto.fi/handle/10024/160456 (visited on 04/01/2022).

— *Yliopistoille myönnetyt uudet lisäpaikat vuodelle 2022*. fi. Dec. 2021. URL: https://okm.fi/documents/1410845/4392480/YO-uudet+lis%C3%A4paikat+2022.pdf/99457406-0502-9d05-c081-ad683d6f76d1/YO-uudet+lis%C3%A4paikat+2022.pdf?t=1639985924200.

Nai Fovino, Igor et al. *A Proposal for a European Cybersecurity Taxonomy*. Publications Office of the European Union, 2019. ISBN: 978-92-76-11603-5. DOI: 10.2760/106002.

Nai Fovino, Igor et al. *European Cybersecurity Centres of Expertise Map - Definitions and Taxonomy*. Publications Office of the European Union, 2018. ISBN: 978-92-79-92956-4. DOI: 10.2760/622400.

Newhouse, William et al. *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. National Institute of Standards and Technology, 2017. DOI: https://doi.org/10.6028/NIST.SP.800-181.

Paananen, Rauli. *Cyber Security Development Programme*. fi. June 2021. URL: http://urn.fi/URN:ISBN:978-952-243-599-6 (visited on 03/31/2022).

Parrish, Allen S. et al. "Global perspectives on cybersecurity education for 2030: a case for a meta-discipline". In: *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (2018).

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

Saharinen, Karo, Mika Karjalainen, and Tero Kokkonen. "A Design Model for a Degree Programme in Cyber Security". In: *Proceedings of the 2019 11th International Conference on Education Technology and Computers*. ICETC 2019. Amsterdam, Netherlands: Association for Computing Machinery, 2019, 3–7. ISBN: 9781450372541. DOI: 10.1145/3369255.3369266. URL: https://doi.org/10.1145/3369255.3369266.

Secretariat of the Security Committee. *Finland's Cyber security Strategy, Government Resolution 24.1.2013*. 2013. URL: https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

— *Finland's Cyber security Strategy, Government Resolution 3.10.2019*. 2019. URL: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf.

Simola, Hannu et al. "Dynamics in Education Politics and the Finnish PISA Miracle". English. In: *Oxford Research Encyclopedias: Education*. Ed. by George W. Noblit. United Kingdom: Oxford University Press, May 2017. DOI: 10.1093/acrefore/9780190264093.013.16.

Statistics Finland. *National classification of education 2016*. 2022. URL: https://tilastokeskus.fi/fi/luokitukset/koulutusala/koulutusala_1_20160101/ (visited on 04/01/2022).

Üstün, Ulaş and Ali Eryilmaz. "Analysis of Finnish Education System to question the reasons behind Finnish success in PISA". In: (Dec. 2018).

The Finnish National Agency for Education and Ministry of Education and Culture. *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*. 2018. ISBN: 978-952-13-6496-9. URL: https://www.oph.fi/sites/default/files/documents/report_on_the_referencing_of_the_finnish_national_qualifications_framework.pdf (visited on 03/31/2022).

UNESCO Institute for Statistics. *International Standard Classification of Education: Fields of education and training 2013 (ISCED-F 2013) Detailed field descriptions*. en. UNESCO Institute for Statistics, 2015. ISBN: 978-92-9189-179-5. DOI: 10.15220/978-92-9189-179-5-en. URL: http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-fields-of-education-and-training-2013-detailed-field-descriptions-2015-en.pdf (visited on 04/01/2022).

Välijärvi, Jouni et al. "The Finnish success in PISA—and some reasons behind it". In: (Jan. 2002).

Švábenský, Valdemar, Jan Vykopal, and Pavel Čeleda. "What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences". In: *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*. New York, NY, USA: Association for Computing Machinery, 2020, 2–8. ISBN: 9781450367936. URL: https://doi.org/10.1145/3328778.3366816.

