jamk

Analysing Cybersecurity Theses

Mapping Higher Education Theses Using Taxonomic Frameworks

Joonatan Ovaska

Bachelor's thesis
August 2022
Bachelor of Engineering, Information and Communication Technology

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Ovaska, Joonatan

Analysing Cybersecurity Theses - Mapping Higher Education Theses Using Taxonomic Frameworks

Jyväskylä: JAMK University of Applied Sciences, August 2022, 48 pages (+ appendices)

Bachelor's degree in information and communications technology

Permission for open access publication: Yes

Language of publication: English

Abstract

Cybersecurity as a field of education and as a workforce has not been quite long around. Building up frameworks to describe workforce and standardizing field of education is still probably finding its place. This study combines these two ideas by analysing theses done on higher education level to workforce by using NICE Framework with assist of European Cybersecurity Taxonomy Framework. Task is to provide an article for IEEE Conference about the topic with analysis done in regional area Central Finland. The analysis is done for publicly open theses found from sources of Theseus and JYX. As a result we can have an analysis providing information about the differences between target universities with the categories of NICE Framework and the thesis mapping of gathered dataset. As a result we can see how many theses are mapped into which category of NICE Framework and how many hits did each category and work role got. Using this knowledge it is possible to have studies on topics like how does these correlate to the current course pool and could it be updated through the findings. As a structure we go through the Finnish education system while giving a overlook for European and international level and structures, describing the current reform of the higher education system with bologna process leading up to the higher level of education on subject of cybersecurity, leading all the way to employment and transforming into workforce done with thesis project.

Keywords/tags (subjects)

Cybersecurity, Education, Thesis, NICE Framework, European Cybersecurity Taxonomy, Bologna Process

Miscellaneous (Confidential information)

-

jamk

Kuvailulehti

Ovaska, Joonatan

Kyberturvallisuuden opinnäytetöiden analysointi – Korkeakoulutasoisten opinnäytetöiden kartoittaminen taksonomiaviitekehyksiä käyttäen

Jyväskylä: Jyväskylän ammattikorkeakoulu. Elokuu 2022, 48 sivua (+ liitteet)

Tieto- ja viestintätekniikan insinöörityutkinto

Julkaisun kieli: englanti

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Kyberturvallisuus koulutusalana tai työvoimana eivät ole olleet pitkään tunnettuja. Työvoimaa kuvaavien viitekehysten rakentaminen ja koulutusalan standardointi on todennäköisesti vielä hakemassa paikkaansa. Tässä tutkimuksessa yhdistetään nämä kaksi idea analysoimalla korkeakoulutasolla tehtyjä opinnäytetöitä työvoimalle kehitetyillä NICE viitekehyksen, sekä Euroopan kyberturvallisuuden taksonomia viitekehyksen avulla. Tehtävänä on toimittaa artikkeli aiheesta IEEE-konfferenssille, jossa käsitellään Keski-Suomen alueellista analyysia. Analyysi on tehty Theseuksen ja JYXin avoimista julkisesti saatavilla olevista opinnäytetöistä. Tuloksena voimme saada analyysin, jossa kartoitetaan tietueesta tietoa kohdeyliopistojen eroista NICE viitekehyksen kategorioiden avulla. Tuloksena voimme nähdä, Kuinka monta opinnäytetyötä on kartoitettu millekin NICE viitekehyksen kategorialle ja kuinka monta osumaa kukin kategoria ja työrooli sai. Tämän tiedon avulla on mahdollista tehdä tutkimuksia aiheista, kuten miten nämä korreloivat nykyikseen koulutustarjontaan ja voitaisiinko sitä päivittää tulosten kautta. Rakenteena käymme läpi suomalaisen koulutusjärjestelmän samalla kun annamme näkemyksen eurooppalaiselle ja kansainväliselle tasolle sekä rakenteisiin. Kuvailemme nykyistä korkeakoulujärjestelmän uudistusta Bologna prosessin avulla, joka johtaa nykyiseen malliin korkeakoulujärjestelmästä aina työllistymiseen, sekä työvoimaan muuntumiseen opinnäytetyöprojektien avulla.

Avainsanat (asiasanat)

Kyberturvallisuus, Koulutus, Opinnäytetyö, NICE Framework, European Cybersecurity Taxonomy, Bolognan Prosessi

Muut tiedot (salassa pidettävät liitteet)

-

Contents

1 Introduction ... 3
2 Literature and frameworks ... 5
2.1 Education system in Finland ... 5
2.2 Bologna Process and Higher Education in Finland ... 7
2.3 Cybersecurity as a field of education ... 8
2.4 Government Decree on Universities and Universities of Applied Sciences ... 10
2.4.1 European Qualifications Framework (EQF) ... 11
2.4.2 International Standard Classification of Education (ISCED) ... 13
2.5 Taxonomy Frameworks ... 19
2.5.1 NICE framework ... 19
2.5.2 The European Cybersecurity Taxonomy ... 28
2.5.3 Other frameworks ... 33
2.6 Related research ... 34
3 Article summary: Analysing Theses of Cyber Security Higher Education ... 35
3.1 Purpose and Objective of the Article ... 35
3.1.1 Tools ... 36
3.2 Dataset, Scoping & Research method ... 37
3.3 Analysis ... 37
3.3.1 NICE Categories ... 38
3.3.2 NICE Work roles ... 39
3.3.3 European Cybersecurity Taxonomy ... 40
3.4 Discussion ... 41
3.4.1 Cybersecurity as a field ... 41
3.4.2 Effects of the education level ... 42
3.4.3 NICE Framework ... 42
4 Conclusion ... 42
References ... 45
Appendices ... 49
Appendix 1. Article LaTeX source code (without comments): ... 49
Appendix 2. NICE Framework refernce spreasheet ... 64
Appendix 3. European Cybersecurity Taxonomy ... 66
Appendix 4. Submitted article as pdf ... 70

Figures

Figure 1 Education system in Finland (Finnish Education System, n.d.). 7

Figure 2 Tertiary education pathways in ISCED (ISCED 2011, 2012). 17

Figure 3 NICE Framework buiding blocks (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020). 21

Figure 4 Using competencies to assess learners through a position description (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020). 22

Figure 5 Using competencies to assess learners through a credential (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020). 23

Figure 6 Work roles' relationship to building blocks (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020). 24

Figure 7 Relationships among NICE Framework components (Newhouse W., Keith S., Scribner B., Witte G., 2017). 25

Figure 8 European Cybersecurity Taxonomy definition steps (Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M., Lazari, A., 2019). 29

Figure 9 High Level view of the European Cybersecurity Taxonomy (Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M., Lazari, A., 2019). 31

Figure 10 CSEC 2017 Knowledge struture linking with NICE Framework (Burley D., Bishop M., Kaza S., Gibson D., Hawthorne E., Buck S., 2017). 34

Figure 11 NICE Frame categories in colors with education type slicers 39

Figure 12 Colour duplicate of the European Cybersecurity Taxonomy industry sectors mapped with NICE Framework 41

Tables

Table 1 European Qualification Framework levels (2017/C 189/03, 2017). 12

Table 2 ISCED coding of levels (first digit) (ISCED 2011, 2012). 15

Table 3 ISCED coding of categories (second digit) (ISCED 2011, 2012). 15

Table 4 ICED coding of sub-categories (third digit) (ISCED 2011, 2012). 16

Table 5 Categories example relating to figure 2. 18

Table 6 Correspondance between ISCED 2011 and ISCED 1997 levels (ISCED 2011, 2012). 18

Table 7 NICE Framework workforce categories (Newhouse W., Keith S., Scribner B., Witte G., 2017). 25

Table 8 NICE Framework tasks, knowledge, skills, and abilities examples table. 27

Table 9 Sources of contributions to the cybersecurity taxonomy (Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M., Lazari, A., 2019). 30

1 Introduction

This thesis presents an article that maps cybersecurity theses using taxonomic frameworks and performs analysis on cybersecurity categories and work roles described in NICE framework based on that mapping. Theory part describes the Finnish education system and how it relates to cybersecurity and higher-level education. The goal is to go through the process of mapping higher-level education theses for given workforce/work field describing frameworks from the point of view where the thesis could land on the workforce side to have analysable data about the relationship between theses and workforce.

There are many frameworks available what we could use for this kind of mapping depending on the point of view one might want to use. This thesis describes the point of view from the workforce side instead of, for example, educational side. Objective is to get findings what kind of work roles are existing for thesis project while trying to reflect the workload of higher-level thesis project. This research can be used to find out where the workforce relation stands with thesis projects regionally.

Commissioner of this thesis is a staff member from JAMK University of Applied Sciences, senior lecturer Karo Saharinen, who suggested this topic for an analysis providing gathered raw dataset with a complete preliminary idea how to carry out the research. Motivation for research was highly interesting for the commissioner of the thesis to get this analysis result for chosen taxonomy frameworks and to study the findings from multiple perspectives.

Theses chosen for the dataset are pre-gathered by commissioner of the thesis with a search parameter from Theseus and JYX databases with a parameter of finding cybersecurity related theses. Each thesis is publicly available and can be used freely. Analysis includes the mapping part of theses and performing analysis depending on the result. Scope of the dataset is limited with regional aspect, dataset includes only theses from Jyväskylä area, therefore it could be used to develop regional education area.

Commissioner of the thesis wanted to get analysis done with the dataset to get the results and see if they match with nature of the compared universities and what are the most clear findings from analysis and to see if theses have clear weight point for certain field.

The research questions are:

- How can theses written in higher level education be mapped using taxonomy frameworks such as NICE Framework or similar frameworks for work roles or job titles?
- How reliable this kind of mapping towards the work role or job title would be?

Used research method is mixed method of quantity and quality research. Typically, in mixed method quantitative and quality dataset are mixed using analysis methods (Seppänen-Järvelä R., Åkerblad L., Haapakoski K., 2019). In this case study quantity dataset is the set of theses and it has been mixed with manual qualitative mapping with dataset of the used frameworks.

From the reliability perspective, the mapping part of the analysis can be done many ways. There is only one way introduced in this thesis. The same dataset can result in a bit different outcome while choosing another criterion. There is only a few thesis wide works that could be mapped only with one conclusion, also multicriteria could be used.

From ethical perspective, all literature and dataset collection has been carried out by either publicly available sources or sources with access of school library. Although the dataset contains works of individual personnel the individuality data is not used in this analysis or mapping process. As a research and literature part, books and scientific publications have been preferred whenever possible and always the original literature, such as law and ministry publications.

This thesis represents a submission (Ovaska, Saharinen, Sipola, 2022) of a paper to *The 7th IEEE Cyber Science and Technology Congress (CyberSciTech 2022)* conference which can be also find as appendix 4. IEEE sponsors nearly over thousand annual conferences and events globally, they provide a forum for authors and speakers to present their work at conferences. “IEEE produces cutting-edge conference publications in various technology areas that are” recognised by academia an industry worldwide. Submitted articles are peer reviewed (IEEE Conference, n.d.).

