jamk

Analysing Cybersecurity Education in Degree Programmes of Finnish Universities

Thesis

Vesa Leino

Master's thesis
May 2021
Cyber Security
Master of Engineering

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Leino, Vesa

Analysing Cybersecurity Education in Degree Programmes of Finnish Universities

Jyväskylä: JAMK University of Applied Sciences, May 2021, 69 pages

Technology, Information, and communication. Degree programme in Cyber Security. Master's thesis.

Permission for web publication: Yes

Language of publication: English

Abstract

Since 2019, Finland's Cyber Security Strategy has set a goal of strengthening education of cyber and information security, software and application development, information networks and telecommunications. The purpose of this thesis was to analyse Finnish higher education by using a quantitative research method. The scope included bachelor's and master's degree programs from the field of information and communication technology in universities and universities of applied sciences. To be able to analyse the data, the data was harmonized and reflected by using the NICE cybersecurity workforce framework. The reflection revealed workforce categories that are emphasised in the studies and as well proven differences between the bachelor's and master's studies in the universities and the universities of applied sciences. In addition, studies related to purely cybersecurity could be found at certain amount in compulsory studies, which is reassuring. Based on the data, some workforce categories were neglected based by the course offerings. The research did not take account, if these categories could be found within the other courses, as a smaller topic. The results showed that higher education in Finland is providing a sufficient amount of education in the field of cybersecurity - either purely cybersecurity related or as framework related. However, there are some categories in cybersecurity framework that have room for improving and the results of the research help to understand the areas, where education sector could more emphasis on and develop further.

Keywords/tags (subjects)

Cybersecurity, education

Miscellaneous (Confidential information)

This thesis is an extension of the article that has been submitted for publication in Journal of Cybersecurity Published by Oxford University Press (Appendix 1).

jamk

Kuvailulehti

Leino, Vesa

Analysing Cybersecurity Education in Degree Programmes of Finnish Universities

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2021, 69 sivua

Tekniikan ala. Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö YAMK.

Julkaisun kieli: englanti

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Suomen kyberturvallisuusstrategia on vuodesta 2019 asettanut tavoitteeksi kyber- ja tietoturvallisuuden, ohjelmisto- ja sovelluskehityksen sekä tietoverkkoihin ja tietoliikenteeseen liittyvien koulutusohjelmien vahvistamisen. Työn tarkoituksena oli analysoida suomalaista korkeakoulutusta määrällisellä tutkimusmenetelmällä. Kohteiksi valittiin joukko kandidaatin ja maisteritason tutkinto-ohjelmia ammattikorkeakouluista ja yliopistoista. Otanta koostui tietojenkäsittelyn sekä tieto- ja viestintätekniikan tutkinto-ohjelmista vuosilta 2018 ja 2020. Materiaalin muoto yhtenäistettiin paremmin analysoitavaan muotoon ja reflektoitiin käyttäen kyberturvallisuuden työvoimakehystä. Reflektoinnin avulla datasta saatiin selville ne kyberturvallisuuden työvoiman alueet, joihin nykyinen koulutusjärjestelmä tuottaa tekijöitä. Kokonaisuutena tietyt osa-alueet näkyivät hyvin painotettuina tutkinto-ohjelmissa, mutta kuitenkin selkeitä eroavaisuuksia kategorioissa oli havaittavissa kandidaatin ja maisteriopintojen sekä ammattikorkeakoulujen ja yliopistojen välillä. Lisäksi materiaalista analysoitiin puhtaasti kyberturvallisuuteen liittyviä opintoja. Näitä opintoja todettiin sisältyvän sekä pakollisiin että vapaavalintaisiin opintoihin. Huolestuttavinta tuloksissa oli tiettyihin viitekehyksen osa-alueisiin liittyvien opintokurssien vähyys. Kuitenkin nämä viitekehyksen osa-alueet voivat sisältyä olemassa oleviin kursseihin osana kokonaisuutta. Tuloksista voitiin todeta, että kyberturvallisuuteen liittyvää koulutusta on saatavilla riittävästi. Työn tulokset auttavat kehittämään suomalaista korkeakoulutusta erityisesti kyberturvallisuuteen opetukseen liittyvissä asioissa. Kerätyn materiaalin ja tulosten myötä on selvillä, mihin kyberturvallisuuden työvoimaviitekehyksen alueisiin opetus painottuu ja mitkä osa-alueet vaatisivat mahdollisesti lisäpanostuksia.

Avainsanat (asiasanat)

Tietoturva, kyberturvallisuus, koulutus

Muut tiedot (salassa pidettävät liitteet)

Tämä opinnäytetyö on laajennos artikkelista, joka on toimitettu julkaistavaksi Oxford Journal of Cybersecurity -lehdessä (Liite 1).

Contents

Figures

Tables

Terms and Abbreviations

ICT	Information and Communications Technology
ECSO	European Cyber Security Organisation
ECTS	European Credit Transfer and Accumulation System
CR	Credit
FiNQF	Finland's National Qualification Framework
EQF	European Qualification Framework
NQF	National Qualification Framework
QF-EHEA	The Framework for Qualification of the European Higher Education
EQF-LLL	European Qualification Framework for Lifelong Learning of the EU
UN	United Nations
OECD	Organisation for Economic Co-operation and Development
OSCE	Organization for Security and Co-operation in Europe
SPARTA	Strategic programs for advanced research and technology in Europe
NICE	National Initiative for Cybersecurity Education
NCWF	National Cybersecurity Workforce Framework
DEV	Software Development
KSA	Knowledge, Skills and Abilities
AI	Artificial Intelligence
SP	Securely Provision category in NICE Framework
OM	Operate and Maintain category in NICE Framework
OV	Oversee and Govern category in NICE Framework
PR	Protect and Defend category in NICE Framework
AN	Analyse category in NICE Framework
CO	Collect and Operate category in NICE Framework
IN	Investigate category in NICE Framework
ENISA	European Union Agency for Cybersecurity
CTI	Cyber Threat Intelligence

1 Introduction

Given the frequent high profile cybersecurity incidents like data breach and extortion campaign against Psykoterapiakeskus Vastaamo Oy and Vastaamo patients in Finland (Ajankohtaista: Vastaamon tiedotteet ja uutiset, 2021), and the biggest cyber-attack at the time in history, that affected shipping conglomerate A.P. Moller – Maersk globally (Greenberg, 2018), cybersecurity has been brought to public discussion and debate. Given the alarming rate of cybersecurity incidents, the need for cybersecurity capable workforce has exponentially increased in an estimation by Frost & Sullivan (2017). The estimation of global workforce deficit at cybersecurity is 1.8M in 2022 (Frost & Sullivan, 2017). This raises a question, whether the education sector reacts to a rapid development of the cybersecurity sector, especially, by increasing the cyber education in the information and communication technology (ICT) curricula.

Finland's Cyber Security Strategy has demanded since 2013, that basic cybersecurity education should be part of every level in Finnish education (Secretariat of the Security Committee, 2013). This was updated in 2019 to include more specific statement (Secretariat of the Security Committee, 2019):

> *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.*

Few different strategic papers and programs have been written on how to succeed on fulfilling this Cyber Strategy. In a strategy paper by Lehto et al. (2019), it is described a ten-year plan from 2019 to 2029 on how to succeed on the strategy. This is done by focusing on four different key areas: wireless and wired communication networks, software development, cybersecurity and artificial intelligence (ibid.). In turn, a research report *Kyberalan tutkimus ja koulutus Suomessa 2019* by Lehto & Niemelä (2019) has focused on describing on common level, what kind of cybersecurity education there is in the degree programs of universities and universities of applied sciences. That research has not considered, if the education is mandatory or elective. In addition, there is neither publicly available data on how these strategies and programs have succeeded, nor data has been made easily publicly available.

For the previous reasons, there has been seen a need for a research that makes visible, whether the cybersecurity strategy has succeeded or not, and whether the cybersecurity education has been taken care of on an obligatory or on a selective course level. This research paper tries to seek the answers on the previous questions.

2 Research methodology

This thesis is the extension of publication submitted for Oxford Journal of Cybersecurity (Appendix 1) and expands and enhances the theory and analysis laid out in the publication. Data and results included in this thesis are based on the submitted journal publication.

The submitted publication focused on researching cybersecurity education in Finnish higher education, how the education curricula match to strategies defined in Finland's Cyber Security Strategy.

Based on this, the leading research question is as follows:

- How has the Finnish higher education carried out the demands stated in Finland's Cyber Security Strategy?

Additionally, three secondary research question were defined as follows:

- How the Cyber Security Education has been implemented in curricula of different, organizationally independent, and geographically distributed universities of Finland?
- How are the courses distributed by Core/Compulsory, Optional, Elective?
- What is the quantitative percentage of cyber security education within the degree programmes based on ECTS amounts?

To answer these questions, the issue was approached by measuring quantitatively the amount of cybersecurity related studies on course catalogues of Finnish universities. Material includes numerical variable in form of ECTS-credit. Scope was set to be bachelor's and master's degrees in universities and universities of applied sciences. As cybersecurity is considered as a technical field, this research targeted degree programmes related to Information and Communications Technology. Finland's Cyber Security Strategy also emphasizes areas related to these degree programs. These are typically present and taught under organizational units related to technology or business. For analysing the material, statistical data analysis methods were used to compare the differences between the observation sets in material.

Inductive approach was first used, collecting suitable amount of material to be analysed and to find suitable patterns and ways to enhance the material.

2.1 Previous research on the subject

Previous research by Lehto & Niemelä (2019) on the subject has been mainly focusing on if cyber-security courses are present in universities or universities of applied sciences, without acknowledging if the courses are mandatory, elective or specialty studies related to specific degree program. Partly similar research to this thesis is Backlund's (2020) *Examination of contemporary cyber security education*. Backlund (2020) focused on his research on comparing purely cybersecurity related bachelor's and master's degree programs in universities and universities of applied sciences in EU and US, to demands stated by stakeholders. As today, no similar research has been done with a similar scope to this thesis.

3 Theoretical-conceptual starting points

Theoretical foundation is based on Finnish education system and regulations, frameworks, strategies, and guidelines provided by European Union and Finnish authorities to create the theory foundation for the study. As the European Union does not yet have a suitable cybersecurity workforce framework that can be used in this study, instead, a NICE cybersecurity framework was chosen. In this chapter 3, different guidelines and frameworks are presented in more details to explain why NICE framework was chosen as a basis for the quantitative part of this study.

3.1 European Credit Transfer and Accumulation System ECTS

European Credit Transfer and Accumulation System (ECTS) system was created and instituted in 1989. Key concept in ECTS is that it defines the amount of work needed to achieve the defined learning outcomes in Qualification Frameworks. A one ECTS-point requires approx. 25-30 hours of full-time workload, including individual study, seminars, practical work and lectures. Degree programs can include from 60 to 240 ECTS-credits. This leads to workload total of 1500 – 7200 hours per degree program. Nominally, one academic year include 60 ECTS-credits. ECTS also determines needed information on programs and individual education components. In this thesis, it is used following information, required to be presented in degree programs and individual education components. (European Union, 2015.):

- Name of the University
- Name of the degree program, qualification, and EQF/NQF-level
- Total number of ECTS-credit
- Curricula year
- Duration of the degree program, according 60 ECTS-credits per academic year
- Course name and code
- Number of ECTS-credits per course
- Course type (mandatory or optional).

ECTS-guide does not define precisely how this information is presented, and each school are free to choose the presentation format. How the school presents the curricula also differs: it could be web-system like Peppi (JAMK University of Applied Sciences, 2021) or PDF-linked to the website (Maanpuolustuskorkeakoulu, 2021). This leads to a problem in defining the courses – which are mandatory or optional in degree programs.

3.2 European and National Qualification Frameworks

To be able to compare efficiently and reliable qualifications and qualification levels in different nations, there must be a reference point. In this chapter, it is described two European Qualification Frameworks: The Framework for Qualification of the European Higher Education (QF-EHEA) and the European Qualification Framework for Lifelong Learning of the EU (EQF-LLL). These two frameworks create a reference point, to compare each EU-nations National Qualification Frameworks. As this thesis focus on Finnish education system, we use Finnish National Framework for Qualifications (FiNQF). These frameworks are part of the theoretical foundation where the research questions are based and gives a reader ability to understand what the goal in education curricula is, we are studying in this thesis.

3.2.1 European Qualifications frameworks

European Qualification Framework for Lifelong Learning of the EU

In 2006, European commission launched a proposal for the EQF-LLL. Framework works as common neutral reference framework in Europe, that holds eight levels of qualification levels (Level 1 – 8). The framework describes relevant learning outcome in knowledge, skills, and competence in each level. (European Commission, 2008) Requirements in learning outcomes on EQF-level 6 and 7 are described on Table 2 in chapter 3.2.2.

The Framework for Qualification of the European Higher Education

QF-EHEA differs from EQF as it includes four different cycles rather than levels: Short, first, second and third cycle, and is dedicated to higher education. In QF-EHEA, the typical amount of work to achieve the qualification is described in ECTS-credits. This framework also describes relevant learning outcome in knowledge, skills and competences on these cycles (Bologna Working Group on Qualifications Frameworks, 2005.) These cycles are referenced to EQF and FiNQF in Table 1, at chapter 3.2.2. Requirements in learning outcomes on QF-EHEA First and second cycle are described on Table 2 in chapter 3.2.2.

3.2.2 The Finnish National Framework for Qualifications

FiNQF, has eight levels based on required competences, and includes general-, vocational-, and higher education. Framework is referenced to EQF Levels 1 – 8. Level 1 and 3 does not include any education certificate, degree or qualifications in Finnish education system but nonetheless are included in FiNQF. (The Finnish National Agency for Education, the Ministry for Education and Culture, 2018.) In Table 1 it is described the FiNQF relation to EQF and QF-EHEA, with relevant educations degree and qualifications and ECTS-credits amount. In this study we concentrate on FiNQF Level 6 bachelor's and Level 7 master's degree programs further explained in.

Table 1. Education System in Finland

Education, degree, or qualification	FiNQF - level	EQF - level	QF-EHEA	ECTS Credits
Basic education certificate / syllabus	Level 2	Level 2		
General upper secondary education certificate / syllabus Matriculation examination Upper secondary vocational qualifications Further vocational qualifications Basic Examination in Prison Services Fire Fighter Qualification Emergency Response Centre Operator Qualification	Level 4	Level 4		
Specialist vocational qualifications Sub-Officer Qualification (Fire and Rescue Services) Vocational Qualification in Air Traffic Control	Level 5	Level 5		120
Bachelor's degrees (universities of applied sciences) Bachelor's degrees (universities)	Level 6	Level 6	First Cycle	180-240
Master's degrees (universities of applied sciences) Master's degrees (universities)	Level 7	Level 7	Second Cycle	60-120
Universities' and the National Defence University's scientific and artistic postgraduate degrees (licentiate and doctor degrees) the General Staff Officer's Degree Specialist Degree in Veterinary Medicine Specialist training in medicine Specialist training in dentistry	Level 8	Level 8	Third Cycle	Not specified

Relevant learning outcomes needed in knowledge, skills and competences are described in Table 2, information in the figure is quoted from (The Finnish National Agency for Education, the

Ministry for Education and Culture, 2018). Figure includes also learning outcomes needed in EQF and QF-EHEA.