PX

DEVELOPMENT NEEDS IN CYBERSECURITY EDUCATION - FINAL REPORT OF THE PROJECT, CHAPTER 5. CYBERSECURITY EDUCATION IN UNIVERSITIES OF APPLIED SCIENCES. PP. 59-75.

by

Karo Saharinen, Tuomo Sipola and Tero Kokkonen 2022

Informaatioteknologian tiedekunnan julkaisuja, 96/2022.
University ofJyväskylä.

URN: http://urn.fi/URN:ISBN:978-951-39-9469-3

5 Cybersecurity education in universities of applied sciences

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

5.1 Research data

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

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

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

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

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

TABLE 1. Number of degree programmes analysed

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

5.2 Curricula

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

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

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

5.2.1 Analysis

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

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

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

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

5.2.2 Model analysis of UAS master's programmes

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

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

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

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

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

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

5.2.3 Model analysis of UAS bachelor's programmes

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

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

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

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

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

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

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

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

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

TABLE 5. Extent of cybersecurity courses in ECTS credits

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

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

5.3 Implementation of the survey study

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

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

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

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

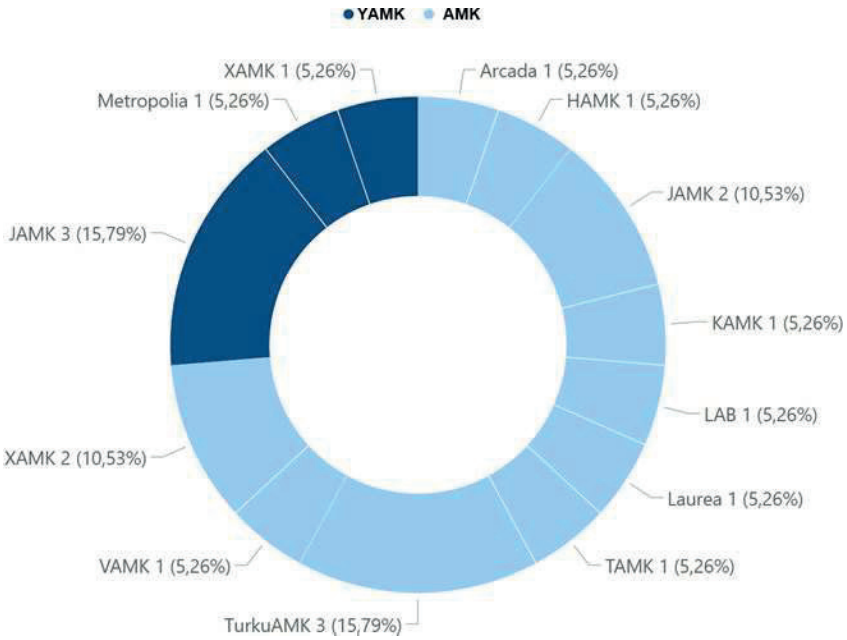


FIGURE 19. Distribution between UAS bachelor's/master's programmes

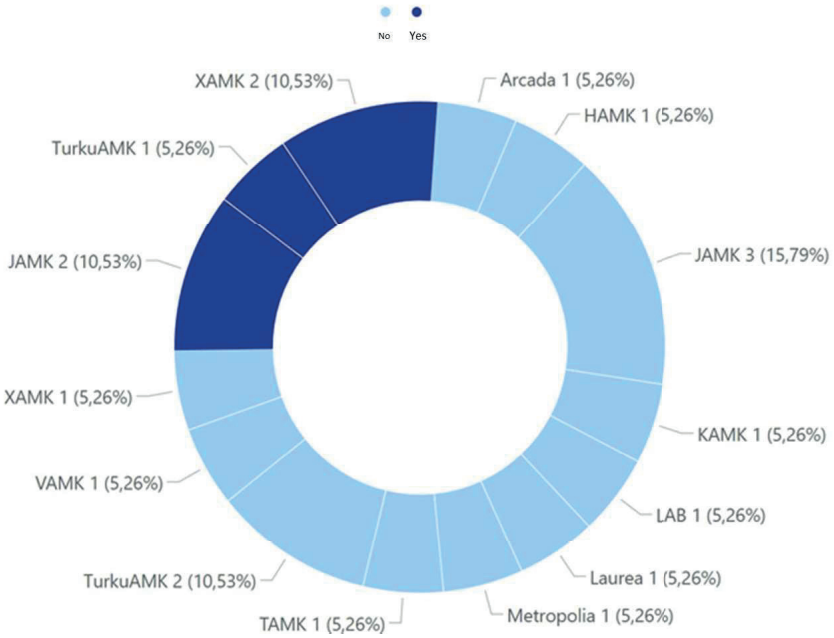


FIGURE 20. Is the degree programme aimed at cybersecurity?