2 Literature and frameworks

Thesis analysis is done for chosen frameworks which can be used to point out the correlation from the workforce point of view. The main idea is to map theses dataset to correspond workforce and industry sectors. Literature includes the degree levels of the theses to correspond the maturity of theses and then open the framework designs and use cases. Degree levels have a major effect on the result of analysis.

The literature section concentrates on the journey from early education up to education level on the field and applied frameworks for the work life.

2.1 Education system in Finland

The Finnish education for each citizen in Finland is free of charge from start to finish, containing early childhood education all the way to up the higher education. The Finnish education system includes early childhood education and care, pre-primary education, basic education (comprehensive school), upper secondary education, higher education, and adult education (Finnish Education System, n.d.).

Early childhood education and care in Finland along with opportunities aims to promote development, health, and wellbeing. Pre-primary education helps children to improve opportunities for learning, which plays important part on the continuum to basic education. Pre-primary education is the first compulsory step for children in Finland. Compulsory education typically begins when children turn seven years old and ends when person reaches age of eighteen or when upper secondary qualification is achieved. Along with other education is progressing basic education in the arts in different fields, which teaches the person skills in self-expression and capabilities needed for vocational and higher education for chosen art (Finnish Education System, n.d.).

Comprehensive school education includes first nine school years. After comprehensive school has been finished person must apply for post-comprehensive school education, person may choose between general upper secondary education (Lukio) or vocational education (Finnish Education System, n.d.).

Lukio (General upper secondary education) provides general education. General upper secondary school does not qualify students for any occupation. After successful graduation from general upper secondary school students are eligible to apply for further studies at vocational institutions or higher education as in universities and universities of applied sciences (Finnish Education System, n.d.).

Vocational qualifications include upper secondary qualifications, further qualifications, and specialist qualifications. Upper secondary vocational school provides just enough basic skills required for the field of study. After successful graduation person is eligible to apply for universities or universities of applied sciences for further studies (Finnish Education System, n.d.).

Higher education in Finland includes universities and universities of applied sciences. The goal of universities is to provide scientific research and education based on it. Universities of applied sciences aims to provide satisfaction for labour market through practical education. Higher education includes bachelor's, master's, and doctoral degrees. Universities of applied sciences provide only bachelor's and master's degrees, while general universities provide also doctoral degrees. Two years work experience is required, if a person wants to progress in university of applied sciences from bachelor's degree towards master's degree (Finnish Education System, n.d.).

Adult education and training includes all sorts of different education, from basic skills up to degree studies, qualifications and more. Adult education could be paid by student or 3rd party, for example, training provided of purchased by employers. Liberal adult education offers studies which are not formal. Liberal adult education does not provide qualification or degree, and it is not governed by legislation (Finnish Education System, n.d.).

Finnish education system does not fully fit into European Qualifications Framework (EQF) nor International Standard Classification of Education (ISCED), especially on the lower levels, but in the field of higher education the degree levels are quite similar as seen from figure 1 from Finnish Education System's provided picture.

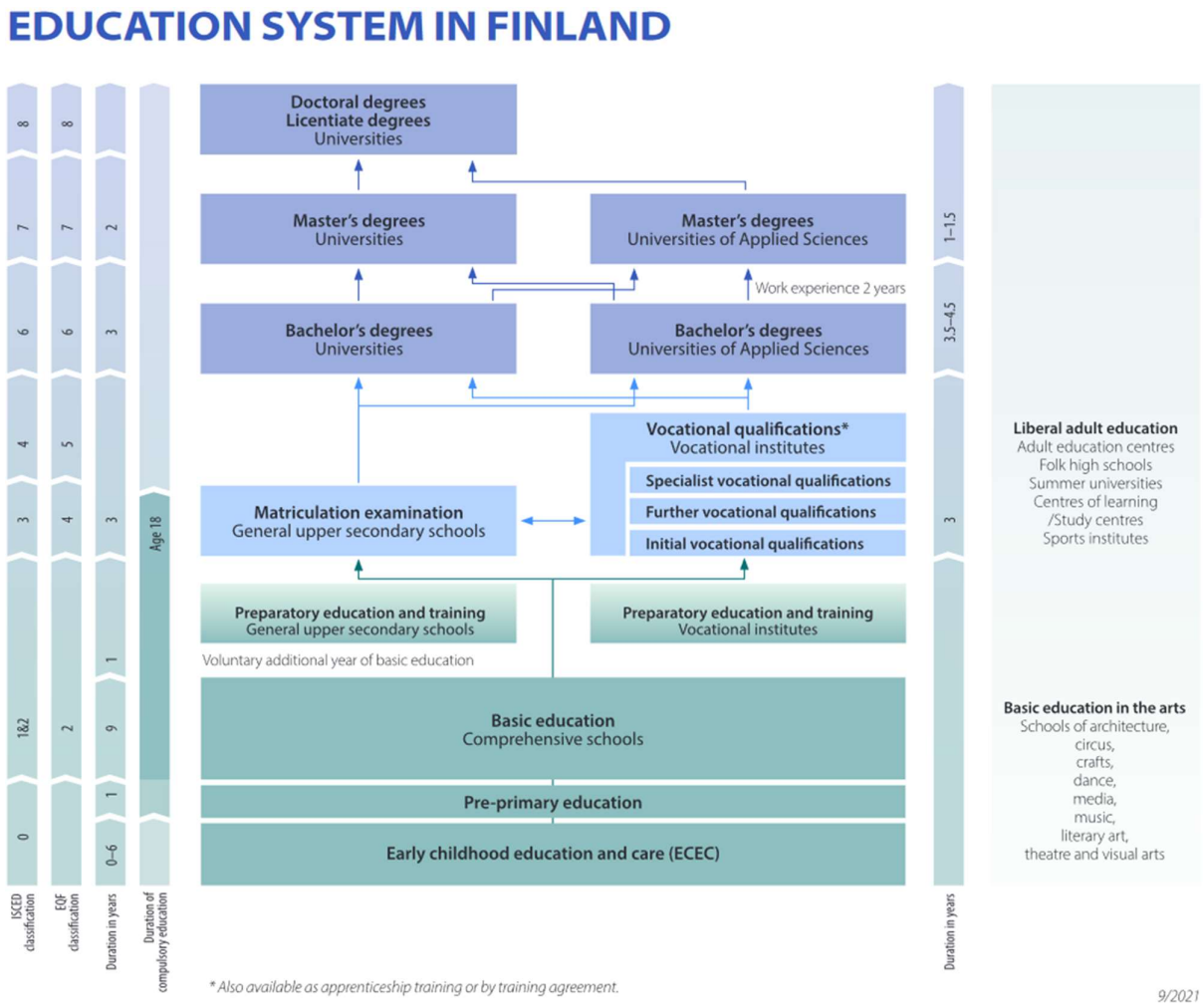

Figure 1 Education system in Finland (Finnish Education System, n.d.).

2.2 Bologna Process and Higher Education in Finland

Current reformation of Finnish higher educational system is implemented from Bologna Declaration of 1999. Bologna process (n.d.) states "Bologna Declaration is one of the main voluntary processes at European level as it implemented in 49 States, which define the European Higher Education Area (EHEA)"

Finnish implementation of the Bologna Declaration and the Prague Communiqué was declared to be implemented August 2003 and to be reformed on August 1, 2005. Finnish polytechnics can offer bachelor-level degrees in all field and postgraduate polytechnic degrees in certain fields. Post-

graduate polytechnic degrees are called second-cycle, post-experience programmes, the extent could vary from 60 up to 90 ECTS credits (EHEA Report, 2003).

Finland used adopted national credit system from the late 1970s, which was used through the higher education and is based on student's workload: one credit refers to 40 hours of student's work. On Bologna Declaration this credit system was to be replaced based directly on the ECTS from August 1, 2005, onwards, with the simultaneous university degree structure reform. The credit system includes both universities and polytechnics. There has been checks every two years from since up to 2015, when the final implementation was declared to be finished. (EHEA Finland, n.d.; EHEA Report, 2003).

Development related to the second-cycle degree in universities of applied sciences was focused after fully adapting to European Credit Transfer and Accumulation System (ECTS). Secondary objective was to strengthen bachelor's degree status, the implementation of master's degree programmes, the promotion of domestic and international mobility (Finnish Higher Education Evaluation Council, 2012, 203).

Bologna Process also demanded reformation for finnish legislation to enable the two-cycle degree structure and international comparability of the Finnish education system. Comparable two-cycle structure is the operational objective of the Bologna Process (Finnish Higher Education Evaluation Council, 2012, 203).

Bologna Process is described in cycles. The first cycle is bachelor level degree, and second cycle is master level degree, and the third cycle is for doctoral degree. Cycles are similar to former Finnish education system where there's universities and universities of applied sciences. University studies represents integrated master studies, which forms from first and second cycles. Bologna Process is concentrating on the first two cycles.

2.3 Cybersecurity as a field of education

Cybersecurity is the art of protecting networks, data and devices from criminal use or unauthorized access and the practice of ensuring confidentiality, integrity, and availability of information (What is cybersecurity?, 2019).

Developing a concept of cybersecurity as a workforce began in 2010, more about this in topic of NICE Framework and the demand for education as a field has grown fast in 2018 there was already a study which reviewed and analysed master's programmes on cybersecurity. There were 21 selected programs, focusing on the contents of their courses, structure, admission requirements, requirements for completion, evolution and duration (NICE Website, n.d.; Cabaj, Domingos, Kotulski & Respício, 2018).

Finland

The Security Committee of Finland was established in February 2012 and started it's working 2013 releasing a "Program for The Implementation of The National Cybersecurity Strategy" on March 2013 (The Security Committee, 2013).

According to cybersecurity strategy Finland should be a global pioneer in preparing for and responding to cyber threats in management by 2016. The strategy defines objectives and policies to meet the criteria, it includes vision operating model and strategic guidelines. The strategy calls for a national cybersecurity implementation program (The Security Committee, 2013).

On international forums, Finland's reference group on political issues is other countries which emphasize human rights, democracy, and the rule of law, especially at Nordic countries and European Union. Finland on cybersecurity issues accordance with OSCE, UN, NATO and other international organisations and processes. Important for Finland is to support strengthening of EU's common policies in cybersecurity strategy which includes the cyber strategy work of EU (The Security Committee, 2013).

Education, research, and business have important role to play in developing and maintaining cybersecurity. Many measures presented in the implementation program aim for solutions that promote cybersecurity, business opportunities and co-operation between authorities and companies in Finland. Companies which are essential for the vital functions of society also develop their cybersecurity as part of their risk and continuity management measures and in co-operation with the security of supply organisation. Research and education are central to the continuous development of cybersecurity and the dissemination of information widely in society. Strengthening of

expertise supports the achievement of the goals of the government program and the cybersecurity strategy (The Security Committee, 2013).