Table 2. Learning outcomes in knowledge, skills and competences level 6 and 7

Level 6	FiNQF	EQF
	•Has a good command of comprehensive and advanced knowledge of his/her field, involving a critical understanding and appraisal of theories, key concepts, methods and principles. •Understands the extent and boundaries of professional functions and/or disciplines. oHas advanced cognitive and practical skills, demonstrating mastery of the issues and the ability to apply knowledge and find creative solutions and applications required in a specialised professional, scientific or artistic field to solve complex or unpredictable problems. •Works independently in expert tasks of the field and in international co-operation or as an entrepreneur. •Manages complex professional activities or projects. •Can make decisions in unpredictable operating environments. In addition to evaluating and developing his/her own competence, he/she takes responsibility for the development of individuals and groups. •Has the ability for lifelong learning. •Considers communal and ethical aspects when dealing with different people in learning and working communities and other groups and networks. •Communicates to a good standard verbally and in writing in his/her mother tongue both to audiences in the field and outside it. •Communicates and interacts in the second national language and is capable of international communication and interaction in his/her field in at least one foreign language.	•Advanced knowledge of a field of work or study, involving a critical understanding of theories and principles •Advanced skills, demonstrating mastery and innovation, required to solve complex and unpredictable problems in a specialised field of work or study •Manage complex technical or professional activities or projects, taking responsibility for decision-making in unpredictable work or study contexts; take responsibility for managing professional development of individuals and groups QF-EHEA •have demonstrated knowledge and understanding in a field of study that builds upon their general secondary education, and is typically at a level that, whilst supported by advanced textbooks, includes some aspects that will be informed by knowledge of the forefront of their field of study •can apply their knowledge and understanding in a manner that indicates a professional approach to their work or vocation, and have competences typically demonstrated through devising and sustaining arguments and solving problems within their field of study •have the ability to gather and interpret relevant data (usually within their field of study) to inform judgments that include reflection on relevant social, scientific or ethical issues •can communicate information, ideas, problems and solutions to both specialist and non-specialist audiences •have developed those learning skills that are necessary for them to continue to undertake further study with a high degree of autonomy
Level 7	FiNQF	EQF
	•Understands comprehensive and highly specialised concepts, methods and knowledge corresponding to the specialised competence in his/her field, which are used as the basis for independent thinking and/or research. •Understands issues that are at the interface between his/her field and different fields and evaluates them and new knowledge critically. •Solves demanding problems, also creatively, in research and/or innovation, which develop new knowledge and procedures and applies and combines knowledge from various fields. •Works independently in demanding expert tasks of the field and in international co-operation or as an entrepreneur. •Manages and develops complex, unpredictable and new strategic approaches. •Manages things and/or people. •Evaluates the activities of individuals and groups. •Accumulates knowledge and practices in his/her field and/or takes responsibility for the development of others. •Has the ability for lifelong learning. •Considers communal and ethical aspects when dealing with different people in learning and working communities and other groups and networks. •Communicates to a good standard verbally and in writing in his/her mother tongue both to audiences in the field and outside it. •Communicates and interacts in the second national language and is capable of demanding international communication and interaction in his/her field in at least one foreign language	•Highly specialised knowledge, some of which is at the forefront of knowledge in a field of work or study, as the basis for original thinking and/or research •Critical awareness of knowledge issues in a field and at the interface between different fields •Specialised problem-solving skills required in research and/or innovation in order to develop new knowledge and procedures and to integrate knowledge from different fields •Manage and transform work or study contexts that are complex, unpredictable and require new strategic approaches; take responsibility for contributing to professional knowledge and practice and/or for reviewing the strategic performance of teams QF-EHEA •have demonstrated knowledge and understanding that is founded upon and extends and/or enhances that typically associated with the first cycle, and that provides a basis or opportunity for originality in developing and/or applying ideas, often within a research context •can apply their knowledge and understanding, and problem solving abilities in new or unfamiliar environments within broader (or multidisciplinary) contexts related to their field of study; •have the ability to integrate knowledge and handle complexity, and formulate judgments with incomplete or limited information, but that include reflecting on social and ethical responsibilities linked to the application of their knowledge and judgments •can communicate their conclusions, and the knowledge and rationale underpinning these, to specialist and non-specialist audiences clearly and unambiguously •have the learning skills to allow them to continue to study in a manner that may be largely self -directed or autonomous

3.3 Finnish education system

As it can be seen in the Figure 2, there are two kinds of universities in Finland: Universities and Universities of Applied Sciences. Both are guided by their own acts, that state mission, goals and responsibilities in research and education. These two kinds of universities differ from each other on several ways. Universities of applied sciences are more dedicated on the applied research, development and innovation, where universities are more dedicated to academic research. Also, the universities of applied sciences are more oriented on providing higher education to professional expert jobs and fulfilling the needs of working life. (Ministry of Education and Culture, 2014; Ministry of Education and Culture, Finland, 2009.)

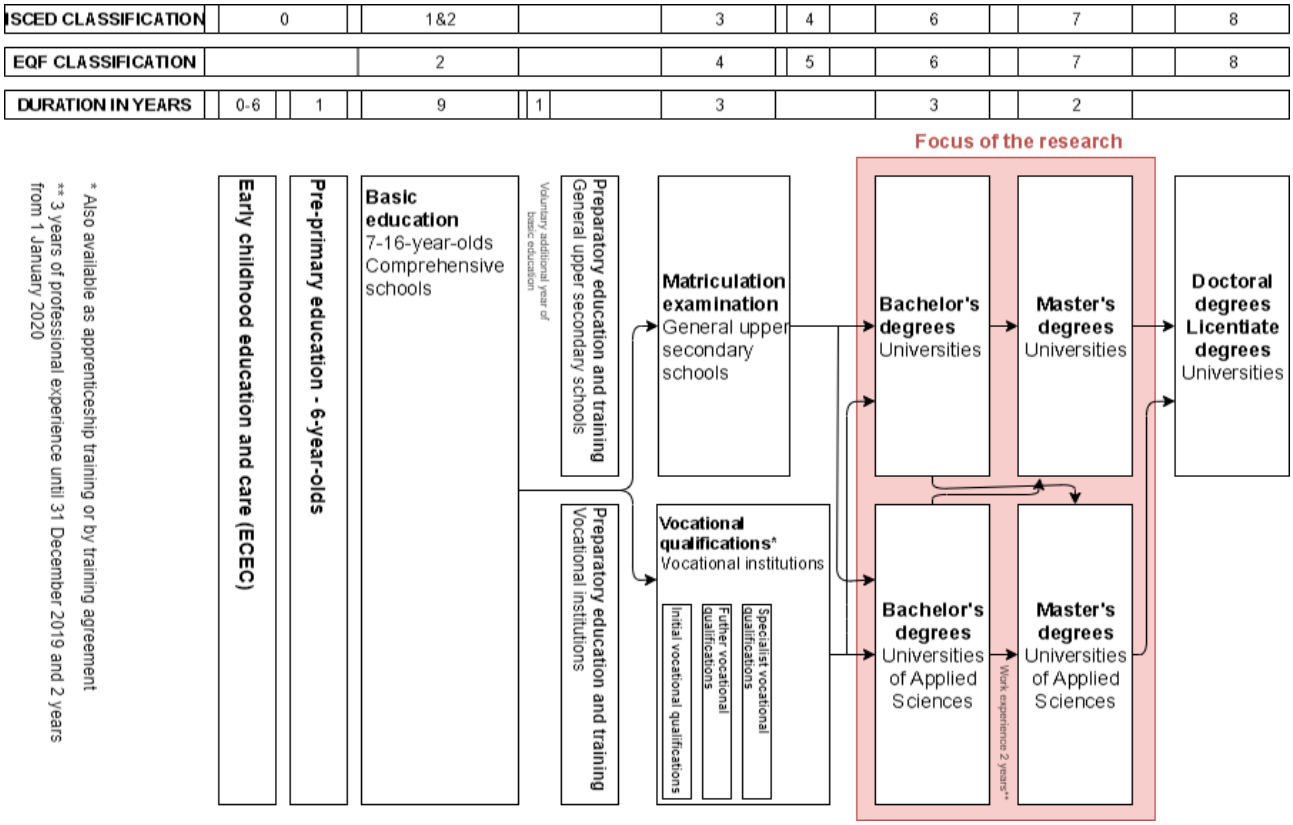

Figure 1. Finnish education system quoted from Saharinen, Leino, & Kokkonen (2021)

3.4 Finland's Cyber Security Strategy

The first revision of Finland's Cyber Security Strategy published in 2013 and in 2019 the strategy was revised. In this study the 2019 version was used. The Finland's Cyber Security Strategy defines

key goals in cybersecurity and it has three major key points (Secretariat of the Security Committee, 2019):

1. DEVELOPMENT OF INTERNATIONAL COOPERATION – protection of the cyber environment without borders.
2. BETTER COORDINATION OF CYBER SECURITY MANAGEMENT, planning and preparedness.
3. DEVELOPMENT OF CYBER SECURITY COMPETENCE – everyday skills and top skills as cyber security safeguards.

The first of the key points focuses on the importance of co-operation between EU- and other Nations, as well with key international organisations like United Nations (UN), Organisation for Economic Co-operation and Development (OECD), Organization for Security and Co-operation in Europe (OSCE). As part of this co-operation, Finland is actively participating in developing EU's Common Foreign and Security Policy on Cyber Security as well EU's Cyber Security Strategy. These policies also affect the cybersecurity at national level. As cyber threats and attacks know no borders, it is imperative to co-operate with other EU-countries when dealing with cyber threats and to response with capable force. (Secretariat of the Security Committee, 2019.)

The second key point emphasises, that to co-operate efficiently, a nation must have an ability and competence to detect and investigate cyber threats, direct businesses and public sector and to have an ability to share the information with other nations. This is also one of the key points in European Union Cyber Security Strategy. (Secretariat of the Security Committee, 2019.)

In the third key point, it is defined the key elements in strengthening national cyber competence. As cybersecurity competence is needed in business and public sector and in all areas of Finnish society, this competence is ensured by a strong education and research in all levels of education. To ensure that the education and research meets these demands, a close co-operation is needed between these entities when creating higher education curricula (Lehto et al., 2019). To full fill these needs, the strategy demands (Secretariat of the Security Committee, 2019): *"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."* Workforce is also enhanced with continuous exercising and training, and with close communication between public-, private- and education sector.

Nevertheless, strong cyber education is needed in providing competence workforce to public administration, when creating a national legislation, developing a cyber secure for comprehensive architecture at national level, and when coordinating and managing the public and private sector (Secretariat of the Security Committee, 2019).

3.5 European Union Cyber Security strategy

In December 2020, European Commission published The EU's Cybersecurity Strategy for the Digital Decade (European Commission, 2020). The strategy defines the key areas to focus on in European Union in the next decade.

Nations' and companies' ability to create safe and reliable communication networks is imperative in the ever digitalizing world. This is even more critical: as during the Covid-19 pandemic, 40% of EU workers switched to telework (Eurofound, 2020), and after the pandemic 82% present of the companies thinking about letting the workforce to partially work remote (Gartner, Inc., 2020). The 5G and future generations of network that are used in communicating and connecting things, require workforce that is capable in designing, creating, and operating these networks in a secure manner.

As cybersecurity knows no borders, it is imperative to co-operate across EU-nations: to develop policies, capabilities and to share information. As part of this co-operation and creating situation awareness in EU-area, EU proposes creating European Cyber Shield, which consists of a network of Cyber Security Operation Centres that works in co-operation with public organizations, private companies and national authorities. (General Secretariat of the Council, 2018.) These Security Operation Centres are a vital part when creating capability to isolate and investigate suspicious events on the communication networks as well as to collect logs. As one can think, also sheer volume of incidents and event occurring in nowadays communication networks, requires machine learning and artificial intelligence (AI) -capabilities to operate efficiently and fast. This leads to a need for competent cybersecurity workforce with an ability to analyse and investigate cyber threats and to create machine learning and AI-capabilities (European Commission, 2020). Nevertheless, the need for competence cybersecurity workforce in these areas, is not limited to these security centres, but also to every nation, public organization or a private company.

In creating cybersecurity capabilities, the ability to defend and protect the key values of European Union: rule of law, fundamental rights, freedom, and democracy, requires workforce, that is capable to create proper measures in defending these values, besides the critical infrastructure, finance, energy, health, security, democratic processes, space, and transportation. (European Commission, 2020.) These areas are also heavily reliant to reliable and secure communication networks. These areas are also important part in Finland's Cyber Security Strategy.

All these areas require policies, standards, processes, and guidelines to operate efficiently and securely. This requires capable professionals who understand the current cyber space and can manage and lead.

3.6 Cyber Security Workforce Frameworks

Cybersecurity field has actively developed frameworks to describe the knowledge, skills and abilities needed for people working on the field.

In European Union, there are few development and research projects ongoing on the field of cybersecurity: Strategic programs for advanced research and technology in Europe – project SPARTA (Sparta, 2021), Cybersecurity competence for research and innovation – project CONCORDIA (Concordia, 2021), Cybersecurity for Europe – project CyberSec4Europe (CyberSec4Europe, 2021) and the European network of Cybersecurity centres and competence Hub for innovation and Operations – project ECHO (Echo, 2021). Each of these projects has some work packages dedicated to cybersecurity skills and education. Further reviewing the published deliveries, SPARTA has published a report D9.1 Cybersecurity skill framework (Hajný, et al., 2020). Report uses NICE framework to preliminary map European Cybersecurity skill framework.

All these projects are on pilot phase and the work related to developing relevant cybersecurity skills frameworks are still in active development. Whereas the first revision of NICE Framework was ready in 2017 (Newhouse, Stephanie, Scribner, & Witte, 2017) and actively developed, NICE Framework was chosen as a theoretical basis of this research paper.

In Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity launched by Joint Task Force on Cybersecurity Education (Joint Task Force On Cybersecurity Education, 2018), it is

quite well presented the challenges of creating cyber education curriculum. As the cybersecurity can be thought as multidisciplinary field, cybersecurity requires a wide range of knowledge from the subfields of IT, for example, software development and networking. These cybersecurity workforce frameworks can be used to develop courses in degree programs, as they usually have relevant knowledge and skills requirements presented. One example, how NICE Framework can be used to design a degree program, can be seen in a research done by Saharinen Karo et al., (Saharinen, Karjalainen, & Kokkonen, 2019).