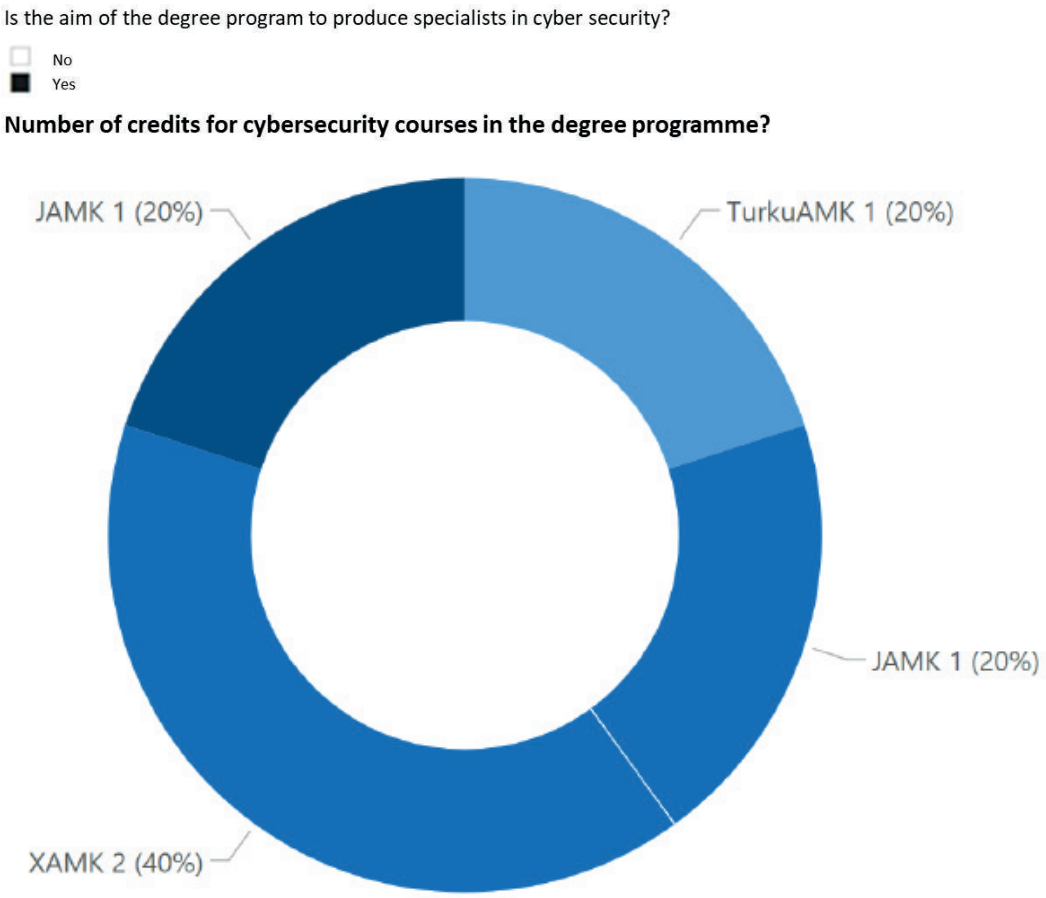


FIGURE 21. Cybersecurity degree programmes

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

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

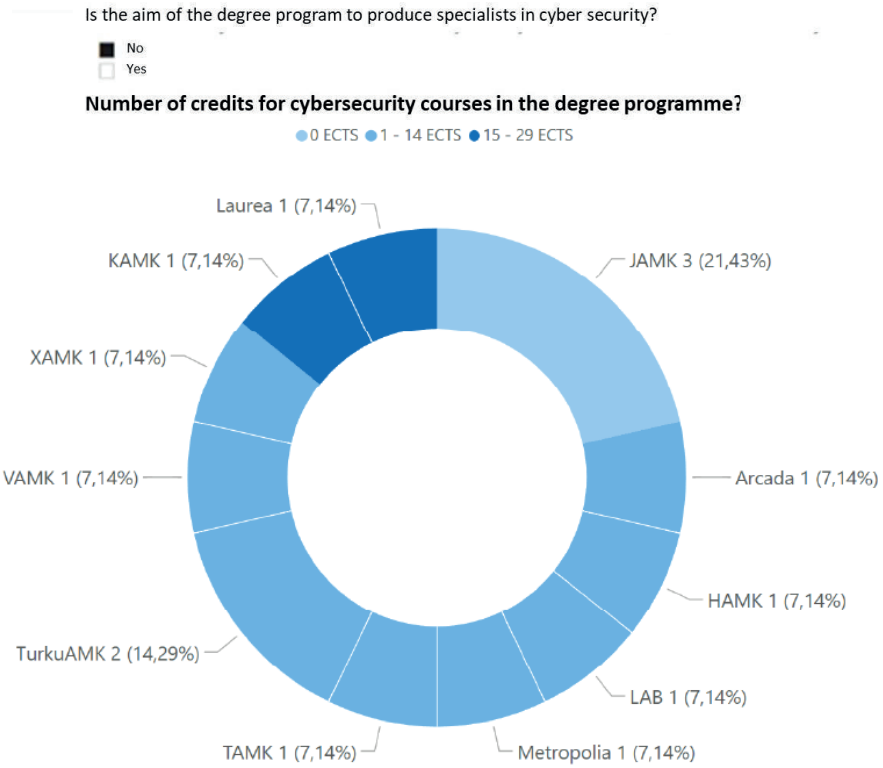


FIGURE 22. Cybersecurity credits in other degree programmes

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

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

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

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

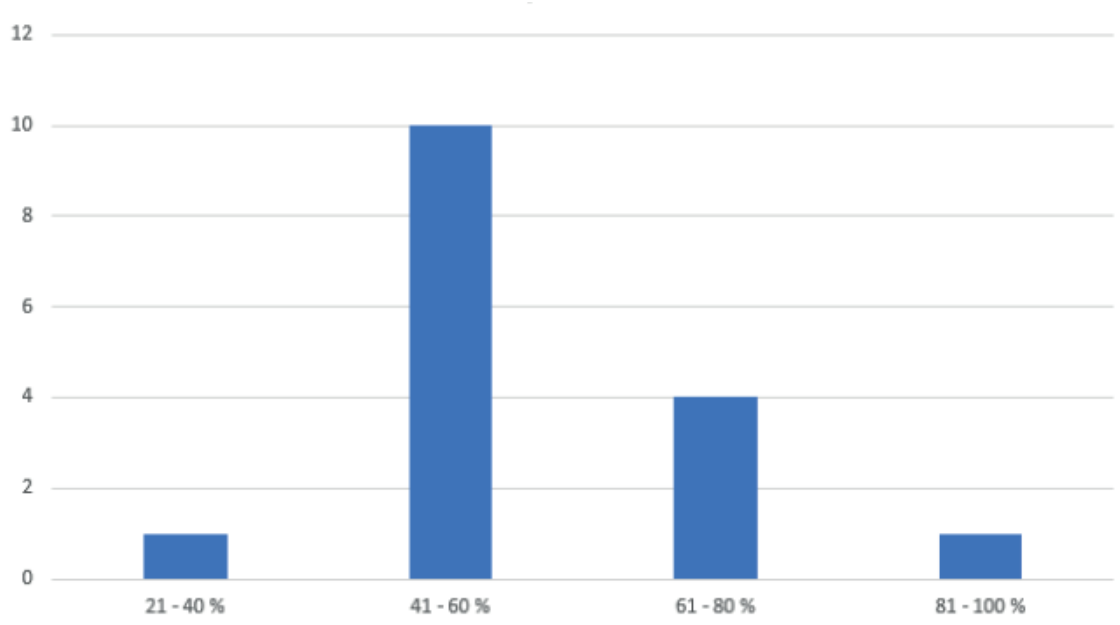


FIGURE 23. Estimated graduation rate

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

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

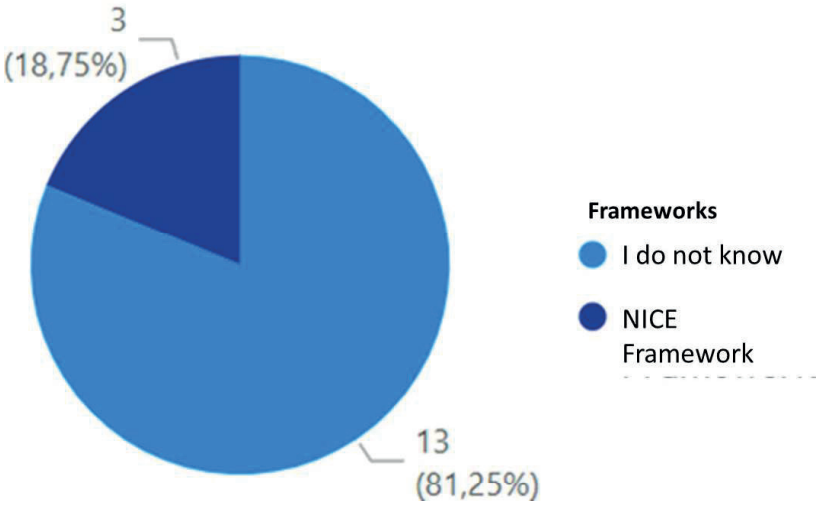


FIGURE 24. Knowledge of frameworks by heads of degree programmes

5.4 Results of the interview study

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

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

TABLE 6. Most frequent topics in the interviews

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

Currently the most significant topics of cybersecurity regarded its management and the cybersecurity of information networks. The actual technical implementation was also seen as a current priority, probably in contrast to administrative aspects. The interviewees mentioned that experts need problem-solving skills in such a way that cybersecurity provides solid background knowledge: offensive and defensive actions, business perspectives and project competence are the desired competence. They also considered it important to teach students about how to operate in a security operations centre (SOC). In the programmes focused on cybersecurity, it was sometimes felt that everything else that needs to be studied may come in the way of building competence in the actual subject matter. For example, orientating towards general management skills might take away from a student's technical competence. Fewer students were estimated to graduate per year than are admitted. Several reasons for this disparity were given. Students seeking a UAS master's degree often pursue their degree while working, which was seen to hinder their studies. However, employment rates among students in the field are high. The interviewees also mentioned a lack of technical skills

among newer applicants and the importance of programming skills. The amount of teaching was seen to have increased, but there were two opinions about the future: on the one hand, teaching was expected to increase, and on the other hand, it was not, in which case the interviewees tended to refer to problems with resources.

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

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

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

5.5 Overall analysis of universities of applied sciences

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

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

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

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

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

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

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

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

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

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

5.6 Conclusions and recommendations

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

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

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

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

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

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

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

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

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

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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