Jyväskylä and Turku organised master's program on cybersecurity as a degree program. Master's program in Jyväskylä began in 2014 and 2011 in Turku. Both Jyväskylä and Turku started by accepting 20 students each for each starting group. On that point other universities in Finland had cybersecurity-related studies as a minor or part of other studies. (Pelkonen et al., 2016).

2.4 Government Decree on Universities and Universities of Applied Sciences

Ministry of Justice in Finland maintains *legislative* documentation for Government Decree on Universities and Universities of Applied Sciences. According to law mission of the scientific universities of Finland is to freely further scientific research, provide scientific education and civilize artistically and act in interaction with the society. On applied sciences universities the mission is to practice research, development, innovation, and artistic actions to improve work life and regional development by the law (University government decree, 2004; University law, 2009).

Ministry of Education and Culture in Finland maintains the regulative documentation for Government Decree on Universities of Applied Sciences and Universities. Relevant topics of documentation is that this documentation maintains and points the structure of studies and the scope of studied workload included. Depending on studies leading to a bachelor's degree in University of Applied Sciences are 180, 210, 240, or 270 credits. The scope of studies leading to master's degree is either 60 or 90 credits. Thesis is part of structure of the studies and the workload is determined in university government decree law. Bachelor's degree must include thesis which is 6 credits on minimum and 10 credits on maximum. Master's degree must include thesis which is 20 credits on minimum and 40 credits on maximum. (Ministry of Education and Culture, 2014; University government decree, 2004)

European Credit Transfer and Accumulation System (ECTS) is coordinated by The European Commission and the guide has been adopted by Ministers for Higher Education of the European Higher Education Area in 2015. ECTS credits express the relation between learning outcomes and the workload. ECTS guide determines academic full-time workload to be 60 credits. Workload ranges between 1,500 to 1,800 hours for academic year, therefore one (1) credit corresponds from 25 to

30 hours of work. In Finland Ministry of Education and Culture has adapted this model for 60 credits to correspond 1,600 hours of average workload, this roughly translates into 27 hours of workload for a full earned credit. (European Commission 2015; Ministry of Education and Culture, 2014)

2.4.1 European Qualifications Framework (EQF)

European Qualifications Framework (EQF) is a framework to appreciate skills and qualifications with the common understanding. Qualifications express what is the learner's knowledge, understanding and capabilities. Qualifications can be, for example, certificates or university diplomas (European Qualifications Framework, 2018):

> "Transparency about what people actually learned in order to obtain a qualification ('learning outcomes') is key to ensuring that individuals, employers and education and training providers give the appropriate economic, social and academic value to qualifications." (*European Qualifications Framework, 2018).*

The European Qualifications Framework is reaching towards transparency, comparability and portability of qualifications. Framework can be used between different qualifications and their corresponding levelling systems. EQF defines a qualification outcome with achieved learning outcomes against given standards and is a common reference to compare qualifications between countries. EQF supports lifelong learning and development within Europe (European Qualifications Framework, 2018).

EQF is defined by eight learning outcomes-based levels which represents the expectations of knowledge, skills, autonomy, and responsibility. Levels progress from level 1 to level 8. Learning outcome descriptors reflect two dimensions: Learning domains and levels. Level dimensions grow up by complexity of the learning outcomes. Learning domains bend between knowledge, skills, and autonomy and responsibility, this allows different types of qualifications to be classified at the same level, these levels can be seen from table 1 which is directly adapted from EQF documentation (European Qualifications Framework, 2018).

Table 1 European Qualification Framework levels (Council of the European Union, 2017).

Levels	Knowledge	Skills	Responsibility and autonomy
Level 1	Basic general knowledge	Basic skills required to carry out simple tasks	Work or study under direct supervision in a structured context
Level 2	Basic factual knowledge of a field of work or study	Basic cognitive and practical skills required to use relevant information in order to carry out tasks and to solve routine problems using simple rules and tools	Work or study under supervision with some autonomy
Level 3	Knowledge of facts, principles, processes and general concepts, in a field of work or study	A range of cognitive and practical skills required to accomplish tasks and solve problems by selecting and applying basic methods, tools, materials and information	Take responsibility for completion of tasks in work or study. Adapt own behaviour to circumstances in solving problems
Level 4	Factual and theoretical knowledge in broad contexts within a field of work or study	A range of cognitive and practical skills required to generate solutions to specific problems in a field of work or study	Exercise self-management within the guidelines of work or study contexts that are usually predictable, but are subject to change. Supervise the routine work of others, taking some responsibility for the evaluation and improvement of work or study activities
Level 5	Comprehensive, specialised, factual and theoretical knowledge within a field of work or study and an awareness of the boundaries of that knowledge	A comprehensive range of cognitive and practical skills required to develop creative solutions to abstract problems	Exercise management and supervision in contexts of work or study activities where there is unpredictable change. Review and develop performance of self and others
Level 6	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
Level 7	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	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

	field and at the interface between different fields		
Level 8	Knowledge at the most advanced frontier of a field of work or study and at the interface between fields	The most advanced and specialised skills and techniques, including synthesis and evaluation, required to solve critical problems in research and/or innovation and to extend and redefine existing knowledge or professional practice	Demonstrate substantial authority, innovation, autonomy, scholarly and professional integrity and sustained commitment to the development of new ideas or processes at the forefront of work or study contexts including research

EQF can be used by various users, for individual it helps to achieve learning and employment careers to match stakeholders needs, who can treat Europe as a single qualification area, that helps mobility inside the labour market (European Qualifications Framework, 2018).

2.4.2 International Standard Classification of Education (ISCED)

United Nations Educational, Scientific and Cultural Organization (UNESCO) has been active since 1946 and currently has 195 Member States. The UNESCO Institute for Statistics (UIS) was established in 1999 and it is the statistical office of UNESCO and is the UN depository for global statistics in the field of education, culture and communication, science, and technology (ISCED 2011, 2012).

International Standard Classification of Education (ISCED) was initially designed to solve the problem of national education systems to vary on benchmarking the performance and creating a framework to be used to categorise and report cross-nationally comparable education statistics. Initially developed 1970s, and first revised in 1997 and on revision 2011 (ISCED 2011, 2012).

ISCED uses cross-classification with two classifications, a level of education and a field of education while using education and qualifications mapping components, concepts and definitions, and classification system. Education qualifications can be obtained various ways, for example, full education or acquiring competencies. ISCED includes formal and non-formal education. Levels, programmes and qualifications have more detailed complex depths which covers programme orientation, level completion, access to higher level, and position in national degree and qualification structure. Levels represent complexity and specialisation of chosen education. There are

many ways to travel from level nil or one up to eight, person may choose or affect the path leading up to target level (ISCED 2011, 2012).

Programme orientation is built-in within levels two to five, so it is possible to use on levels six to eight. Orientation splits between general education and vocational education. General education is teaching literacy and numeracy and developing knowledge, skills, and competencies. General education provides possibility to entry into vocational education but do not prepare for occupation nor lead toward a labour market-relevant qualification. Vocational education leads towards knowledge, skills, and competencies for a specific occupation. Completing such programmes leads to a labour market-relevant, vocational qualifications (ISCED 2011, 2012).

Education programme completion requires attendance requirements, demonstrated acquisition of expected knowledge, skills, and competencies. Final, curriculum-based examination or series of examinations and accumulating required number of credits are needed for validation (ISCED 2011, 2012).

Levels one and two do not always concluded with a qualification. Successful completion of programmes at levels one to three is always considered as level completion when the qualification is obtained which provides access to higher ISCED level. Successful completion of program at levels 2 or 3 which do not give access to programmes at higher ISCED level is considered as level completion or partial level completion (ISCED 2011, 2012).

Typical ranges of duration of levels are used to classifying formal education programmes (ISCED 2011, 2012):

- Level 0: No duration criteria
- Level 1: Duration typically from 4 to 7 years. Most commonly 6 years.
- Level 2: Duration typically from 2 to 5 years. Most commonly 3 years.
- Level 3: Duration typically from 2 to 5 years. Most commonly 3 years.
- Level 4: Duration typically from 0,5 to 3 years.
- Level 5: Duration typically from 2 to 3 years.
- Level 6: Duration typically from 3 to 4 years. Most commonly 6 years.
    - When following another ISCED level 6 from 1 to 2 years.
- Level 7: Duration typically from 1 to 4 years.
    - When directly from ISCED level 3 from 5 to 7 years.
- Level 8: Duration minimum of 3 years.

To accurately measure enrolment, students must be assigned to ISCED level, category and sub-category. ISCED classification consists of parallel coding schemes for education programmes and levels of educational attainment as seen from tables 2, 3 and 4 which are directly quoted from ISCED documentation (ISCED 2011, 2012).

Table 2 ISCED coding of levels (first digit) (ISCED 2011, 2012).

ISCED-Programmes (ISCED-P)		**ISCED-Attainment (ISCED-A)**	
0	Early Childhood education	0	Less than primary education
1	Primary education	1	Primary education
2	Lower secondary education	2	Lower secondary education
3	Upper secondary education	3	Upper secondary education
4	Post-secondary non-tertiary education	4	Post-secondary non-tertiary education
5	Short-cycle tertiary education	5	Short-cycle tertiary education
6	Bachelor's or equivalent level	6	Bachelor's or equivalent level
7	Master's or equivalent level	7	Master's or equivalent level
8	Doctoral or equivalent level	8	Doctoral or equivalent level
9	Not elsewhere classified	9	Not elsewhere classified

Table 3 ISCED coding of categories (second digit) (ISCED 2011, 2012).

ISCED-Programmes (ISCED-P)		**ISCED-Attainment (ISCED-A)**	
0	Not further defined	0	Not further defined
1	Early childhood educational develop-ment	1	Never attended an education pro-gramme
2	Pre-primary education	2	Some early childhood education
3	Not used	3	Some primary education (without completion of ISCED level 1)

4	General / academic	4	General / academic
5	Vocational / professional	5	Vocational / professional
6	Orientation unspecified	6	Orientation unspecified
7	Not used	7	Not used
8	Not used	8	Not used
9	Not elsewhere classified	9	Not elsewhere classified

Table 4 ICED coding of sub-categories (third digit) (ISCED 2011, 2012).

ISCED-Programmes (ISCED-P)		**ISCED-Attainment (ISCED-A)**	
0	Not further defined	0	Not further defined
1	Recognised successful completion of programme is insufficient for completion or partial completion of level	1	Partial level completion without direct access to programmes at higher levels
2	Recognised successful completion of programme is sufficient for partial completion of level but without direct access to programmes at higher levels	2	Level completion without direct access to programmes at higher levels
3	Recognised successful completion of programme is sufficient for completion of level but without direct access to programmes at higher levels	3	Level completion with direct access to programmes at higher levels
4	Recognised successful completion of programme is sufficient for completion of level and with direct access to programmes at higher levels	4	Not used
5	First degree programme – Bachelor's or equivalent level	5	Not used
6	Long first-degree programme – Bachelor's or Master's, or equivalent level	6	Not used
7	Second or further degree programme,	7	Not used

	following a bachelor's or equivalent programme		
8	Second or further degree programme, following a master's or equivalent pro-gramme	8	Not used
9	Not elsewhere classified	9	Not elsewhere classified

These levelling combined with category and sub-category system can be used to show an example of higher education tertiary education pathways in ISCED, see figure 2.