3.6.1 NICE Cybersecurity Workforce Framework

One cybersecurity related workforce framework is National Cybersecurity Workforce Framework (NCWF) provided by an organization called National Initiative for Cybersecurity Education (NICE). Later referenced as NICE Framework. Its purpose is to work as a tool for organizations, by supplying a vocabulary to describe and categorise cyber workforce. This is done by supplying three different attributes called KSA's abbreviation for words Knowledge, Skills and Attributes. NICE describes these three attributes in a following way: *"Knowledge is a body of information applied directly to the performance of a function. Skill is often defined as an observable competence to perform a learned psychomotor act. Skills in the psychomotor domain describe the ability to physically manipulate a tool or instrument like a hand or a hammer. Skills needed for cybersecurity rely less on physical manipulation of tools and instruments and more on applying tools, frameworks, processes, and controls that have an impact on the cybersecurity posture of an organization or individual. Ability is competence to perform an observable behaviour or a behaviour that results in an observable product.".* (Newhouse et al., 2017.)

NICE contains seven workforce categories that are described in Table 3 (Newhouse et al., 2017). These categories are focused on specific areas in cybersecurity.

Table 3. Workforce categories

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.
Analyse (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

Each of these categories include specialty areas and work roles related to that specific category. For example, Securely Provision (SP) category contains Software Development (DEV) specialty with two defined work roles: Software Developer and Secure Software Assessor. (ibid.). This mapping is shown in Table 4.

Table 4. Specialty and Work role

Workforce Category	Specialty Area	Specialty Area Description	Work role	Work role description
Securely Provision (SP)	Software Development (DEV)	Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.	Software Developer	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
			Secure Software Assessor	Analyses the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.

Different work tasks are described by using five character long “Task id, TXXXX” and description. Description describes specific task for example T0008. “*Analyse and plan for anticipated changes in data capacity requirements.”* (Newhouse et al., 2017).

KSA

KSA is a term defined in the NICE framework. It describes Knowledge, Skills and Abilities that are needed in specific work role. These attributes are presented by using five character long “KSA ID” as follows:

- Knowledge = KXXXX.
- Skill = SXXXX.
- Ability = AXXXX.

Each of the ID includes a brief description as presented in Table 5.

Table 5. Small Part of KSA.s needed in Software Developer work role

KSA ID	KSA
Knowledge	
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0004	Knowledge of cybersecurity and privacy principles.
Skills	
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
S0014	Skill in conducting software debugging.
S0017	Skill in creating and utilizing mathematical or statistical models.
S0019	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.
Abilities	
A0007	Ability to tailor code analysis for application-specific concerns.
A0021	Ability to use and understand complex mathematical concepts (e.g., discrete math).
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.
A0123	Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

Knowledge describes one's knowledge in facts, theories, frameworks, laws, best practices, overall information that is needed. Skills describes one's skill to do specific task. Ability describes one's competence to use knowledge and skill to perform and produce observable results. (Newhouse et al., 2017.)

4 Implementation

4.1 Statistical data analysis method

The thesis includes key terms that are important in statistical data analysis. A population group in this study is information and communication technology degree programs in Finnish higher education. A sample from this population included 132 different degree programs, divided to four different observation sets presented in Table 6. Unit CR in the table means European Credit Transfer and Accumulation System (ECTS) credit.

Table 6. Observation sets

Observation sets	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			

Units in these samples are individual courses included in each degree program. Each unit has different categorial variables: number of ECTS credits allocated, title, type (compulsory/optional), NICE category and a note if the course is cyber related. Observation sets were analysed at first by calculating key frequency percentage values from the variables per degree program. These values included a total amount of core, elective and specialty studies per curricula and how those total amounts had NICE-category distribution, purely cyber related courses within them. An example of Excel-formula used to calculate these key frequency percentage values can be seen in Table 7. And the full list of Excel-formulas can be found in the open data set of the research in Gitlab (Saharinen, Leino, & Kokkonen, 2021).

Table 7. Example of the Excel-formulas used

Securely Provision (SP)-category studies in Core (Mandatory Studies)	= IF(Degree[@Core]>0; SUMIFS(Curricula[Content.Course Ects];Curricula[Content.Studies];"C";Curricula[Content.University];Degree[@[Content.University]];Curricula[Content.Degree program];Degree[@[Content.Degree program]];Curricula[SP];"SP")/Degree[@Core];"")
Where	Degree[@Core] = Amount of Core (mandatory) studies in degree program Curricula[Content.Course Ects] = amount of ECTS-credits awarded from the course Curricula[Content.Studies] = if the course is C = Core, E = Elective, S = Specialty Curricula[Content.University] = Criteria used to find per university degree programs in data Degree[@[Content.University] = Criteria range in table Curricula[Content.Degree program] = Criteria used to find per degree program related courses Degree[@[Content.Degree program]] =Criteria range in table Curricula[SP] = Criteria keyword list used to define the course NICE-category "SP" = Criteria range in table

Mathematical formula for calculating percentage can be seen in formula 1.

$$x = \frac{y}{n} \quad (1)$$

Where x = amount of studies in degree program as percentage

y = total sum of ECTS-credits per variable in degree program

n = total number of ECTS-credit in degree program

These frequency values were used in calculating the arithmetic mean percentage. Arithmetic mean is calculated with formula 2.

$$\bar{x} = \frac{\sum_{i=0}^{n} Xi}{n} \quad (2)$$

Where X = arithmetic mean of values X_1, X_2,…, Xn of variable X

n = degree program in the observation set

These arithmetic mean percentages were used to compare the differences between observation sets (Kallio, Korhonen, & Salo, 2003).

4.2 Data gathering and normalizing

The most up-to-date list of Finnish Universities and Universities of Applied Sciences were collected from the Finnish Ministry of Education website (Ministry of Education and Culture, 2020). Total of thirteen universities and twenty-three universities of applied sciences were first included, and a further examination on the universities' curricula showed, that the universities that are purely concentrated to arts, human-studies or business did not contain any ICT-related degree programs, and for that cause, the previous were removed from this research's scope. From the rest of the universities, curricula were revised to find out ICT-related curricula with an exception on Police Service and Military Science, as these two are key part of the overall security in Finnish society. How the university presents the curricula and the name or specification of the degree program, depends on the university. Qualification is the same in all universities. Curricula were not limited

to purely cybersecurity concentrated. As the Finnish education system includes English and Finnish degree programs, the qualification is presented in the degree programs' format. The full list of qualifications included with relevant English and Finnish terms and ECTS-credits is presented in Table 8.

Table 8. Qualification and ECTS-credits

Finnish	English	ECTS-credit
Tradenomi (AMK)	Bachelor of Business Administration	210
Tradenomi (YAMK)	Master of Business Administration	90
Insinööri (AMK)	Bachelor of Engineering	240
Insinööri (YAMK)	Master of Engineering	60
Tekniikan Kandidaatti	Bachelor of Engineering	180
Luonnontieteiden Kandidaatti	Bachelor of Science	180
Diplomi-Insinööri	Master of Engineering	120
Luonnontieteiden Maisteri	Master of Science	120
Poliisi (AMK)	Bachelor of Police Service	180
Poliisi (YAMK)	Master of Police Service	120
Sotatieteiden Kandidaatti	Bachelor of Military Science	180
Sotatieteiden Maisteri	Master of Military Science	120

The full list of universities included in study is presented in Table 9.

Table 9. Full list of the Universities

University of Applied Sciences	University
Arcada University of Applied Sciences	Aalto University
Centria University of Applied Sciences	University of Helsinki
Haaga-Helia University of Applied Sciences	University of Eastern Finland
Häme University of Applied Sciences	University of Jyväskylä
JAMK University of Applied Sciences	University of Lapland
South-Eastern Finland University of Applied	LUT University
Kajaani University of Applied Sciences	University of Oulu
Karelia University of Applied Sciences	Tampere University
LAB University of Applied Sciences	University of Turku
Lapland University of Applied Sciences	University of Vaasa
Laurea University of Applied Sciences	Åbo Akademi University
Metropolia University of Applied Sciences	National Defence University
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	

Those universities that are dedicated to economics or arts are not included. These include Hanken School on Economics, University of the Arts Helsinki, Diaconia University of Applied Sciences and Humak University of Applied Sciences.

Data normalizing

Detailed process chart of how the data was collected is presented in Figure 2.

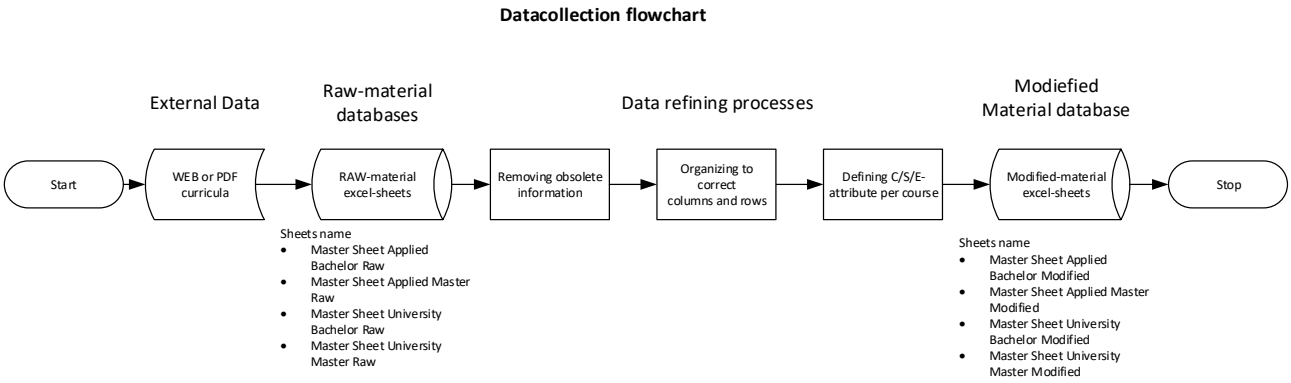

Figure 2. Data collection

To normalize data and to use it in a reliable manner to diminish possible errors, the following methods were used. At first, redundant information like course and module descriptions and possible other irrelevant information not required in the analysis were removed. This cleaned the data into a form, where data normalization was able to be done. The normalization was started by dividing course name, descriptions, ECTS-credits, and course-code into separate columns. Numerical rounding was made upwards, in case, some course had ECTS-credits reported as a range from one to five credits. In such cases, where the curricula comprehended various obligatory language courses for students with Finnish or Swedish as their mother tongue, for example, only Finnish and its credits were included to control a total amount of ECTS' in the degree programmes' obligatory courses. This was done also to secure that the total number of ECTS do not exceed the required number of credits of a degree program.

Modifying the data

To be able to analyse data, the data was modified by adding several fields. The fields added to courses were following:

- Studies - field to inform if course is core (mandatory), elective or specialty.
- Security related - field to inform if course is purely cyber related.
- NICE Category - field to inform course NICE Framework categories.

Letters were used in the studies' field to present whether the course is Core = C, Elective = E or Specialty = S. The core courses are mandatory courses in the curricula. The elective studies are free to choose courses in course catalogue, and the specialty studies are specialisation studies, for example, programming or cybersecurity. Typically, a student chooses one of these specialty studies as their field of expertise. The information, which of the courses are mandatory, elective or specialty studies, is presented in various ways or not at all in curricula. This gives room for interpretation. This should be noted as a reliability problem of an actual student understanding the curricula. This interpretation problem is also partly reflected in the reliability of our dataset. Few measures were made to minimise the error rate in defining the studies field. First, sum of ECTS-credits awarded from the mandatory courses was calculated and compared to the total required amount in a degree program. In case, the sum was larger than required, dataset was revised and compared to the originally published curricula.

Mapping the courses to security related and to NICE categories was done by using keyword lists. These lists were category specific and included words derived from NICE Framework category, specialty and work-role description fields. The lists were further enhanced by a word list derived from all the course names in full dataset, to find the singular and plural forms and different inflected forms present in the course names. An example of the keywords can be seen in Table 10. And the full lists can be seen in the open dataset. These wordlists were later used to calculate the attribute hits in the course names and in the modules.

Table 10. Example of the keywords used in categorization

Group	Attribute	Hits	Category
Ethics	Eettinen	6	OV
Ethics	Eettisyys	1	OV
Ethics	Ethical	1	OV
Ethics	Ethics	10	OV
Ethics	Etiikka	8	OV

As the NICE framework category descriptions classify workforce in a cyber related manner, for example, in Oversee and Govern (OV) category*: "Provides leadership, management, direction, or development and advocacy so the organisation may effectively conduct cybersecurity work"* (Newhouse et al., 2017). As this study is not specified to concern only cybersecurity related degree programs, a certain generalisation was done when defining the course category. For example, management courses included in curricula were defined to OV-category, even if the course concerns a specific management type, for example human resources management. In cases, the course matched to more than two categories, the least suitable categories were removed. Security related field was tagged in case a course can be categorised to purely cybersecurity related, for example course name includes words hacking or information security.

Finally, the full dataset was reviewed to find obvious errors and anomalies. Possible anomalies were for example categorising courses like *Electrical safety course* (Finnish: Sähkötyöturvallisuuskurssi) to cybersecurity. To remove these courses from the analysis, the attribute attachment was deleted.

4.3 Analysis of data

Analysis of the data was done by using the Microsoft Excel's data-analysis tools. Visualisation was done by using the Excel's PivotTable and Chart features. In analysing, arithmetic mean was used when calculating values for several reasons. First, the data does not include considerable amount of variables that are noticeable higher or lower. Second, the data includes variables that are defined by authors subjective view from the material, for examples keywords used in defining the

course NICE-categorization. Third, authors felt that using arithmetic mean, is adequate in this research, as the research is not purely quantitative by nature. This is because, in enhancing the data, the attributes for data categorization had to be chosen in subjective manner. This had also excluded the other statistical calculation methods, like median or standard deviation.

Before the data can be analysed, several key frequency values (or descriptive statistics) were calculated per curricula. These values included the NICE category distribution from the core, elective and specialty studies per curriculum and purely cyber related courses within them. These values were used in calculating the arithmetic mean values presented in the results chapter.

5 Results

Overall, the results present the current emphases in workforce categories in Finnish higher education curricula and reveal possible areas to improve. For the study subscriber, this research presented possible areas to focus on, to stand out from the ever-competing universities of applied science. When using percentage in comparing the amount of studies in NICE-categories, it was concluded that this helps visualizing the differences between observation sets and different NICE-categories, rather than just using the amount of ECTS-credits. However, the amount of ECTS-credits is calculated where applicable to present the approximal amount of work, amount of work per ECTS-credit can be seen in chapter 3.1. Results presented in the next chapters 5.1-5.8 complement the submitted journal publication.

Results are one of a kind in Finnish research with this wide scope of the data. Meaning, all the universities and universities of applied sciences and their curricula were reviewed and analysed whether the degree programmes were able to be used in this research.