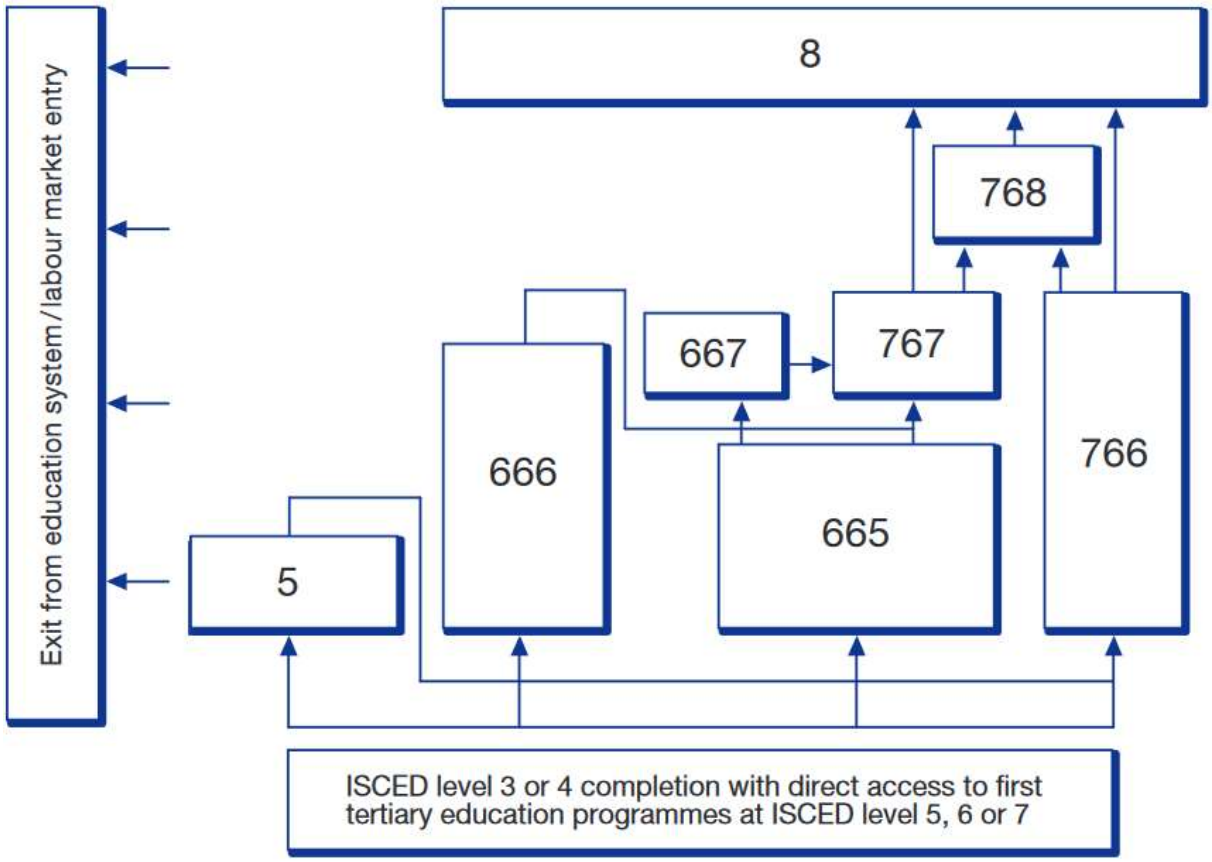

Figure 2 Tertiary education pathways in ISCED (ISCED 2011, 2012).

To breakdown these specific levels with subcategories are listed in table 5 which is directly adapted from ISCED documentation.

Table 5 Categories example relating to figure 2.

Category (orientation)		Sub-category (duration/position)	Description
5	Short-cycle tertiary education		
66	Bachelor's or equivalent level, orientation unspecified	665	First degree (3-4 years)
		666	Long first degree (more than 4 years)
		667	Second or further degree, following successful completion of bachelor's or equivalent programme
76	Master's or equivalent level, orientation unspecified	766	Long first degree (at least 5 years)
		767	Second or further degree (following successful completion of a bachelor's or equivalent programme)
		768	Second or further degree (following successful completion of a master's or equivalent programme)
8	Doctoral or equivalent level		

ISCED is used widely and the version 2011 has quite differences when speaking of levelling system, in table 6 which is directly adapted from ISCED documentation the differences of ISCED 2011 and ISCED 1997 are listed.

Table 6 Correspondance between ISCED 2011 and ISCED 1997 levels (ISCED 2011, 2012).

ISCED 2011	**ISCED 1997**
ISCED 01	-
ISCED 02	ISCED 0
ISCED level 1	ISCED level 1
ISCED level 2	ISCED level 2

ISCED level 3	ISCED level 3
ISCED level 4	ISCED level 4
ISCED level 5	ISCED level 5
ISCED level 6	
ISCED level 7	
ISCED level 8	ISCED level 6

2.5 Taxonomy Frameworks

Dictionary Merriam-Webster (n.d.) states "that taxonomy is the study of the general principles of scientific classification especially orderly classification of plants and animals according to their presumed natural relationships".

Taxonomy frameworks used in this analysis were National Initiative for Cybersecurity Education (NICE) framework and European Cybersecurity Taxonomy. Other similar frameworks do exist. NICE frameworks seem to be most used one for describing workforce correlation with skills, knowledge, and abilities.

2.5.1 NICE framework

The concept for the National Initiative for Cybersecurity Education (NICE) Framework began before the establishment of NICE in 2010 and has been focusing since 2011 defining the NICE Cybersecurity Workforce Framework (NCWF) to provide the common language to define cybersecurity skills, tasks, and requirements. The first version was posted in September 2012. After first reviews from U.S. government-wide review noted specific areas to be examined and refined was noticed and second version 2.0 was published in 2014. The Office of the Secretary of Defence (OSD) expanded on version 2.0 through internal and external engagements. The Department of Homeland Security (DHS) and NIST co-authors worked together with OSD and third version was published on august 2017. NICE convened a Core Authoring Team including numerous departments and agencies in U.S. they began with revisions and got responses from a Request for Comments and updated the NICE Framework to improve agility, flexibility, interoperability, and modularity. Forth and the current version was published November 2020 (NICE Website, n.d.).

NICE approach does not define security as a monolithic field nor a single profession, it in holds full assortment on required task and knowledge, skills, and abilities competencies for specialty areas and functions. NICE framework demonstrate authoritative and standard cybersecurity knowledge and competencies for a area of interest. NICE model represents the accepted definition of cyber-security work (Shoemaker D., Kohnke A., Sigler K., 2016).

Cybersecurity is an emerging profession, fifteen years ago, the notation of workforce dedicated only for cybersecurity of ICT assets would be unheard of. If the cybersecurity teaching would be in diverse places on campus, we are not getting coherent message, let alone evolve the field into a mature discipline. The NICE Framework has taken step in providing that definition with the publi-cation of NICE National Cybersecurity Workforce Framework. The framework is intended to be applied in the public, private, and academic sectors (Shoemaker D., Kohnke A., Sigler K., 2016).

Framework specifies a comprehensive set of generic tasks and knowledge, skills, and abilities re-quirements for cybersecurity. Advantage of broad range of generic practices is that companies whose personnel have been trained in them can be confident that effective security exists in their organisation to the level of that employee. Disadvantage of such wide range is that set of practices rests with the level of detail they have been described at (Shoemaker D., Kohnke A., Sigler K., 2016).

In the current version revision 1 of NICE Framework the previously used knowledge, skills, and abilities have compromised of tasks, knowledge, and skills. Revision 1 presents streamlined set of “building blocks” among tasks, knowledge, and skills. Relationships among tasks, knowledge, skills, and abilities have also changed (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020).

The main building blocks are tasks, knowledge, and skills statements. There are two generic terms for organisations used: “the work” and “the learner”, see figure 3 (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020).

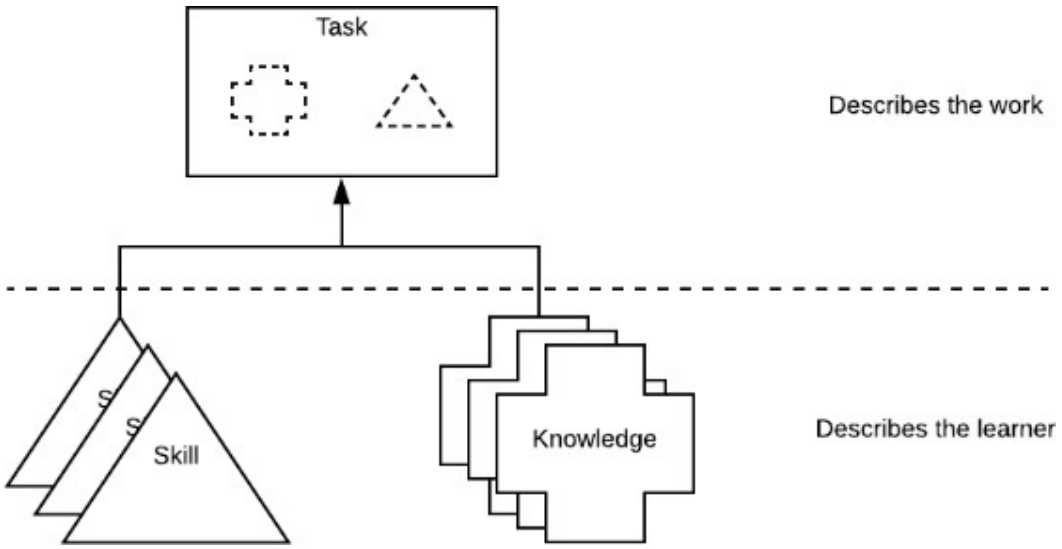

Figure 3 NICE Framework buiding blocks (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020).

Work defines the needs to achieve risk management objectives, to describe work framework provides knowledge and skill statements. Learner is a person who opposes a set of knowledge and skills. A learner does not have to be a student, but is a term to used for a person that can acquire new knowledge and skills. By describing both the work and the learner framework provides a common language to describe cybersecurity work and workforce. Furthermore, this provides a mechanism to communicate across organisations using same building blocks (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020).

Task statements focus on the organisational language and communication patterns to provide value to the organisation. Tasks describe work, a task can be defined as activity toward achievement of objectives, which should be straightforward. Complexity of a task is explained with knowledge and skill statements (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020).

Knowledge statements describes the understanding needed to complete the task. Knowledge is defined as a retrievable set of concepts within individuals' memory. Tasks might need multiple knowledge statements, which can be either foundational or specific (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020).

Skill statements demonstrates a skill of learner on performing task statements. A learner who fails to demonstrate the describe skill would not be able to perform a task which relies on that skill. Tasks might require multiple skill statements and they can be either simple or complex (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020).

Competencies provides a mechanism to assess the learners. Competencies are defined through employer-driven approach and allow education and training providers to be responsive for sector needs. One way to use competencies is to use them as a part of hiring process. Organisation could then use competencies to assess whether a candidate can perform those tasks, see the example from figure 4 (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020).

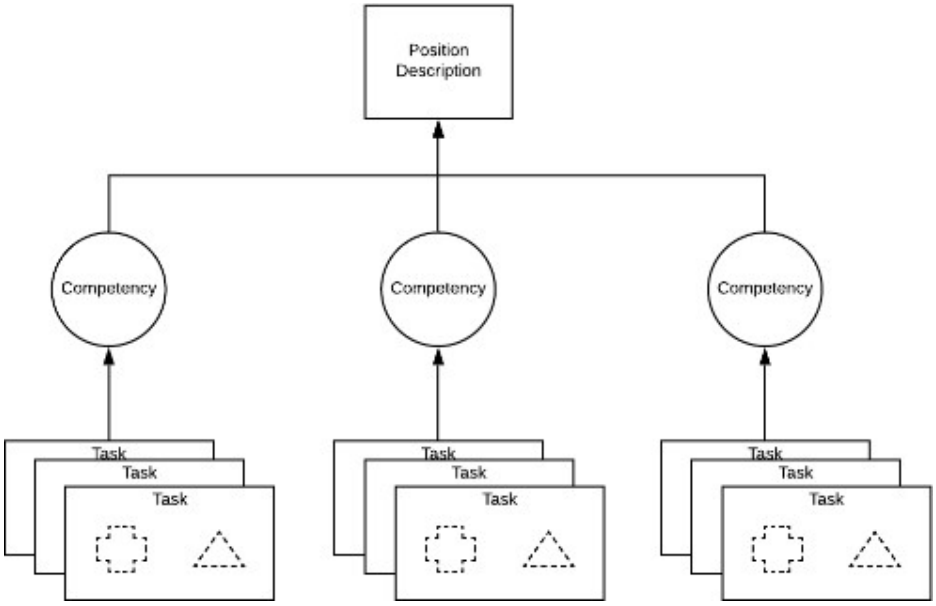

Figure 4 Using competencies to assess learners through a position description (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020).

Another way is to use competencies to determine whether a learner has achieved defined set of skills and knowledge. Assessment could take the form of tests, lab-based demonstration, or oral evaluations, see figure 5. (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020).

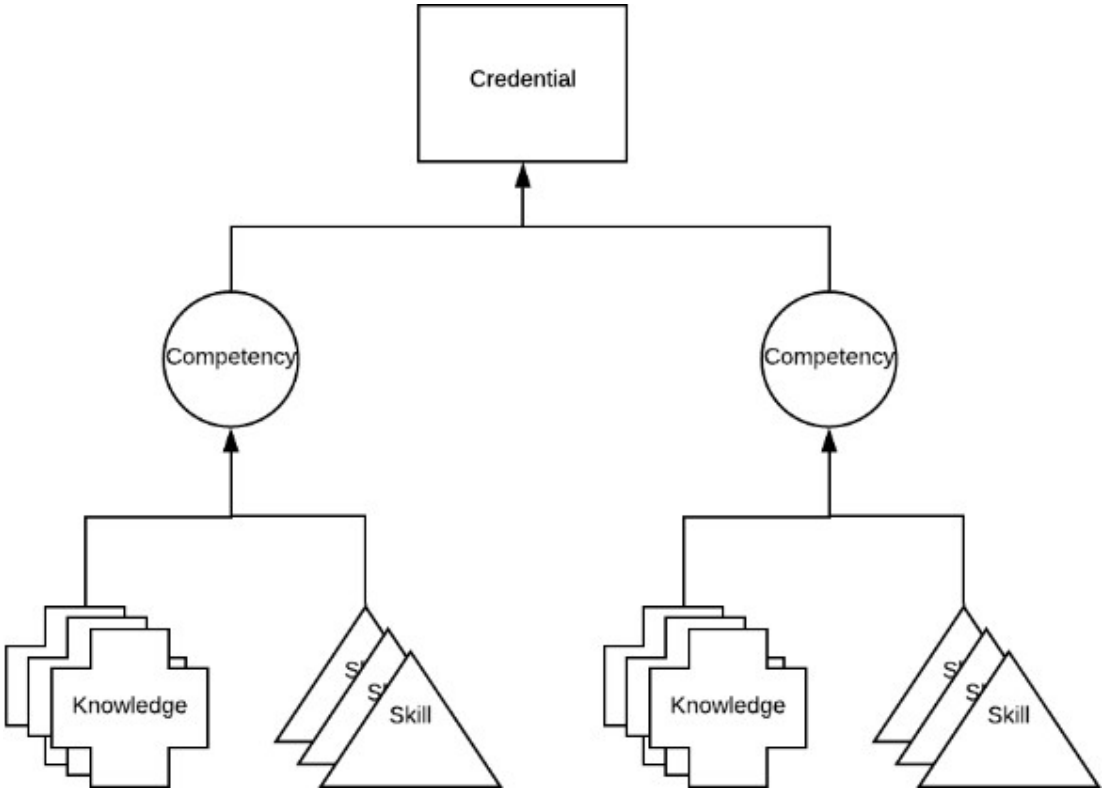

Figure 5 Using competencies to assess learners through a credential (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020).

Work roles are common use case of the NICE framework. Work roles can be used to describe a grouping of someone's responsible or accountable work. Work roles include a set of tasks which are required for the work to be done. Tasks includes a corresponding set of knowledge and skill statements for chosen task, this supports and simplifies communication, see figure 6 (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020).

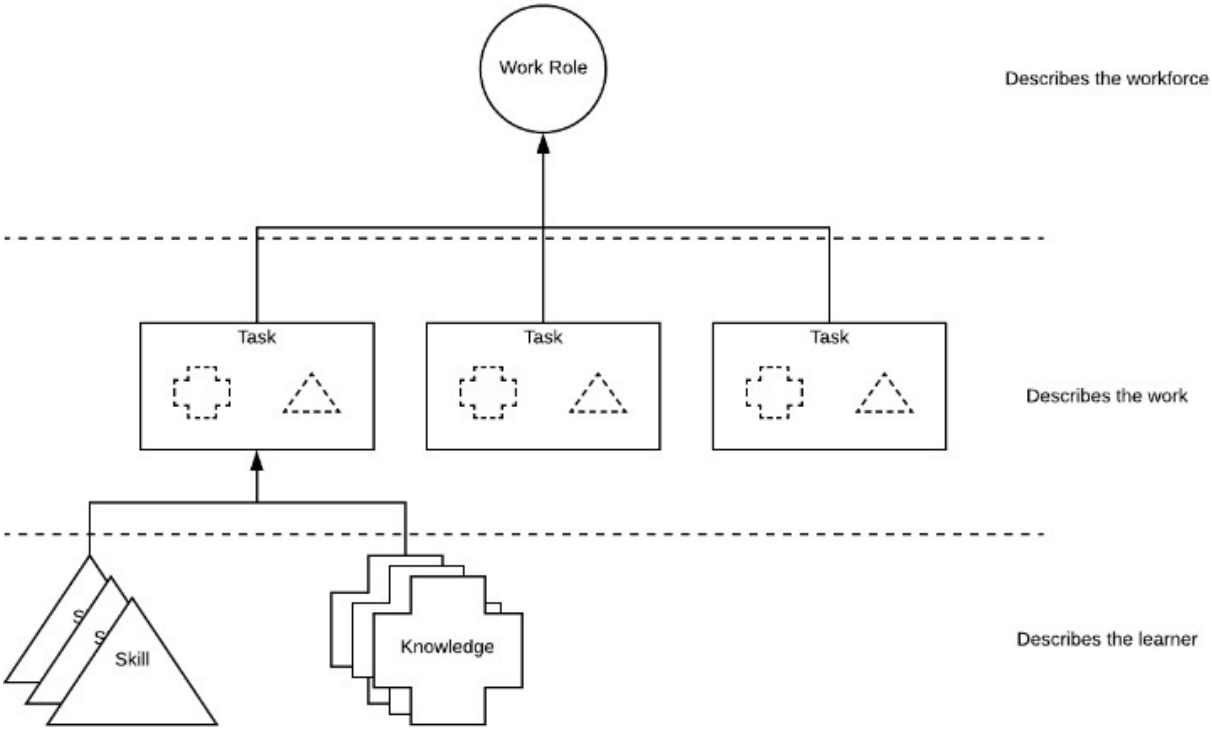

Figure 6 Work roles' relationship to building blocks (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020).

Work roles are not synonymous with job titles. Some jobs may and most likely contain multiple work roles, work roles also are not synonymous with occupations. A simple example would be work role “software developer”, which could be part of job titles like “software engineer, application developer, etc.”. It is good to note that NICE Framework does not define proficiency levels (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020).

Using NICE Framework there is an option to create new task, knowledge, and skill statements and new competencies and new work roles. However, if one is to use the current Framework status using existing ones can be browsed from NICE Framework resource center (Petersen R., Santos D., Smith M., Wetzel K., Witte G., 2020).

Now we have approached the NICE Framework from perspective of individual, on the original NIST Special Publication 800-181 we can approach the NICE Framework from cybersecurity fields, by naming categories, speciality areas and then come to the meeting point on the work roles.

Framework offers seven categories which provide the overarching organisational structure of the framework. Categories are composed from thirty-two speciality areas which contains one or more work roles. This structure group together work and workers that share common major functions, regardless of occupational terms or job titles. This grouping of these components is done like shown in figure 7 and described in table 7 which are directly adapted from NIST documentation (Newhouse W., Keith S., Scribner B., Witte G., 2017).