5.1 Total amount of studies in observation sets

To further clarify the results presented in the submitted article, the arithmetic mean value from the total amount of core, specialty, and elective studies in ECTS-credits per observation set were analysed. These values were used in calculating the results in categories presented in the submitted journal publication. Results are presented in Figure 3.

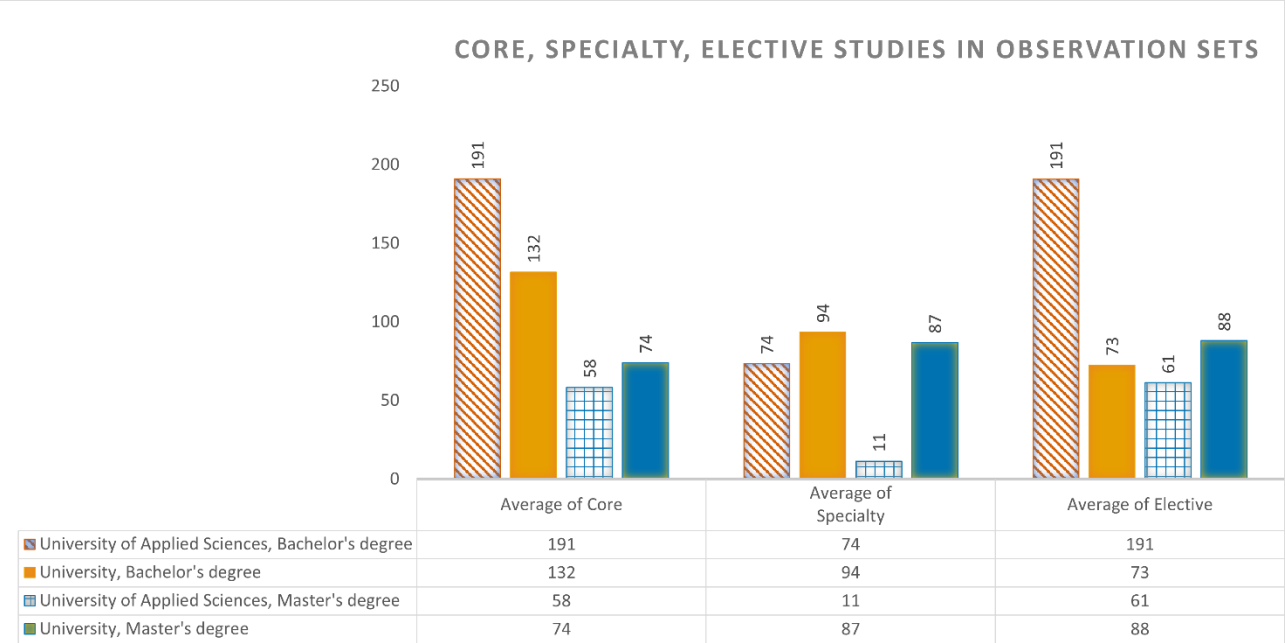

Figure 3. Core, Specialty, and Elective studies in observation sets

5.2 Attribute hits within the Curricula's

First, research results were analysed with looking the top five attributes hitting each NICE category in Figure 4. A full sample set included 8321 individual courses. Each of the attributes total sum number presented in bar chart includes Finnish and English keywords as well different inflected forms. The results did not take into account if an individual course was in Core (Mandatory), Specialty or Elective course and the differences between observation sets.

The following four categories rose above else: Securely provision (SP), Operate and Maintain (OM), Oversee and Govern (OV) and Analyse (AN). A further examination of these four categories revealed five attributes primarily: Programming, Network, Systems, Management and Analytics. Programming, Network and System attributes were expected to be the top attributes, as ICT-education and the degree programs are highly oriented to these areas. The development of the society is heavily emphasizing programming, which explains it to be the highest. One of the interesting thing is that the following three categories had a lower amount of hits: Protect and Defend (PR), Collect and Operate (CO), and Investigate (IN).

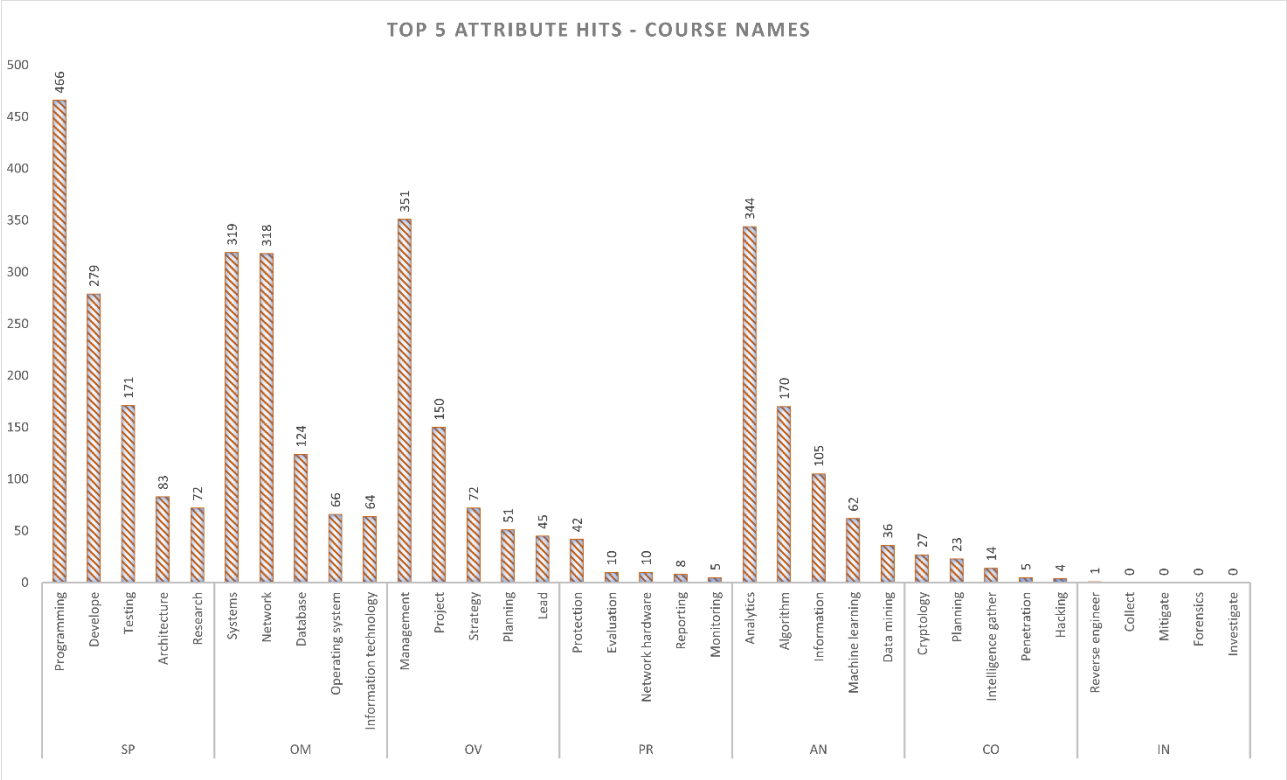

Figure 4. Attribute hits - course names

To get better overall picture of the result, the total amount of hits and percentage is presented in Table 11.

Table 11. Top attribute hits and percentage in course names

Category	Total hits	Percentage
Securely Provision (SP)	1071	30,63 %
Operate and Maintain (OM)	891	25,48 %
Analyse (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 %
	3497	100,00 %

As the ECTS's Guide mandates that the course structure should be modular, the attribute hits in the module names were calculated. In the results, the same phenomenon could still be seen, but

in a slightly changed order, as seen in Figure 5. Each of the attributes' total sum number presented in bar chart were calculated from the individual modules in the full sample set.

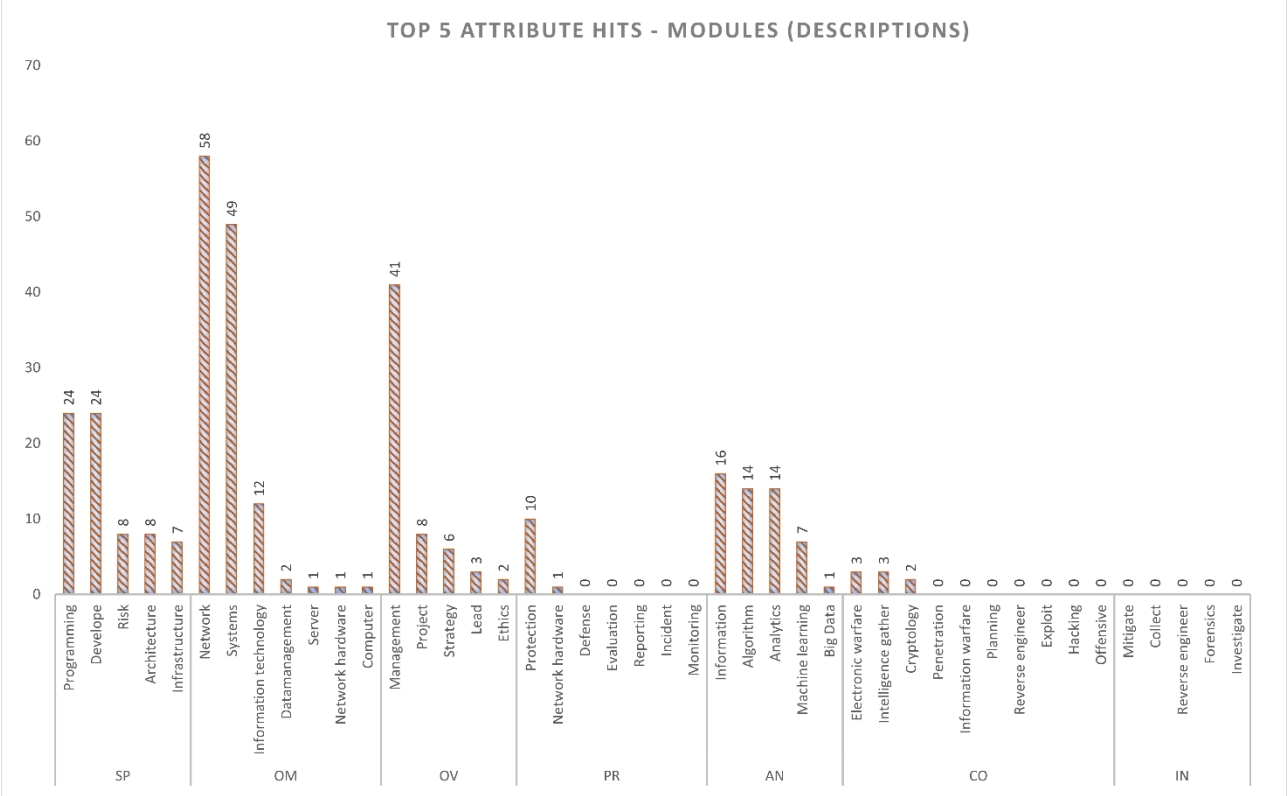

Figure 5. Attribute hits - Modules (descriptions)

In modules, the top four categories switched positions: Operate and Maintain (OM) took the first position and Securely Provision (SP) fell on to the second place, where Oversee and Govern (OV) took the third position and Analyse (AN) fell on to the fourth place. From the results, it can be seen that Protect and Defend (PR) and Collect and Operate (CO) had hits on the course modules but Investigate (IN) had none. To get better overall picture of the result, the total amount of hits and percentage is presented in Table 12.

Table 12. Top attribute hits and percentage in modules

Category	Total hits	Percentage
Operate and Maintain (OM)	124	38,04 %
Securely Provision (SP)	71	21,78 %
Oversee and Govern (OV)	60	18,40 %
Analyse (AN)	52	15,95 %
Protect and Defend (PR)	11	3,37 %
Collect and Operate (CO)	8	2,45 %
Investigate (IN)	0	0,00 %
	326	100,00 %

5.3 NICE Category Distributions in Core studies

The forementioned attribute calculations were purely statistical. However, to find category distribution in Core (Mandatory), Specialty and Elective studies, first, the amount of NICE-category studies in Core-studies was calculated. This was done by calculating the percentage of per degree program category distribution from total of 132 different degree programs. These values were used in calculating arithmetic mean percentage in the observation sets. Used formulas can be seen in chapter 4.1. These results per observation set are presented in Figure 6.

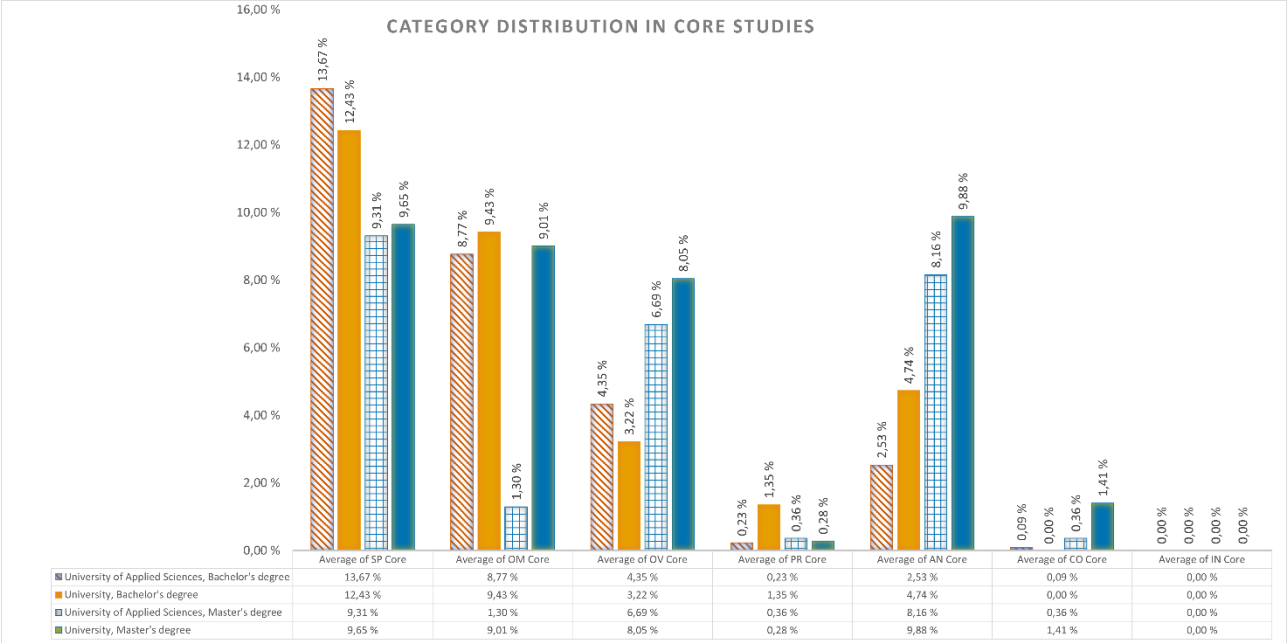

Figure 6. Category Distribution in Core studies

How much the percentage is, it is presented in Figure 6, and the same in ECTS-credits, is presented on Table 13.

Table 13. Category distribution in Core studies in percentage with the amount of ECTS-credits

Category	University of Applied Sciences, Bachelor's degree	ECTS	University, Bachelor's degree	ECTS2	University of Applied Sciences, Master's degree	ECTS3	University, Master's degree	ECTS4
Average of SP Core	13.67 %	26	12.43 %	16	9.31 %	5	9.65 %	7
Average of OM Core	8.77 %	17	9.43 %	12	1.30 %	1	9.01 %	7
Average of OV Core	4.35 %	8	3.22 %	4	6.69 %	4	8.32 %	6
Average of PR Core	0.23 %	0	1.35 %	2	0.36 %	0	0.28 %	0
Average of AN Core	2.53 %	5	4.74 %	6	8.16 %	5	9.88 %	7
Average of CO Core	0.09 %	0	0.00 %	0	0.36 %	0	1.41 %	1
Average of IN Core	0.00 %	0	0.00 %	0	0.00 %	0	0.00 %	0

When reading values, it should be noted that these values were calculated from the values presented in Figure 3. For instance, in total amount of 192 ECTS-credit core studies in the university of

applied sciences, a bachelor's degree set includes 26 ECTS-credits amount of SP-category studies and so forth.

The results showed that there was a clear emphasis on SP and OM categories in the bachelor's level degree programs, in both in the university and in the university of applied sciences. If these results were compared to requirements presented in Table 2, it could be noticed that these categories quite well matched to the requirements in FiNQF level 6. OV and AN were emphasised on the master's level degree programs. If these were compared to requirements in FiNQF level 7 presented in Table 2, these results matched quite well, as typically the master's level included the ability to make management decisions according to analysis.

Notable is that the categories were much more distributed in master's degree programs, especially in the universities. An exception was that OM category in the universities of applied sciences was a notably smaller than in the universities. A one explanation for OM category to be notably smaller, is as master's degree programs in the universities of applied sciences are shorter than universities, typically 60-90 ECTS-credits, are highly focused on some specific area, for example cybersecurity or management. Therefor categories that are emphasized in bachelor's degree could have smaller percentage in master studies.

5.4 NICE Category Distribution in Speciality studies

Specialty studies are courses in curricula that student typically choose as a field of expertise. The variety of categorisation is well represented in Figure 7. The same process in calculating values was used as in core-studies.

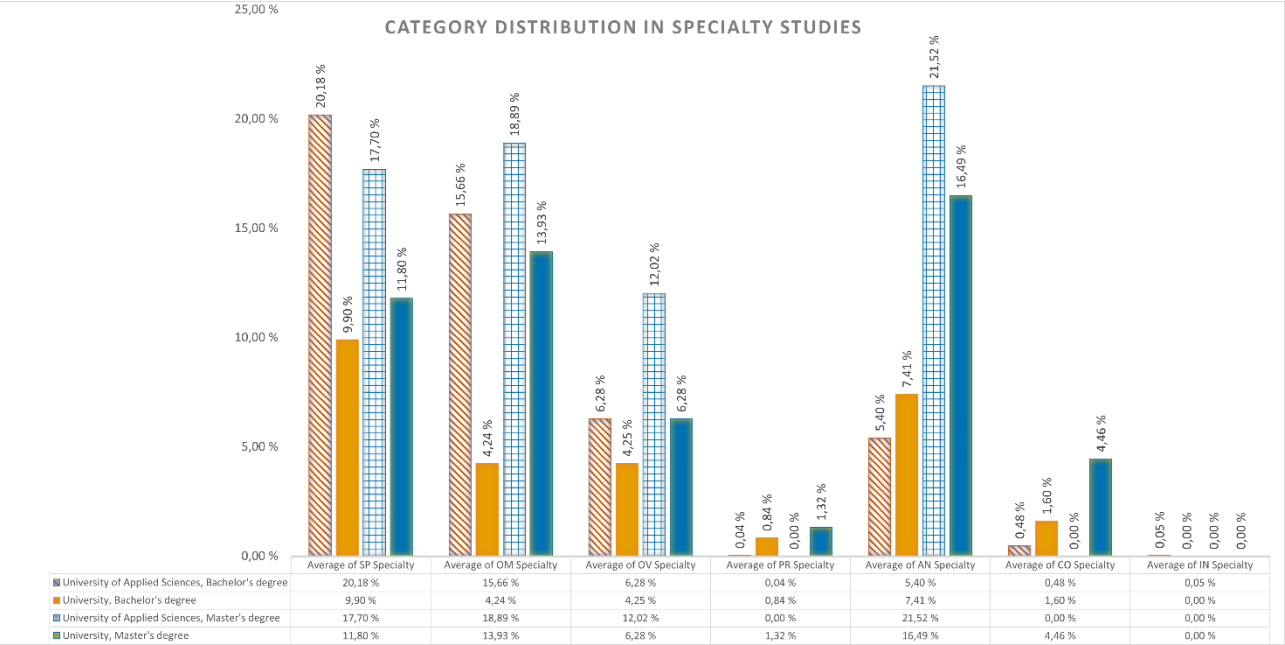

Figure 7. Distribution in Specialty studies

How much the percentage is, it is presented in Figure 7, and the same in ECTS-credits, is presented on Table 14.

Table 14. Category distribution in Specialty studies in percentage with the amount of ECTS-credits

Category	University of Applied Sciences, Bachelor's degree	ECTS	University, Bachelor's degree	ECTS2	University of Applied Sciences, Master's degree	ECTS3	University, Master's degree	ECTS4
Average of SP Specialty	20.18 %	15	9.90 %	9	17.70 %	2	11.80 %	10
Average of OM Specialty	15.66 %	12	4.24 %	4	18.89 %	2	13.93 %	12
Average of OV Specialty	6.28 %	5	4.25 %	4	12.02 %	1	6.28 %	5
Average of PR Specialty	0.04 %	0	0.84 %	1	0.00 %	0	1.32 %	1
Average of AN Specialty	5.40 %	4	7.41 %	7	21.52 %	2	16.49 %	14
Average of CO Specialty	0.48 %	0	1.60 %	2	0.00 %	0	4.46 %	4
Average of IN Specialty	0.05 %	0	0.00 %	0	0.00 %	0	0.00 %	0

The first thing that could be observed from the results, was the variety of studies that a student could choose, especially what the bachelor's and master's degree program students in the universities could choose. A concerning thing was that the same phenomenon that was present in core-studies was observable – lack of PR, CO, and IN category studies.

5.5 NICE Category Distribution in Elective studies

Elective studies are studies in course catalogues that can be freely chosen. Typically, a degree program includes a handful of elective courses, where students typically choose from. But exemptions were present, for instance, South-Eastern Finland University of Applied Sciences provided hundreds of different courses as elective, ranging from the basics of first aid to public music event design (designing Emma Gala) in Information Technology, the Bachelor of Engineering degree program.

When calculating values presented in Figure 8, the same processes were used as in core and specialty studies.

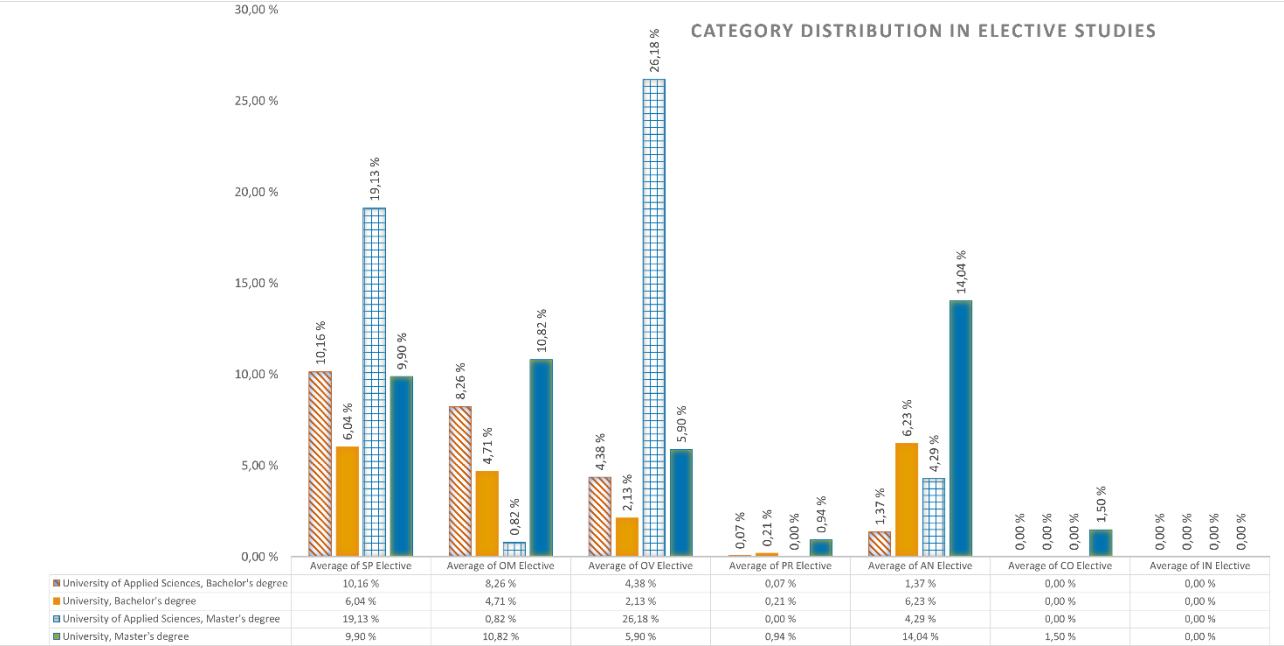

Figure 8. Category Distribution in Elective studies

How much the percentages presented above, are in ECTS-credits, is presented in Table 15.

Table 15. Category distribution in Elective studies in percentage with the amount of ECTS-credits

Category	University of Applied Sciences, Bachelor's degree	ECTS	University, Bachelor's degree	ECTS2	University of Applied Sciences, Master's degree	ECTS3	University, Master's degree	ECTS4
Average of SP Elective	10.16 %	19	6.04 %	4	19.13 %	12	9.90 %	9
Average of OM Elective	8.26 %	16	4.71 %	3	0.82 %	0	10.82 %	10
Average of OV Elective	4.38 %	8	2.13 %	2	26.18 %	16	5.99 %	5
Average of PR Elective	0.07 %	0	0.21 %	0	0.00 %	0	0.94 %	1
Average of AN Elective	1.37 %	3	6.23 %	5	4.29 %	3	14.04 %	12
Average of CO Elective	0.00 %	0	0.00 %	0	0.00 %	0	1.50 %	1
Average of IN Elective	0.00 %	0	0.00 %	0	0.00 %	0	0.00 %	0

In elective studies, two categories could be seen rising above all others. Securely Provision and Oversee and Govern categories in master's degrees programme in the universities of applied sciences. In the figure, we can detect slight problems relating to presentation of the curricula and categorisation of the courses, whereas the number of elective studies presented in course catalogues varies. In here, possible problems could also be seen, as arithmetic mean in calculations was used. This caused the calculated averages having to be interpreted by the reader as more of a trend rather than actual hard quantitative percentage.

5.6 NICE Category Distribution in all studies

Finally, the category distribution in all studies was analysed, including core, specialty, and elective studies. Percentages presented in the Figure 9, are calculated from the arithmetic mean percentage values from the required ECTS-amount per degree program. This varies from before, where we calculated from per Core, Specialty or Elective studies.

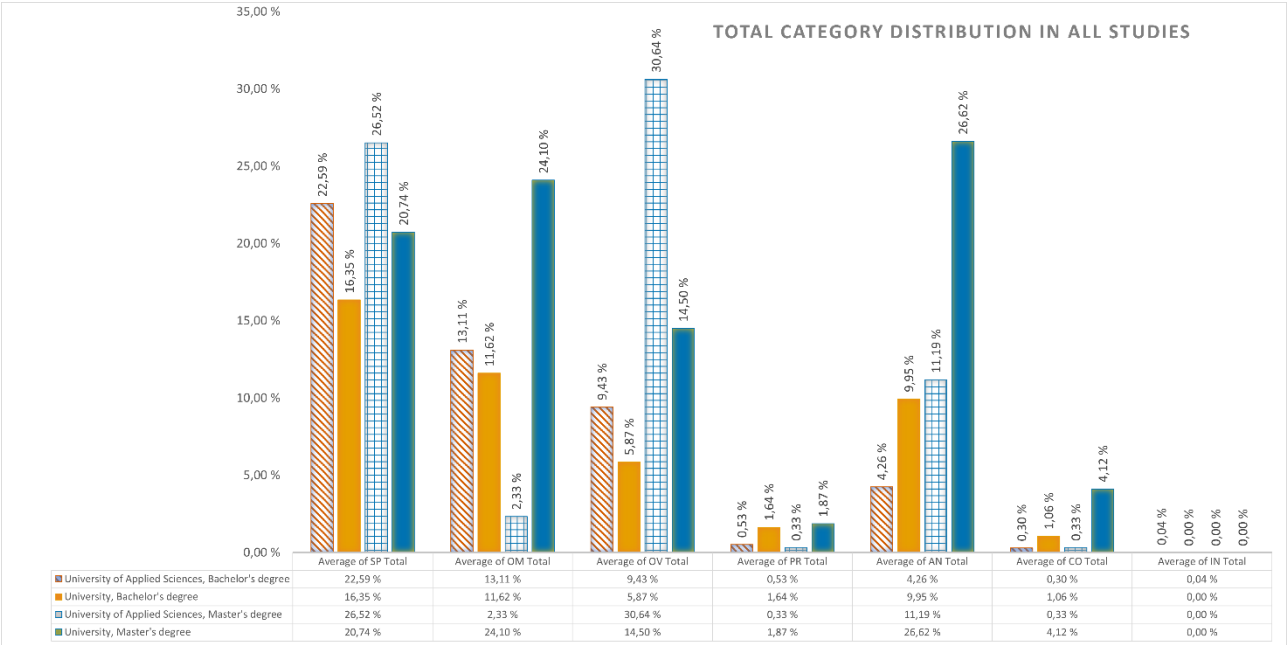

Figure 9. Total Category Distribution in all studies

How much the percentages presented above, are in ECTS-credits, is presented on Table 16.