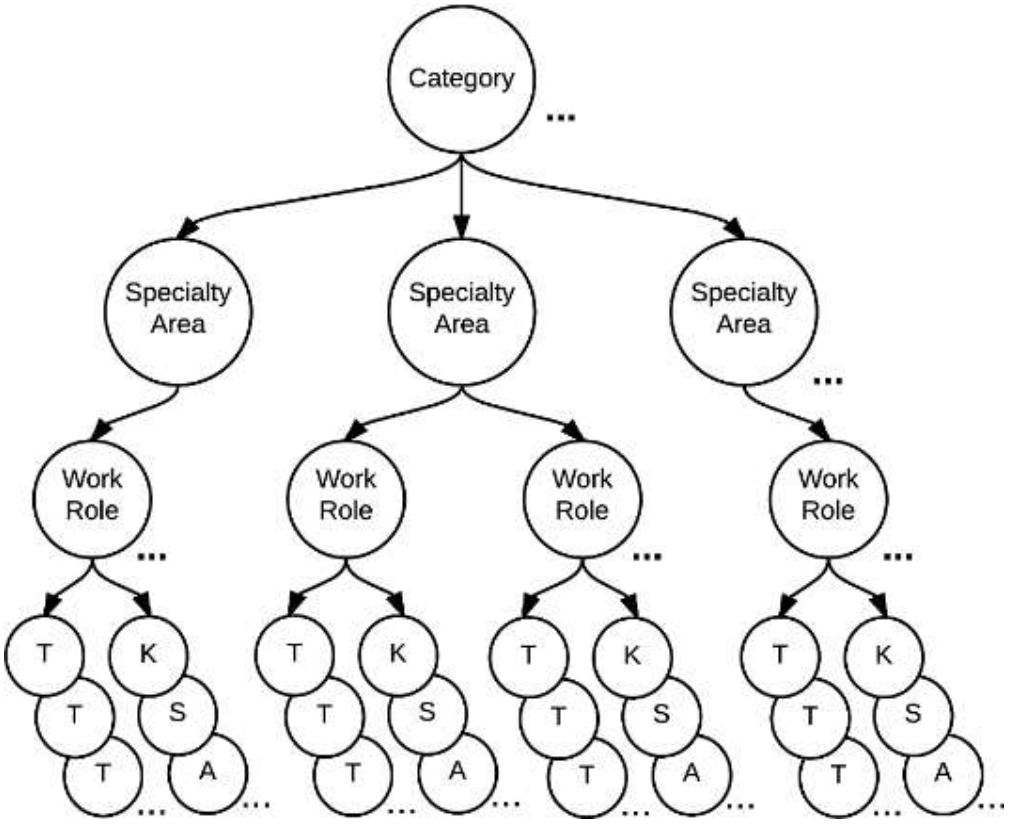

Figure 7 Relationships among NICE Framework components (Newhouse W., Keith S., Scribner B., Witte G., 2017).

NICE Framework elements

Table 7 NICE Framework workforce categories (Newhouse W., Keith S., Scribner B., Witte G., 2017).

Categories	Descriptions

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, analyzes, 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 technology (IT) systems, networks, and digital evidence.

Each category has from two up to seven speciality areas, also each area has deeper description, but since these are not used in the analysis, only listing provided here. Full descriptions on the speciality areas and work roles can be found from appendix 3.

NIST Special Publication 800-181 (Newhouse W., Keith S., Scribner B., Witte G., 2017) includes total of 176 listed abilities, 374 skills, 630 knowledge, and 1007 task statements. Full listing can be found from mentioned documentation or from reference spreadsheet's corresponding tabs. Three examples from each listed in table 8 examples are directly adapted from NIST documentation.

Table 8 NICE Framework tasks, knowledge, skills, and abilities examples table

Task, Knowledge, Skills, Abilities ID	**Description**
T0397	Perform Windows registry analysis
T0548	Provide advice and input for Disaster Recovery, Contingency and Continuity of Operations Plans
T0898	Establish an internal privacy audit program
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies
K0188	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro)
K0268	Knowledge of forensic footprint identification
S0025	Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort)
S0091	Skill in analyzing volatile data
S0248	Skill in performing target system analysis
A0010	Ability to analyze malware
A0036	Ability to identify common coding flaws at a high level
A0105	Ability to tailor technical and planning information to a customer's level of understanding

2.5.2 The European Cybersecurity Taxonomy

European Commission proposed in 2018 a regulation setting up a European cybersecurity industrial, technology and research centre with a network of national coordination centres. Four pilot projects were requested and one of these was proposed taxonomy. Ideology reflects on different dimensions of cybersecurity domain, and using widely accepted standards as sources, international working group classification systems, regulations, best-practices, and recommendations. High level set of definitions and categorisation can be used to index the cybersecurity research entities (Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M., Lazari, A., 2019).

Methodology of taxonomy follow detailed steps shown in figure 8. Defining the subject scope of European cybersecurity taxonomy is providing definition of the cybersecurity context, its domains of application, research and knowledge. Identifying sources that are widely adopted and recognised by scientific and technological community. Collecting terms and concepts. Grouping similar clustered concepts together. Adding other relationship and details to identify and simplify the structure of the taxonomy, resulting a three-dimensional taxonomy (Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M., Lazari, A., 2019).

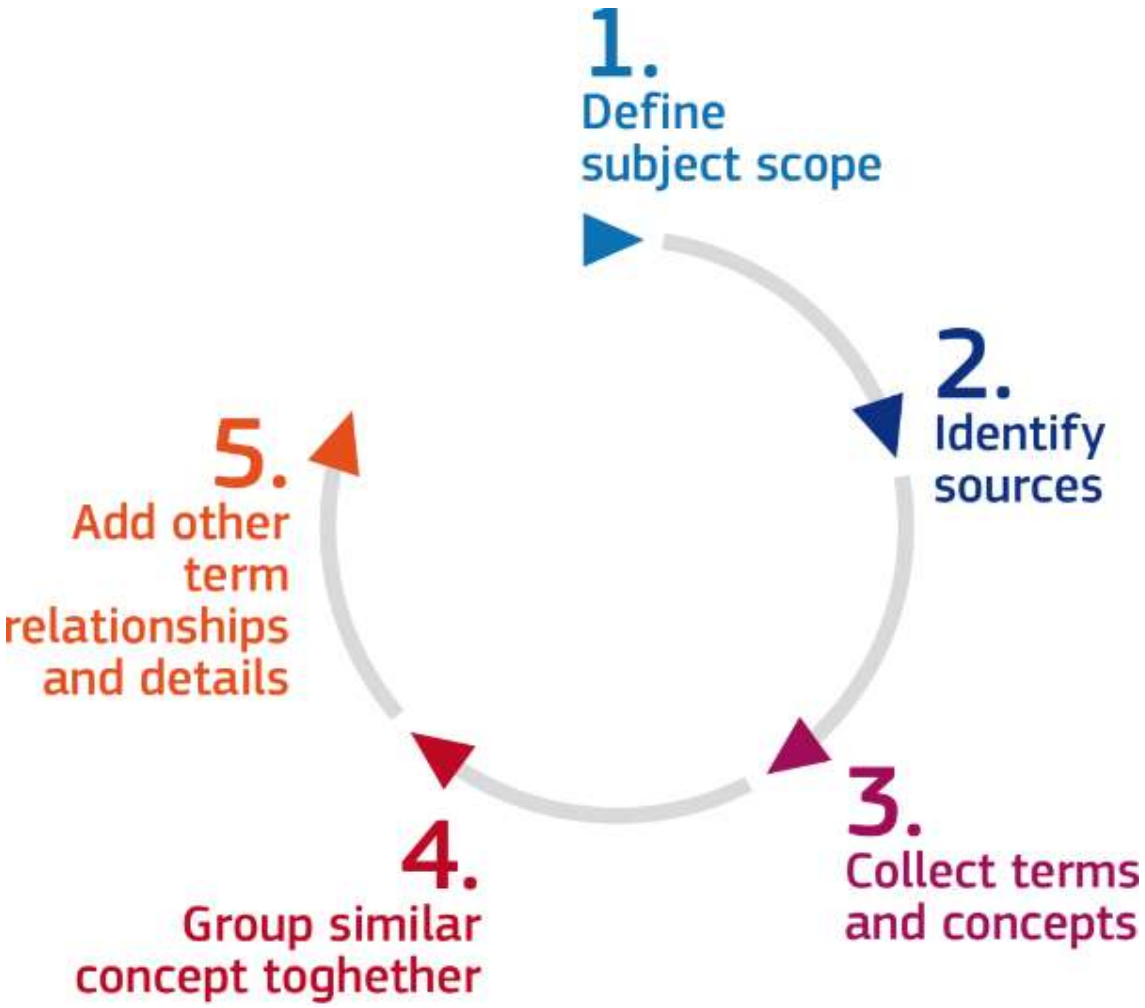

Figure 8 European Cybersecurity Taxonomy definition steps (Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M., Lazari, A., 2019).

European cybersecurity taxonomy has been grouped or formed from following existing clustering approaches: Cyberwatching, ACM Classification System, NIST CSRC Taxonomy, IEEE Taxonomy, ETSI TC-Cyber working groups domains, IFIP TC11 Working Groups taxonomy, IT-baseline protection catalog (IT-Grundschutz) and by using following international standards and reference documents ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27005, ISA 62443, ISO/IEC 15408 and NIST SP 800. Other international working groups and organisations are a source for the European cybersecurity taxonomy: Internet Engineering Task Force (IETF): Request for Comments (RFC) 4949 “internet Security Glossary, Version 2”, Intel Threat Agent Library (TAL) and Threat Agent Motivation, MACE Taxonomy, Adversary Types, CAPEC ATT&CK from Mitre, Cyber Kill Chain. Furthermore, Tallinn Manual on the International Law Applicable to Cyber Warfare prepared by the NATO Cooperative

Cyber Defence Centre of Excellence, Open Web Application Security Project Foundation (OWASP), Information Systems Audit and Control Association (ISACA), European Union Agency for Network and Information Security (ENISA), NATO Cooperative Cyber Defence Centre of Excellence (CCD-COE) and European Cyber Security Organisation (ECSO) (Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M., Lazari, A., 2019).

Mentioned sources provide terms for sub-domains and a set of applicable sectors. However, there was some general considerations on many sources and much of overlapping. Contributions for the cybersecurity taxonomy can be seen from table 9 (Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M., Lazari, A., 2019).

Table 9 Sources of contributions to the cybersecurity taxonomy (Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M., Lazari, A., 2019).

Source	General concepts	Academic Research	Regulatory	Operational	Sectorial	Application	Economic and Business	Social	Standards	Vocabulary
Cyberwatching	x	x		x						
ACM Classification System	x	x				x	x	x		
NIST CSRC Taxonomy	x	x	x	x	x	x	x	x		
IEEE	x	x								
ETSI TC-Cyber	x	x		x					x	
IFIP WG 11	x	x				x	x	x		
IT-Grundschutz	x	x				x				
International Standards (Section 2.2)	x		x	x	x	x			x	x
OWASP	x									x
ENISA reports	x		x	x	x					x
ECSO	x					x	x			
EU Regulations (see Section 2.2.4)	x		x	x	x	x		x	x	x
PWC Study						x	x			
SEREMA						x	x			
CGP						x	x			

The goal of the European taxonomy is to support European cybersecurity competencies available, not for the products, services, or processes including operational activities. While having complicated and multidimensional representation of the discipline leads towards the proposed three-dimensional way. Three-dimensional high-level view can be seen from figure 9 (Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M., Lazari, A., 2019).