Table 16. Category distribution in all studies in percentage with the amount of ECTS-credits

Category	University of Applied Sciences, Bachelor's degree	ECTS	University, Bachelor's degree	ECTS2	University of Applied Sciences, Master's degree	ECTS3	University, Master's degree	ECTS4
Average of SP Total	22.59 %	51	16.35 %	29	26.52 %	20	20.74 %	25
Average of OM Total	13.11 %	30	11.62 %	21	2.33 %	2	24.10 %	29
Average of OV Total	9.43 %	21	5.87 %	11	30.64 %	23	14.84 %	18
Average of PR Total	0.53 %	1	1.64 %	3	0.33 %	0	1.87 %	2
Average of AN Total	4.26 %	10	9.95 %	18	11.19 %	8	26.62 %	32
Average of CO Total	0.30 %	1	1.06 %	2	0.33 %	0	4.12 %	5
Average of IN Total	0.04 %	0	0.00 %	0	0.00 %	0	0.00 %	0

5.7 Purely Cyber Security focused courses in Core studies

The next analysis focused on the amount of purely cybersecurity focused courses in core studies. Results included courses that are categorised as purely cybersecurity focused, for example, network and information security or basics of cyber security. The results are presented in Figure 10.

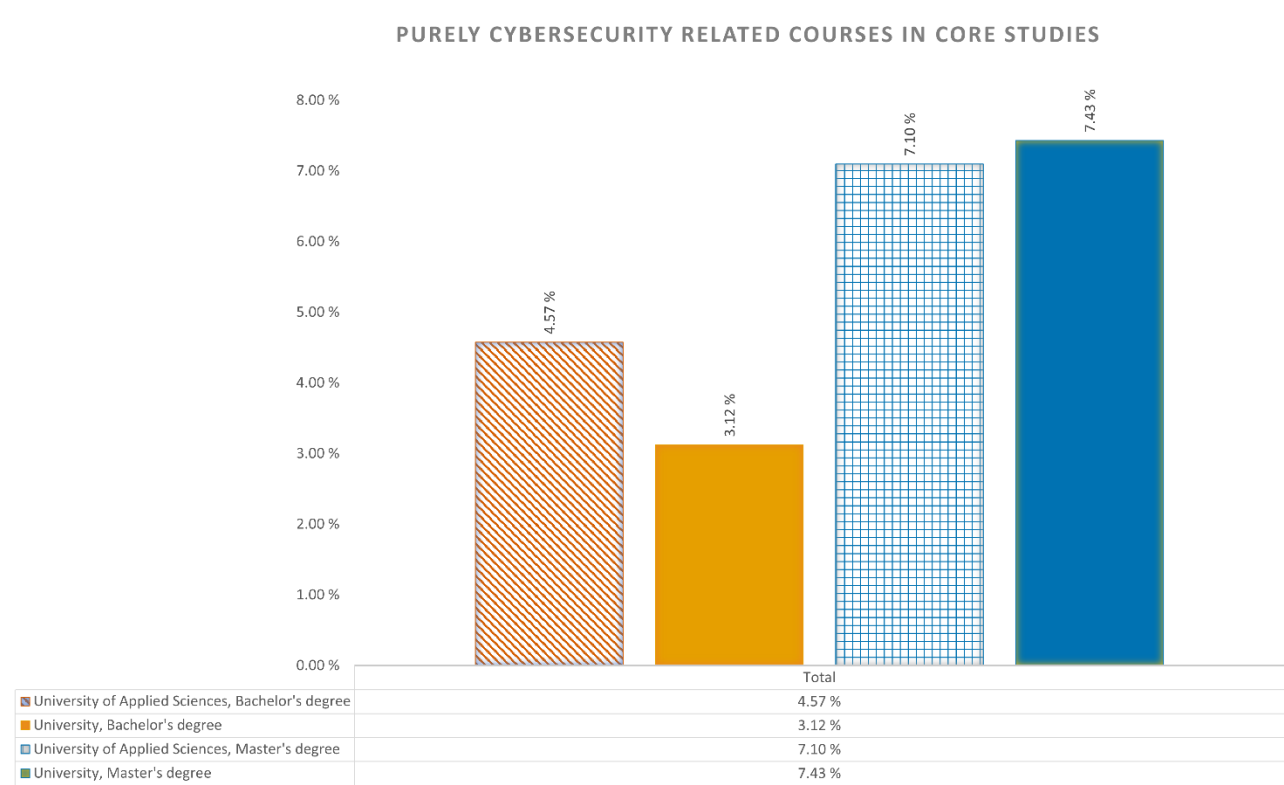

Figure 10. Purely Cyber Security related courses in Core studies

How much the percentage presented in Figure 10, is in ECTS-credits, is presented on Table 17.

Table 17. Purely Cyber Security related courses in Core studies in percentage with the amount of ECTS-credits

Category	University of Applied Sciences, Bachelor's degree	ECTS	University, Bachelor's degree	ECTS2	University of Applied Sciences, Master's degree	ECTS3	University, Master's degree	ECTS4
Average of Cyber Core	4.57 %	9	3.12 %	4	7.10 %	4	7.43 %	5

From the results, we could see that each of the degree programs include some amount of cyber security studies: in the bachelor's level typically one to two courses and in the master's level one course. Overall, this was a quite good result, as purely cyber security related studies were present in all levels.

Of course, as we used arithmetic mean in calculating these values, degree programs could include none and above the average amount. Cybersecurity oriented degree programs also raised the average.

5.8 Total of Cyber Security related courses in Core studies

Finally, total amount of cyber security related studies in core studies was calculated. Results included all the categories and a note if the course was cybersecurity related. The results are presented in Figure 11.

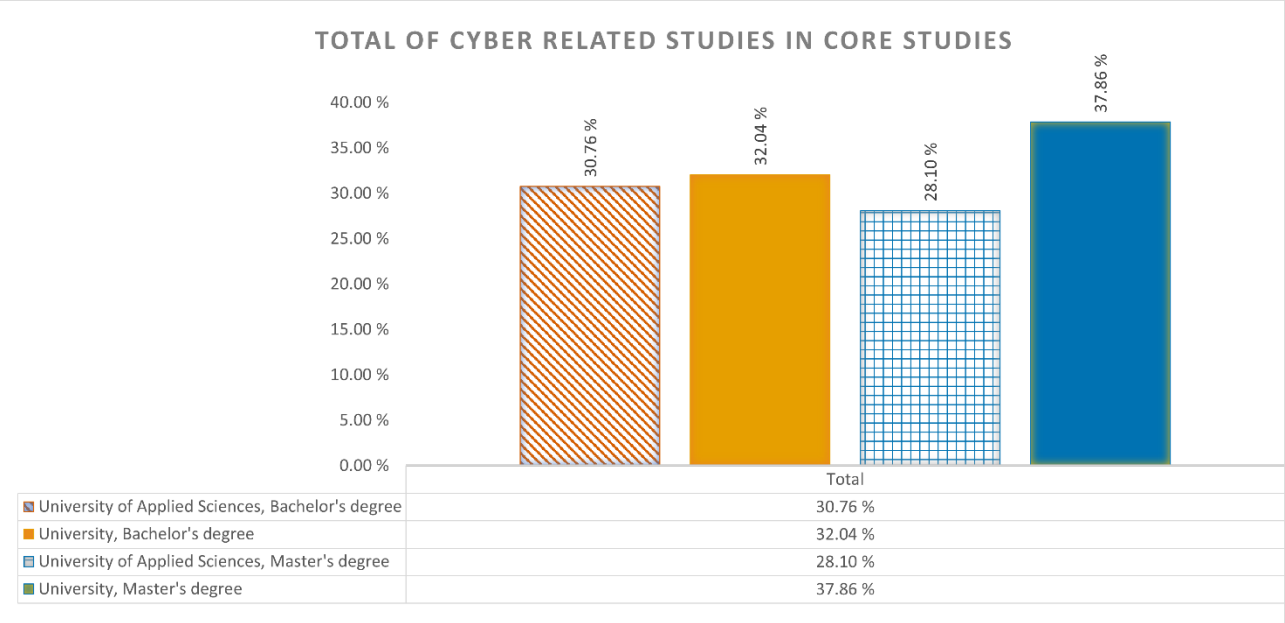

Figure 11. Total amount of cyber related studies in Core studies

How much the percentage presented in Figure 11, is in ECTS-credits, is presented in Table 18.

Table 18. Total amount of Cyber Security related courses in Core studies in percentage with the amount of ECTS-credits

Category	University of Applied Sciences, Bachelor's degree	ECTS	University, Bachelor's degree	ECTS2	University of Applied Sciences, Master's degree	ECTS3	University, Master's degree	ECTS4
Average of Cyber Core	30.76 %	59	32.04 %	42	28.10 %	16	32.47 %	24

The results showed that approximately a third of the studies in core-studies could be categorised as cyber security related. This in overall is good percentage.

6 Conclusions

6.1 Reliability and ethicality

Authors have collected the material with minimal affection to source material, from publicly available sources at university websites. Authors relies on that the material collected from these sources, are authentic and are based on the guidelines and frameworks provided by Finland Ministry of Education. These frameworks and guidelines have been presented in chapters 3.2.2 and 3.3.

Material does not include any personal details or copyright material. Material collected to the submitted journal publication and used in this thesis is in publicly available in public repository, with links to the original source materials, see (Saharinen, Leino, & Kokkonen, 2021). Material does not also include any technical details or processes, that can be exploited by malicious third-party actor.

The author (Leino) has followed Ethical Principles for JAMK University of Applied Sciences (JAMK University of Applied Sciences, 2018) and guidelines defined by JAMK University of Applied Sciences in writing this thesis and the author guidelines and publication ethics defined by Oxford Academic Journal of Cybersecurity (Oxford University Press, 2021).

Since the universities can choose the format and presentation of the source material freely, this leads to certain author interpretation when normalizing and organizing the data into more harmonized format. This process is presented in the chapter 4.2 and should be noted as reliability problem. By using an author defined keywords in categorising the courses, this should be noted as a reliability problem, as the keywords are defined according to the author's subjective interpretation from NICE descriptions and from course names.

6.2 Inspection of key results related to the theoretical framework presented in the beginning of thesis

When comparing the overall results with Finland's Cyber Security Strategy, it can be concluded that Finland's higher education system achieves quite well part of the strengthening requirements laid in cyber strategy. This can be seen in the number of studies related to Securely Provision, Op-

erate and Maintain categories in the bachelor level core studies and Oversee and Govern and Analyse categories in the master level core studies. The first two categories, Securely Provision and Operate and Maintain, are focused on designing, building, and maintaining secure information networks and systems, as well as on developing software. Oversee and Govern and Analyse categories are focused on making management decision according to the analysis. The amount of cybersecurity related studies in core studies also confirm this conclusion. An alarming thing is a lack of the following three categories in all studies: Protect and Defend, Collect and Operate and Investigate. These categories are focused on offensive, defensive and investigative areas in cybersecurity, and these categories are important when creating cybersecurity capability.

Protect and Defend category is important in identifying and handling cybersecurity incidents as well as protecting systems. These tasks are important in a day-to-day job in cybersecurity. These areas are also important in co-operation, as the ability to detect possible threats and defend is an imperative ability to have in current cyber domain, where cyberthreats knows no borders. Investigate is an important category when investigating already happened cybersecurity incidents. Collect and Operate is the category that is focused on the more offensive cybersecurity that is an important and rising topic in cybersecurity, especially in EU-area. European Union Agency for Cybersecurity (ENISA) is actively campaigning on the research projects in area of Cyber Threat Intelligence (CTI) (European Union Agency for Cybersecurity, 2021). The area where Collect and Operate category closely relates to.

What could explain the lack of courses related to these previous categories in higher education? A one possible explanation could be whether the courses provided by organisations like SANS are fulfilling the workforce requirement in these areas. An example of these courses provided by SANS is FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics, that is concentrated on the investigate category (SANS, 2021). These courses are expensive costing thousands of dollars for students to attend to, and are out of reach for the majority, if companies are not willing to pay. Another possible reason could be that these areas are thought as a part of, for instance, Finnish Defence Forces or Police. A further examination to curricula in police academy revealed that no relevant courses to protect and defend, investigate or collect and operate are available.

As the global cybersecurity workforce deficits rises, it would be advisable to increase the education in the following three categories: Protect and Defend, Investigate and Collect and Operate, at least in the elective studies, if not in mandatory level. By increasing the education in these three categories, Finland could handle future challenges, as cybersecurity incidents are rising and co-operation between EU-nations deepening.

One of the key points was using keywords (attribute list) rather than using intuition and interpretation in defining the course relation to NICE categories. By using predefined attributes, this gives room for debate, whether the keyword list includes all the possible attributes in correct categories and whether the relation to category is valid. The data and used attributes are freely available. This gives a reader the ability to analyse and compare results to different set of keywords.

6.3 Future research topics

Even though, a wide range of course catalogues were reviewed and gathered in this research, to better understand the state of the current Finnish cybersecurity education, it would be advisable to research how many of the students choose cybersecurity courses as part of their education and whether these students complete the courses or not. This would possibly give an understanding on the actual cybersecurity knowledge among students, which could speak out for authorities to increase the amount of cybersecurity education, but also to help to fulfil different industries' need for skilled and educated cybersecurity experts. In the research results, it was noted that especially PR, CO and IN type of studies were under-represented, and to meet the Finnish cybersecurity strategy requirements in full, some focus should be put on the previous.

As the course catalogue goes through major overhauls typically in three to five years on the bachelor's degree and from two to four years on the master's degree in Finland higher education. This type of research could be done in every three to five years, to further get trends how the education sector will develop over time.

As always in research questions or datasets, the methods how the original data is published and presented could always be improved. This would improve the future research if the publication

methods and presentation could be standardised. A one possible method could be using, for example, the studyinfo.fi -website (Ministry of Education and Culture, 2021) to present the full curricula.

References

Ajankohtaista: Vastaamon tiedotteet ja uutiset. (12. April 2021). Retrieved from Psykoterapiakeskus Vastaamo.fi: https://vastaamo.fi/?entry

Backlund, J. (2020). *Examination of contemporary cyber security education.* JAMK University of Applied Sciences. Retrieved from http://urn.fi/URN:NBN:fi:amk-2020060416851

Blackstone, A. (2012). Inductive or Deductive? Two Different Approaches. Teoksessa A. Blackstone, *Principles of Sociological Inquiry – Qualitative and Quantitative Methods* (pp. 19-20). Saylor Foundation.

Bologna Working Group on Qualifications Frameworks. (23. 2 2005). *A Framework for Qualifications of the European Higher Education Area.* Copenhagen, Denmark: Ministry of Science, Technology and Innovation. Retrieved from A Framework for Qualifications of the European Higher Education Area: http://ecahe.eu/w/images/7/76/A_Framework_for_Qualifications_for_the_European_Higher_Education_Area.pdf

Concordia. (16. 5 2021). *Concordia consortium*. Retrieved from CONCORDIA website: https://www.concordia-h2020.eu/

CyberSec4Europe. (16. 5 2021). *About: CyberSec4Europe*. Retrieved from CyberSec4Europe Website: https://cybersec4europe.eu/about/

De Zan, T.;& Di Franco, F. (2019). *CYBERSECURITY SKILLS DEVELOPMENT IN THE EU.* Athens: European Union Agency for Cybersecurity (ENISA). doi:10.2824/525144

Echo. (16. 5 2021). *Project summary: ECHO*. Retrieved from ECHO website: https://echonetwork.eu/project-summary/

Eurofound. (2020). *Living, working and COVID-19, COVID-19 series.* Luxembourg.: Publications Office of the European Union.