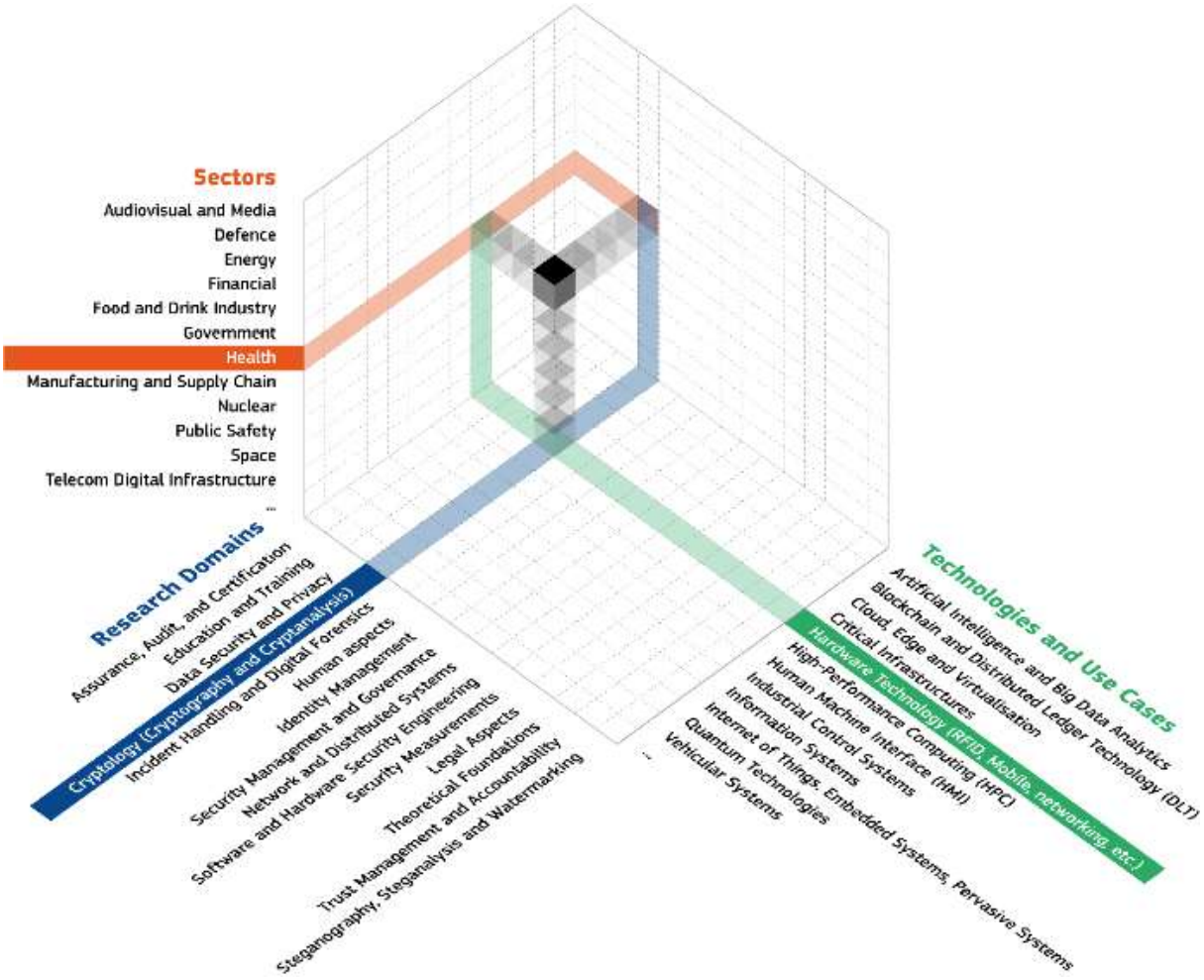

Figure 9 High Level view of the European Cybersecurity Taxonomy (Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M., Lazari, A., 2019).

The European Cybersecurity Taxonomy domains

Research domains represent areas of knowledge, intended to cover different areas including human, legal, ethical and technological aspects. The following listing has listed domains, more de-

tailed listing can be found from appendix 3, which includes their corresponding subdomains (Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M., Lazari, A., 2019).

- Assurance, Audit and Certification
- Cryptology (Cryptography and Cryptanalysis)
- Data Security and Privacy
- Education and Training
- Human Aspects
- Identity Management
- Incident Handling and Digital Forensics
- Legal Aspects
- Network and Distributed Systems
- Security Management and Governance
- Security Measurements
- Software and Hardware Security Engineering
- Steganography, Steganalysis and Watermarking
- Theoretical Foundations
- Trust Management and Accountability

The European Cybersecurity Taxonomy sectors

Another dimension is sectors which "are proposed to highlight the need for considering different requirements and challenges" in scenarios, such as energy, transport or health sector. List of sectors proposed for cybersecurity taxonomy can be seen below (Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M., Lazari, A., 2019).

- Audiovisual and media
- Chemical
- Defence
- Digital Services and Platforms
- Energy
- Financial
- Food and drink
- Government
- Health
- Manufacturing and Supply Chain
- Nuclear
- Safety and Security
- Space
- Telecomm Infrastructure
- Transportation

The European Cybersecurity Taxonomy technologies and use cases

Last dimension is technologies and use cases which represent the technological enablers to enhance the development of different sectors. Following list describes the technologies and use cases dimensions (Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M., Lazari, A., 2019).

- Artificial intelligence
- Big Data
- Blockchain and Distributed Ledger Technology (DLT)
- Cloud, Edge and Virtualisation
- Critical Infrastructure Protection (CIP)
- Protection of public spaces
- Disaster resilience and crisis management
- Fight against crime and terrorism
- Border and external security
- Local/wide area observation and surveillance
- Hardware technology (RFID, chips, sensors, networking, etc.)
- High-performance computing (HPC)
- Human Machine Interface (HMI) e
- Industrial IoT and Control Systems (e.g. SCADA and Cyber Physical Systems – CPS)
- Information Systems
- Internet of Things, embedded systems, pervasive systems
- Mobile Devices
- Operating Systems
- Quantum Technologies (e.g. computing and communication)
- Robotics
- Satellite systems and applications
- Vehicular Systems (e.g. autonomous vehicles)
- UAV (unmanned aerial vehicles)

2.5.3 Other frameworks

Similar frameworks on cybersecurity on the educational point of view is, for example, Association for Computing Machinery (ACM)'s Cybersecurity curricula 2017 with a report of Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity: A report in the Computing Curricula Series Joint Task Force on Cybersecurity Education, which aims for knowledge areas and learning outcomes which's structure can be linked to NICE Framework see figure 10 (Burley D., Bishop M., Kaza S., Gibson D., Hawthorne E., Buck S., 2017).

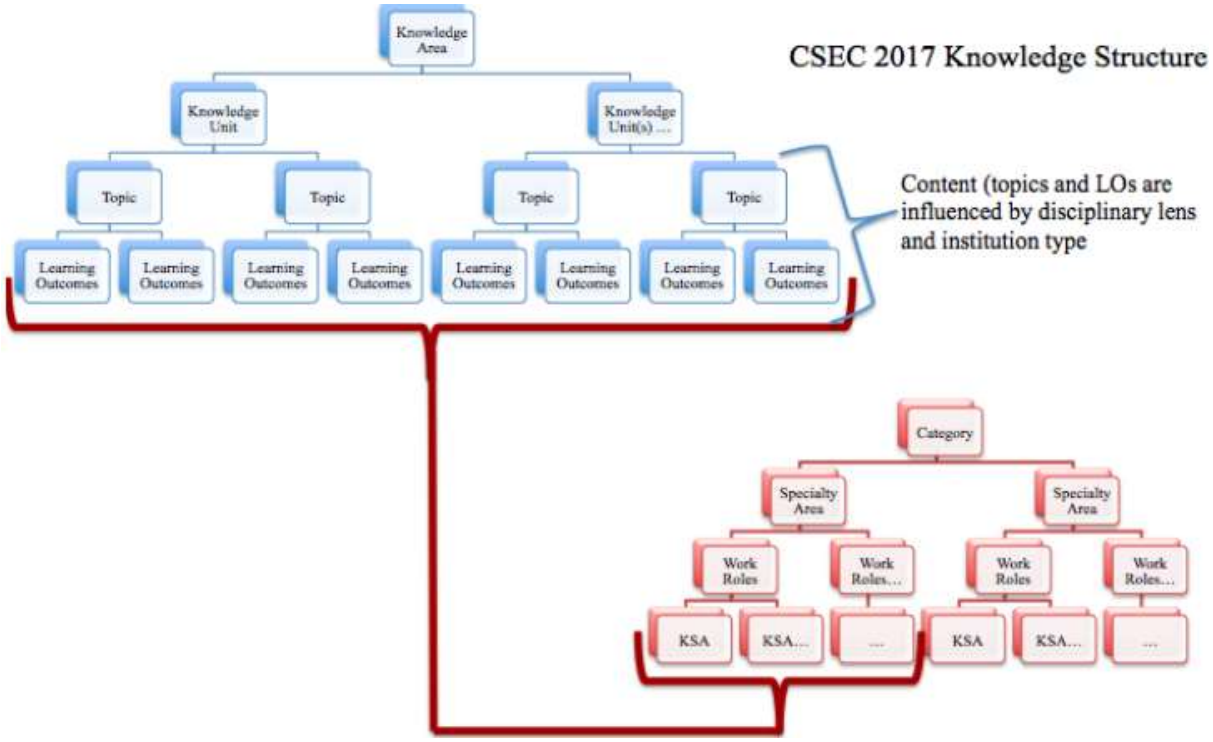

Figure 10 CSEC 2017 Knowledge struture linking with NICE Framework (Burley D., Bishop M., Kaza S., Gibson D., Hawthorne E., Buck S., 2017).

National Centers of Academic Excellence in Cybersecurity (CAE), has also a curricular program CAE-Cyber Defense (CAE-CD) which can also be mapped into NICE Framework and has similarity by using categories and knowledge units, more on this can be found from CAE Documentation with provided NICE knowledge unit mapping spreadsheet (CAE Documents Library, n.d.).

As mentioned in chapter 2.5.2. European Cybersecurity Taxonomy gathers elements from many different frameworks or taxonomies, which can be somewhat similar frameworks on their perspective, however designated workforce frameworks are not available so many and almost each time the topic is in workforce, taxonomy or categories they almost always reflect back to NICE Framework.

2.6 Related research

Saharinen, Backlund and Nevala (2020) researched topic assessing cyber security education through NICE cybersecurity workforce framework where they did quantitative research of the ed-

ucation curricula data mapped to NICE Cybersecurity Workforce Frameworks. Stange, Tucker, Tang, Servin and Geissler (2020) researched topic pre-bachelor's curricular guidance for cybersecurity programs, which included usage of NICE Framework for pre-bachelor's level of studies. Amir (2020) wrote a bachelor-level thesis topic developing cyber security competences using NICE KSAs in cyber ranges where NICE framework is taken in place from the point of knowledge, skills and abilities.

Saharinen, Karjalainen and Kokkonen (2019) researched design models for a degree programme in cybersecurity where they reflected the curriculum contents for industry's knowledge needs. Švábenský, Vykopal and Čeleda (2020) researched what are cybersecurity papers about, a systematic literature review of SIGCSE and ITiCSE conferences. This paper concentrates on the cybersecurity as a field of education and teaching.