European Commission. (2008). *Explaining the European Qualifications Framework for Lifelong Learning.* Luxembourg: Office for Official Publications of the European Communities.

European Commission. (2020). *The EU's Cybersecurity Strategy for the Digital Decade.* Brussels: HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY. Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN

European Union. (2015). *ECTS Users' Guide.* Luxembourg: Publications Office of the European Union. doi:10.2766/87192

European Union. (23. 2 2021). *Cedefop Europa*. Retrieved from European qualifications framework (EQF): https://www.cedefop.europa.eu/en/events-and-projects/projects/european-qualifications-framework-eqf

European Union Agency for Cybersecurity. (2021). *ENISA Threat Landscape 2020 - Research topics.* Attiki: European Union Agency for Cybersecurity (ENISA).

Frost & Sullivan. (2017). *2017 Global Information Security Workforce Study.* Center for Cyber Safety and Education.

Gartner, Inc. (9. May 2020). *Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time* . Retrieved from Gartner website: https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time

General Secretariat of the Council. (2018). *EU Cyber Defence Policy Framework.* Brussels: Council of theEuropean Union.

Greenberg, A. (22. 8 2018). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Retrieved from Wired.com: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hajný, J., Levillain, O., Grigaliunas, S., Versinskiene, E., Bruze, E., & Zylius, R. (2020). *Cybersecurity skills framework.* European Union: SPARTA.

JAMK University of Applied Sciences. (2018). *Ethical Principles for JAMK University of Applied Sciences.* Jyväskylä: JAMK University of Applied Sciences. Retrieved from https://www.jamk.fi/globalassets/opinto-opas-amk/opiskelu/pedagogiset-ja-eettiset-periaatteet/eettiset-periaatteet-11122018-en.pdf

JAMK University of Applied Sciences. (17. 4 2021). *Study Guide Curricula*. Retrieved from https://opetussuunnitelmat.peppi.jamk.fi/en/49/en

Joint Task Force On Cybersecurity Education. (2018). *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity.* New York: Association for Computing Machinery. doi:https://doi.org/10.1145/3184594

Jones, K., Namin, A., & Armstrong, M. (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. doi:https://doi.org/10.1145/3152893

Kallio, M., Korhonen, P., & Salo, S. (2003). *Johdatus kvantitatiiviseen analyysin taloustieteissä.* Helsinki: Hakapaino Oy.

Lehto, M., & Niemelä, J. (2019). *Kyberalan tutkimus ja koulutus Suomessa 2019.* Jyväskylä: Jyväskylän Yliopisto. Retrieved from https://www.jyu.fi/it/fi/tutkimus/julkaisut/it-julkaisut/kyberalan_koulutus_suomessa_verkkoversio.pdf

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T., & Salminen, M. (2017). *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan*

saavuttamiseksi. Helsinki: Valtioneuvoston kanslia. Retrieved from https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160233/Suomen_kyberturvallisuuden_nykytila%2c__tavoitetila_ja.pdf

Lehto, M., Tyrväinen, P., Pöyhönen, J., & Talja, R. (2019). *Kyberturvallisuus Suomessa 2019–2029.* Jyväskylä: Jyväskylän Yliopisto.

Maanpuolustuskorkeakoulu. (17. 4 2021). *National Defence Universty.* Retrieved from Yleinen opintojen opas : sotatieteelliset perus- ja jatkotutkinnot: https://www.doria.fi/bitstream/handle/10024/178064/MPKK_opinto_opas_yleinen_osa_2020_WEB.pdf?sequence=1&isAllowed=y

Mertens, W., Pugliese, A., & Recker, J. (2017). *Quantitative Data Analysis.* Switzerland: Springer International Publishing. doi:10.1007/978-3-319-42700-3

Ministry of Education and Culture. (2009). *Universities Act.* Helsinki: Ministry of Education and Culture, Finland. Retrieved from https://www.finlex.fi/en/laki/kaannokset/2009/en20090558.pdf

Ministry of Education and Culture. (2014). *Universities of Applied Sciences Act.* Helsinki: Ministry of Education and Culture. Retrieved from https://www.finlex.fi/en/laki/kaannokset/2014/en20140932_20160563.pdf

Ministry of Education and Culture. (15. 12 2020). *Higher education institutions, science agencies, research institutes and other public research organisations*. Retrieved from Ministry of Higher Education Web site: https://minedu.fi/en/heis-and-science-agencies

Ministry of Education and Culture. (23. 5 2021). *What is Studyinfo*. Retrieved from Studyinfo.fi Web site: https://studyinfo.fi/wp2/en/what-is-studyinfo/

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

Newhouse, W., Stephanie, K., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE).* National Institute of Standards and Technology. doi:https://doi.org/10.6028/NIST.SP.800-181

Oxford University Press. (2021). *Oxford Academic, Journal of Cybersecurity*. Retrieved from https://academic.oup.com/cybersecurity/pages/General_Instructions

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

Saharinen, K., Karjalainen, M., & Kokkonen, T. (2019). A Design Model for a Degree Programme in Cyber Security. *ICETC 2019: 2019 11th International Conference on Education Technology*

and Computers (pp. 3-7). New York: Association for Computing Machinery. doi:10.1145/3369255.3369266

Saharinen, K., Leino, V., & Kokkonen, T. (9. 5 2021). *Analysing Cyber Security Education in Degree Programmes of Finnish Universities*. Retrieved from Jamk labranet Gitlab: https://gitlab.labranet.jamk.fi/cs4e/analysing-cyber-security-education-in-degree-programmes-of-finnish-universities

Saharinen, K., Leino, V., & Kokkonen, T. (2021). *Analysing Cybersecurity Education in Degree.* Oxford Journal of Cybersecurity.

SANS. (2. may 2021). *Cybersecurity Courses & Certifications*. Retrieved from SANS Website: https://www.sans.org/cyber-security-courses/

Secretariat of the Security Committee. (2013). *Finland's Cyber security Strategy.* Helsinki: Secretariat of the Security Committee.

Secretariat of the Security Committee. (2019). *Finland's Cyber security Strategy.* Helsinki: Secretariat of the Security Committee.

Sparta. (16. 5 2021). *About: Sparta*. Retrieved from SPARTA website: https://sparta.eu/#SPARTA

The Finnish National Agency for Education, the Ministry for 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.* Helsinki: The Finnish National Agency for Education.

Appendices

Appendix 1. Submitted Journal Publication

Oxford Journal of Cybersecurity, 2021, 1–15
doi: DOI HERE
Advance Access Publication Date: Day Month Year
Research Paper

Analysing Cybersecurity Education in Degree Programmes of Finnish Universities

Karo Saharinen,[1,*] Vesa Leino[1] and Tero Kokkonen[1]

[1]Institute of Information Technology, JAMK University of Applied Sciences, Piippukatu 2, 40100, Jyväskylä, Finland

*Corresponding author. karo.saharinen@jamk.fi

FOR PUBLISHER ONLY Received on Date Month Year; revised on Date Month Year; accepted on Date Month Year

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 measurement 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 framework, 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.

Key words: Cybersecurity, Education, Degree Programme, Cybersecurity Workforce

Introduction

Given the frequent cybersecurity incidents and threats facing Global 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 [1]. ECSO has also announced estimation by Frost & Sullivan about 1.8 million cybersecurity professionals workforce deficit by 2022 [2]. Finland's Cyber Security Strategy has demanded since 2013, that cybersecurity education should be established and implemented on all levels of education in Finland [3]. The updated 2019 version of the strategy [4] 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 and what results it has yielded. Different strategic papers and implementation 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. [5] mostly mentions the education sector of other countries to have degree programmes of their own dedicated solely to cybersecurity. Also, another report by Lehto et al. [6] only lists the available course

names and codes in different educational organisations in Finland, however does not take into account if the courses are in any way mandatory; they just exist within the curricula.

Based on this, 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 quantitaive 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 related to Information and Communications Technology. These are typically present and taught in organisational units related to technology or business, but sometimes can be found in defence related education.

Higher Education in Europe

European Qualifications Framework [7] (EQF) sets out the levels of education. 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 [8] (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 [9].

European Credit Transfer and Accumulation System (ECTS) [10] is a generally agreed specification 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 [11] 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[1])

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. [12] and Simola et al. [13]. It is a subject that has facinated researchers of other countries aspiring towards the same phenomenon e.g. Üstün and Eryilmaz [14] and Altaf et al. [15]. Finnish higher education has

[1] The terms Core, Specialty and Elective are used throughout the paper in synonym to ECTS Guide terminology

two placements in the top 250 university lists[2] 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[3] highlighting the focus of this research paper.

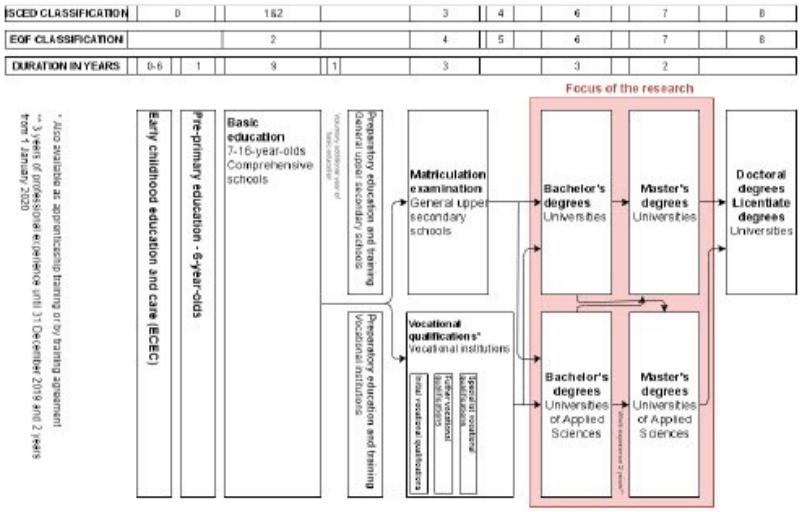

Fig. 1: The Finnish Education System and this research context

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[4][5] 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.

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

[2] https://www.timeshighereducation.com/

[3] https://minedu.fi/en/education-system

[4] https://www.finlex.fi/fi/laki/kaannokset/2009/en20090558.pdf

[5] https://finlex.fi/fi/laki/kaannokset/2014/en20140932_20160563.pdf

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*.

Cybersecurity Frameworks

Cybersecurity field has developed in the past few years actively by different frameworks 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 et al. [16] describe on how these frameworks could be utilised to design cybersecurity curricula.

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. [17] and updated in 2020 by Petersen et al. [18]. The framework was developed throughout a decade of development[6] and research accompanying it such as Jones et al. [19] and Armstrong et al [20].

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[7].

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)[8], Cyber Security Competence for Research and Innovation (CONCORDIA)[9] and Strategic Programs for Advanced Research and Technology in Europe (SPARTA)[10] 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. [21]. 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. [22] which resulted in A Proposal for a European Cybersecurity Taxonomy [23]. 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 21, pg. 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 Skills Framework, assuming the basis of its creation stays the same. These seven workforce categories that are described in Table 3 [17].

Table 3. NICE framework [17] Categories

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.

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

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

[8] https://cybersec4europe.eu/

[9] https://www.concordia-h2020.eu/

[10] https://www.sparta.eu/

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[11] or plainly just PDF- linked[12] to the public website of the higher education organisation.

This process is presented in Figure 2

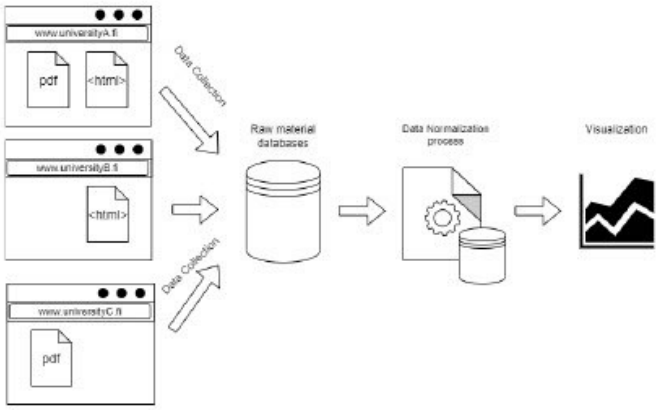

Fig. 2: Research flowchart

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.

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.

[11] `https://opetussuunnitelmat.peppi.jamk.fi/en/49/en`

[12] `https://www.jyu.fi/ops/fi/it/tietotekniikan-kandidaattiohjelma`

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	-	-	-

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.

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[13].

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 [24] of the research.

[13] 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.

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.

Results

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.

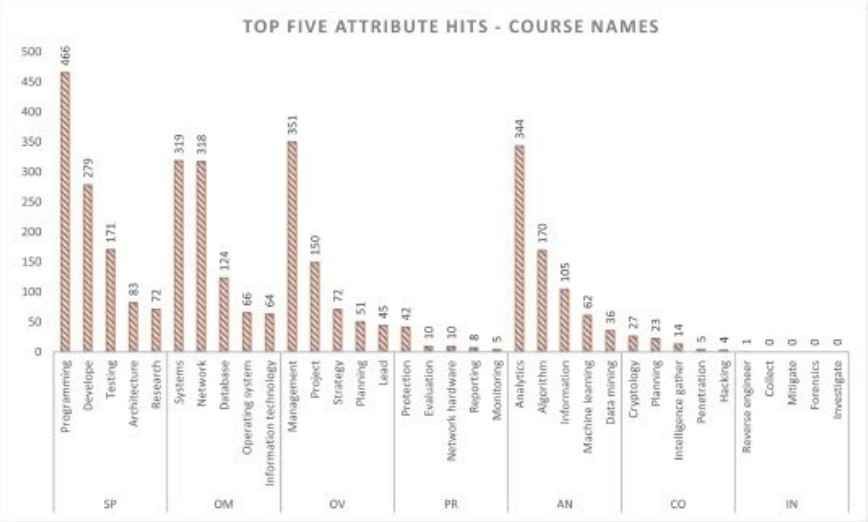

Fig. 3: Attribute hits in course names

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.

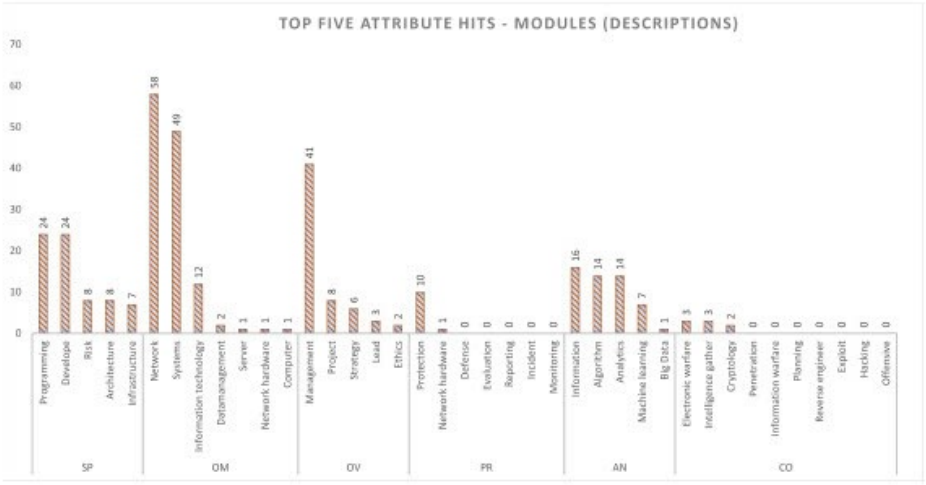

Fig. 4: Attribute hits in Modules Descriptions

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.

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.

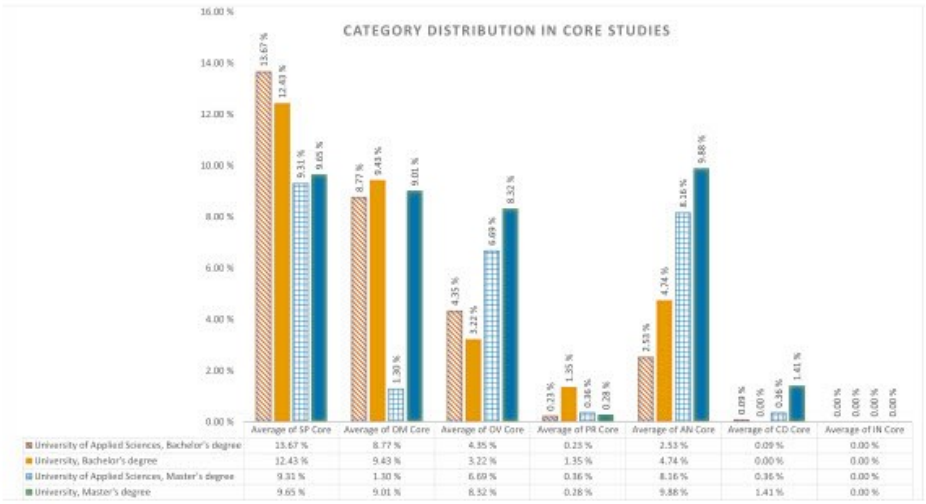

Fig. 5: Category Distribution in Core Studies

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[14].

- 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.

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.

[14] depends on the length of the bachelor's degree, thus an generalisation/approximated value

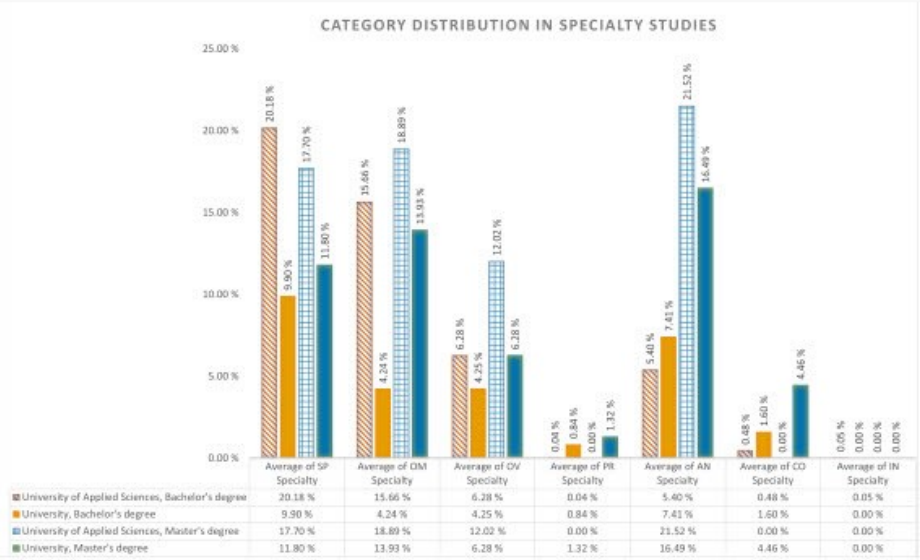

Fig. 6: Category Distribution in Specialty studies

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.

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[15]. The distribution is visualised in Figure 7.

[15] 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/ITNI21SP/year/2021`

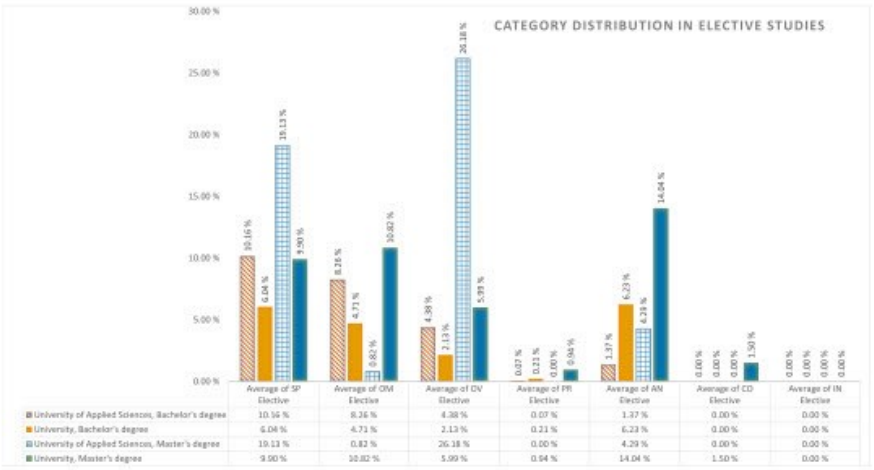

Fig. 7: Category Distribution in Elective studies

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.

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.

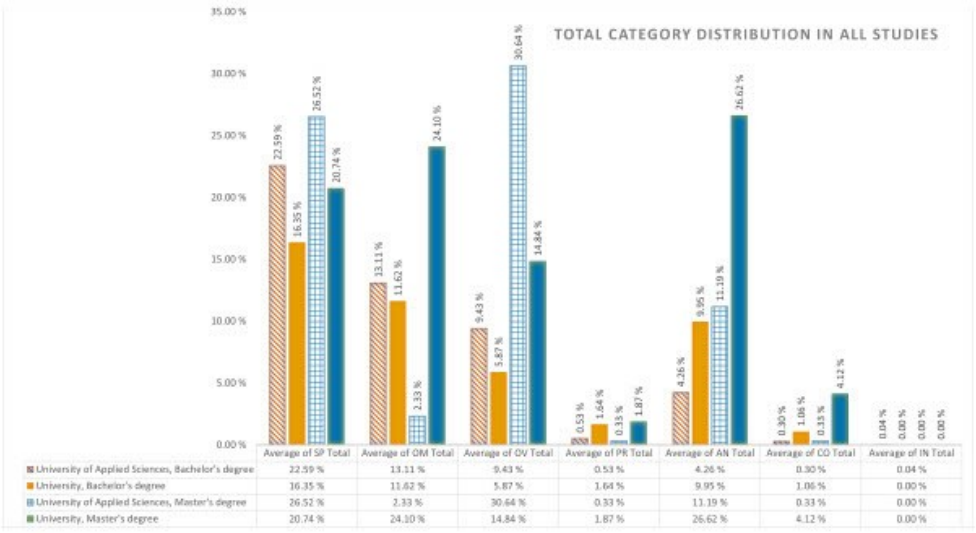

Fig. 8: Total Category Distribution in All Studies

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. Rocketing sky-high is the *Oversee and Govern* for 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.

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.

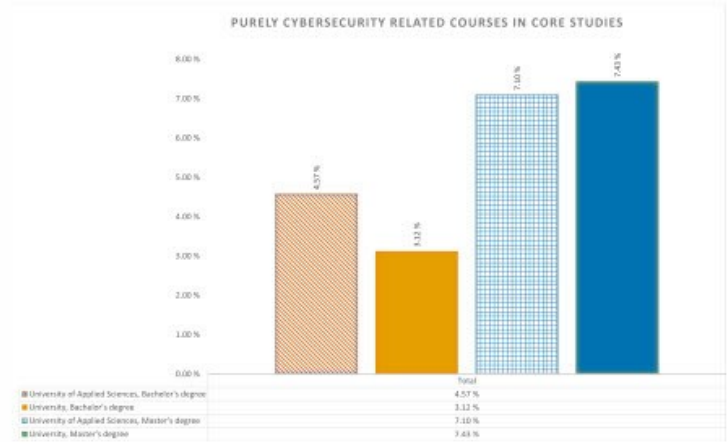

Fig. 9: Purely Cybersecurity Related Courses in Core studies

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.

Conclusions

Cybersecurity Education in Finland

As a conclusion, it is evident that the cybersecurity aspect is being handled in the higher education of Finland with either courses completely dedicated for cybersecurity and compulsory for participation, or somehow elective and categorizable to a cybersecurity framework.

The most important aspect is that as a generalisation, 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 categories of *Investigate*, *Protect and Defend* and *Collect and Operate* are seemed to be of very little emphasis/presence 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 [25]. 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.

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. This 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/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[16], however it does not offer much to the degree/course development and quality improvement of the given education field, what ever it might be.

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.

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 [17] 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.

[16] `https://vipunen.fi/en-gb/university-education`

[17] `https://cybersec4europe.eu/about/`

References

1. European Cyber Security Organisation (ECSO). POSITION PAPER, Gaps in European Cyber Education and Professional Training. https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf, Nov 2017.
2. European Cyber Security Organisation (ECSO). WG5 ANALYSIS, Information and Cyber Security Professional Certification. https://ecs-org.eu/documents/publications/60101ad752a50.pdf, Nov 2018.
3. Secretariat of the Security Committee. Finland's Cyber security Strategy, Government Resolution 24.1.2013. https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf, Jan 2013.
4. Secretariat of the Security Committee. Finland's Cyber security Strategy, Government Resolution 3.10.2019. https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf, Oct 2019.
5. Martti Lehto, Jarno Limnéll, Eeva Innola, Jouni Pöyhönen, Tarja Rusi, and Mirva Salminen. Finland's cyber security: the present state, vision and the actions needed to achieve the vision. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160233/Suomen_kyberturvallisuuden_nykytila%2c__tavoitetila_ja.pdf, 02 2017.
6. Martti Lehto, Jukka Niemelä, and Petri Vähäkainu. Cybersecurity research and education in finland 2019. https://www.jyu.fi/it/fi/tutkimus/julkaisut/it-julkaisut/kyberalan_koulutus_suomessa_verkkoversio.pdf, 2019.
7. Council of the European Union. *Council Recommendation on the European Qualifications Framework for lifelong learning.* Official Journal of the European Union, 2017.
8. Bologna Working Group. *A Framework for Qualifications of the European Higher Education Area.* Bologna Working Group Report on Qualifications Frameworks (Copenhagen, Danish Ministry of Science, Technology and Innovation), 2005.
9. *Report on the referencing of the Finnish National Qualifications Framework to the European Qualifications Framework and the Framework for Qualifications of the European Higher Education Area.* The Finnish National Agency for Education Ministry of Education and Culture, 2018.
10. European credit transfer and accumulation system (ects).
11. *ECTS Users' Guide.* Publications Office of the European Union, 2015.
12. Jouni Välijärvi, Pirjo Linnakyla¨, Pekka Kupari, Pasi Reinikainen, and Inga Arffman. The finnish success in pisa—and some reasons behind it. 01 2002.
13. Hannu Simola, Jaakko Kauko, Janne Varjo, Mira Kalalahti, and Fritjof Sahlström. *Dynamics in Education Politics and the Finnish PISA Miracle.* Oxford University Press, United Kingdom, May 2017.
14. Ulaş Üstün and Ali Eryilmaz. Analysis of finnish education system to question the reasons behind finnish success in pisa. 12 2018.
15. Sobia Altaf, Abid Shehzad, and Aneela Akhtar. Finnish education system and its triumph in pisa: Lessons to learn for pakistan. *Global Regional Review*, V:479–487, 03 2020.
16. Karo Saharinen, 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, page 3–7, New York, NY, USA, 2019. Association for Computing Machinery.
17. William Newhouse, Stephanie Keith, Benjamin Scribner, and Greg Witte. *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* National Institute of Standards and Technology, 2017.
18. Rodney Petersen, Danielle Santos, Matthew C. Smith, Karen A. Wetzel, and Greg Witte. *Workforce Framework for Cybersecurity (NICE Framework).* National Institute of Standards and Technology, 2020.
19. Keith S. Jones, 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. *ACM Trans. Comput. Educ.*, 18(3), August 2018.
20. Miriam E. Armstrong, Keith S. Jones, Akbar Siami Namin, and David C. Newton. Knowledge, skills, and abilities for specialized curricula in cyber defense: Results from interviews with cyber professionals. *ACM Trans. Comput. Educ.*, 20(4), November 2020.
21. Jan Hajný, Olivier Levillain, Sarunas Grigaliunas, Egidija Versinskiene, Evaldas Bruze, and Rimantas Zylius. *Cybersecurity skills framework.* SPARTA project, 2020.
22. Igor Nai Fovino, Ricardo Neisse, Alessandro Lazari, GianLuigi Ruzzante, Nineta Polemi, and Malgorzata Figwer. *European Cybersecurity Centres of Expertise Map - Definitions and Taxonomy.* Publications Office of the European Union, 2018.
23. Igor Nai Fovino, Ricardo Neisse, Jose Luis Hernandez Ramos, Nineta Polemi, GianLuigi Ruzzante, Malgorzata Figwer, and Alessandro Lazari. *A Proposal for a European Cybersecurity Taxonomy.* Publications Office of the European Union, 2019.
24. Vesa Leino and Karo Saharinen. [dataset]* open data set of the research, April 2021.
25. *ENISA Threat Landscape 2020 - Research topics.* European Union Agency for Cybersecurity, 2020.

Karo Saharinen. Saharinen is working as a Senior Lecturer in IT. He is the degree programme coordinator of the Master's Degree programme in Information Technology, Cyber Security at JAMK University of Applied Sciences. He is currently working on his PhD related to Cyber Security Education.

Vesa Leino. Leino is working as Security Analyst in Elisa and doing his Master's degree in Cyber Security at JAMK University of Applied Sciences.

Tero Kokkonen. Dr. Kokkonen works as a R&D-Manager at the Institute of Information Technology of JAMK University of Applied Sciences. He has significantly conducted research and development activities in the domain of cyber security and artificial intelligence including several international scientific publications. Tero is the Adjunct Professor in the Faculty of Information Technology at the University of Jyväskylä.