The Finnish education field has also been researched. Savola (2017) delivered a short paper with the topic of current level of cybersecurity competence and future development: case Finland, which handled the curricular topic in the scope of Finland as a country. Lehto (2015) made an article on the topic of cyber security competencies: cyber security education and research in Finnish universities, where research was scoped for Finnish universities reflecting to Finland's Cyber Security Strategy (2013).

3 Article summary: Analysing Theses of Cyber Security Higher Education

The paper was submitted for the *The 7th IEEE Cyber Science and Technology Congress (CyberSciTech 2022)* conference. Original deadline of paper submission was June 1st, but the conference extended the paper submission dates, so this summary will be aimed for the polished later submission which had contributions from each authors, myself, Karo Saharinen and Tuomo Sipola. Submitted version can be found as appendix 4 on this documentation.

3.1 Purpose and Objective of the Article

The purpose of this article was to make an analysis on higher level cybersecurity theses and map them into NICE Framework categories and work roles while using European Cybersecurity Taxon-

omy to add industry sectors for dataset. After successful mapping of theses analysis can be done and results can be filtered by using any considered mapping used during this mapping phase.

Dataset was gathered by regional basis; theses were gathered from Jamk University of Applied Sciences and University of Jyväskylä. JAMK University of Applied Science theses were also divided between bachelor- and master-level theses.

For comparison, a few specific relations were taken for analysis. First overview was to see total of category division through the full dataset and another look for this by dividing these by education type (JAMK Bachelor's, JAMK Master's vs. JYU Master's). Comparison between universities can be also done with this method.

3.1.1 Tools

To generate analysable data after successful mapping an analysation tool must be chosen. There are plenty of options available. For data analysis Power BI was strongly recommended by client of the thesis, however at the beginning the Microsoft Excel data analysis tools were tried out and found out not to be dynamic enough and Power BI was chosen for this purpose.

For the conference paper a few templates were presented by IEEE, there was template for Microsoft Word and for Latex and Overleaf. (IEEE Templates, n.d.) First though was to go with Microsoft Word since it was familiar before, but the client of the thesis again strongly recommended to go for LaTeX, so LaTeX was taken into the test and found out to be excellent for paper writing.

Power BI

Microsoft Power BI is a data analysis tool, commonly used with prepared excel dataset, but also supports another format such as SQL databases, JSON, and more. Power BI is interactive and can be used in cloud (Microsoft Power BI, n.d).

LaTeX

LaTeX is a typesetting system for communication for technical and scientific documentation, initially released in 1984 and still being updated and used frequently. LaTeX uses tagging method and

provides tools for citations and cross-references. LaTeX is commonly used scientific journal articles and conferences (The LaTeX Project, n.d.; Wikipedia contributors, 2022).

3.2 Dataset, Scoping & Research method

Dataset was gathered from theses made in Central Finland that were publicly available and released over several years to get big enough dataset, therefore regional approach was chosen. Jyväskylä has been active since the very first days of cybersecurity education, research and innovation processes (Lehto M., 2015; Savola R. 2017).

Theses done for Jamk University of Applied Sciences can be found publicly from Theseus site with using search term keywords such as cybersecurity. University of Jyväskylä theses are called as pro-gradu and those can be extracted similarly from the database of JYX, where also theses are publicly available. More detailly explained in the actual submitted paper (Arene ry n.d.; University of Jyväskylä n.d.).

Quantity of the analysed theses of the scope was 173 theses, which were mapped with the Frameworks described in chapter 2. Every thesis with keyword of cybersecurity did not fit for this purpose and that number is already excluded from that 173 quantity. Examples of left out works were on topics such as when cybersecurity was only in calling for future research. Mapping theses with used the Framework could result very different result depending on the criteria of analyser to map it into just one or another way, the same dataset could have a bit different result when performed by another analyser, meanwhile I would not recommend mapping one thesis onto many ways, the data output might be hard to analyse. Same could be said on industry sector mapping when it was not too clear. This mapping part was the most crucial part for getting the results of this research.

3.3 Analysis

Analysis was done with Power BI and after combining and slicing data in as multiple ways to get reasonable results. A few of the most relevant analyse patterns were chosen. Commissioner of this thesis had clear visions what kind of results could be extracted from the dataset, selected analysis results were mostly decided by commissioner of this thesis. However other analysis was also per-

formed on Power BI and presented for the commissioner, these rejected analysis parts included such things as mapping into European Cybersecurity Taxonomy domains and sectors. On the NICE Framework side, the mapping for specialty areas was also performed.

Something that could have been also extracted from this dataset would be such as comparing results between NICE Framework and European Cybersecurity Taxonomy, with Categories and Specialty Areas against Domains, since they overlap a bit, but this kind of analysis does not fit into the subject of analysing workforce relation against theses.

3.3.1 NICE Categories

NICE Framework categorising was the highest level of analysis performed in this work. When comparing universities to each other and the nature of the university and its fundamental learning outcomes are taken into consideration, the categorising seems to fit as expected. Jamk University of Applied Sciences had more hits in categories which are more of an appliance of sciences while University of Jyväskylä had more hits on analysis of theorical fundamentals.

Power BI enabled even more advanced graphs to work than was used in the article. Article had limitations on colours and size, where the size was dramatically problematic when providing more detailed graphs, one example is figure 11. If there were a need to fit everything also from tiny sectors, adjustment would have been needed to rename the education type to something shorter like “JAMK EQF-6”. Full table of category hits can be found from submitted paper appendix 1.

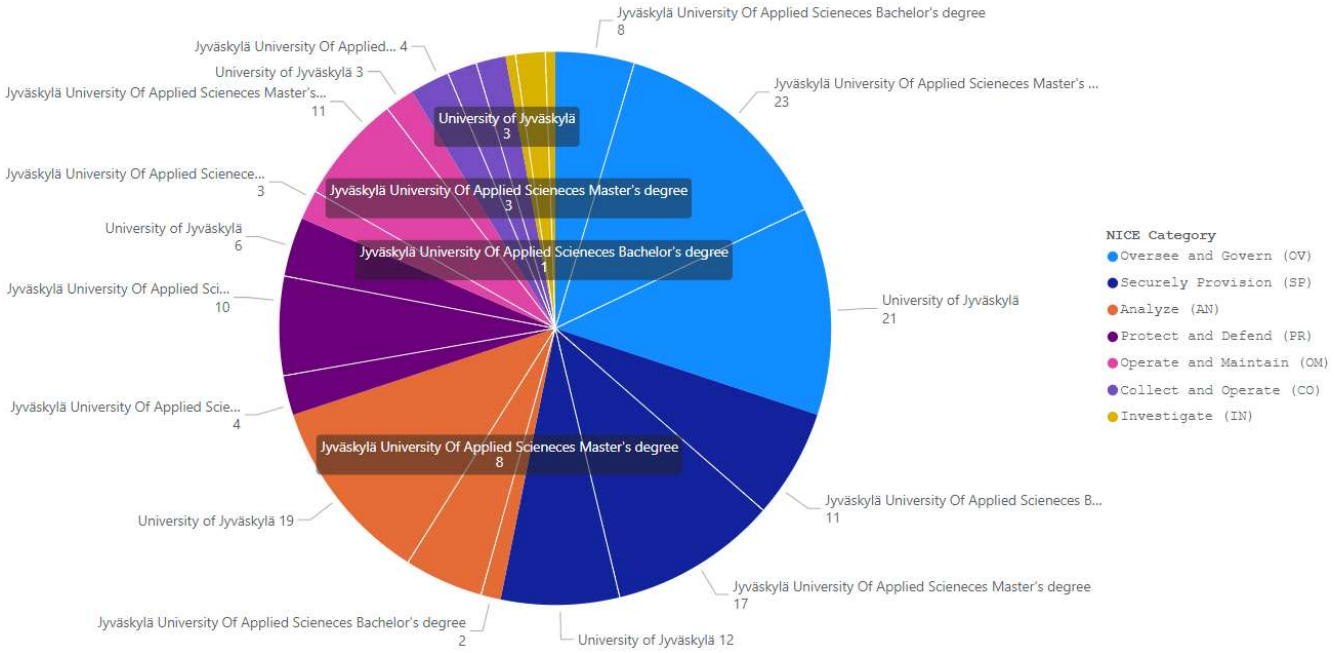

Figure 11 NICE Frame categories in colors with education type slicers

3.3.2 NICE Work roles

NICE work roles were also used in the article. The article lists only top 15 of the mapped roles and provides corresponding graph on those top 15. Here's the full listing on work roles with the number of hits.

- Threat/Warning Analyst, 19
- Research & Development Specialist, 18
- Cyber Policy and Strategy Planner, 15
- Vulnerability Assessment Analyst, 11
- Privacy Officer/Privacy Compliance Manager, 8
- Cyber Instructor, 7
- Cyber Legal Advisor, 6
- Security Architect, 6
- Cyber Crime Investigator, 5
- Cyber Instructional Curriculum Developer, 5
- Cyber Workforce Developer and Manager, 5
- Network Operations Specialist, 5
- Security Control Assessor, 5
- Systems Requirements Planner, 5
- Systems Security Analyst, 5
- All-Source Analyst, 4
- Cyber Defence Infrastructure Support Specialist, 4
- Data Analyst, 4

- Information Systems Security Manager, 4
- System Administrator, 4
- Cyber Defence Analyst, 3
- Cyber Operator, 3
- Exploit Analyst, 3
- All Source-Collection Manager, 2
- Authorizing Official/Designating Representative, 2
- Cyber Intel Planner, 2
- Cyber Ops Planner, 2
- Mission Assessment Specialist, 2
- Executive Cyber Leadership, 1
- Information Systems Security Developer, 1
- IT Program Auditor, 1
- Multi-Disciplined Language Analyst, 1
- Partner Integration Planner, 1
- Secure Software Assessor, 1
- Software Developer, 1
- System Testing and Evaluation Specialist, 1
- Technical Support Specialist, 1

NICE Framework supports even more work roles, but these were only ones to get hits. It is a good idea to get only the most common ones to create at least some findings from the analysis instead of listing each one on the submitted article. Also, in this case filtering, for example, by education type or even industry sector could be done. In the article there is education type graph for top 15 work roles.

3.3.3 European Cybersecurity Taxonomy

On the theses mapping part this was probably the most difficult. On the Jamk University of Applied Sciences there is usually commissioner for the thesis, therefore these theses could be mapped blindly by applying the sector the commissioner represents, while that might not be always accurate either since if commissioner is a contractor, should we map it for the target company or the commissioner company? University of Jyväskylä progradus, does not always have a client and if, the subject is unclear to which industry it would be applied to, since it could be applied to many if not all, the mapping was decided on the ideology of the most logical one, therefore mappings for government and digital services and platforms got huge amount of hits, since these are the most likely to get benefit from general works.

Greyscale documentation makes the graph used in article quite unclear when readability in mind. Coloured version of the same graph is added here as figure 12.

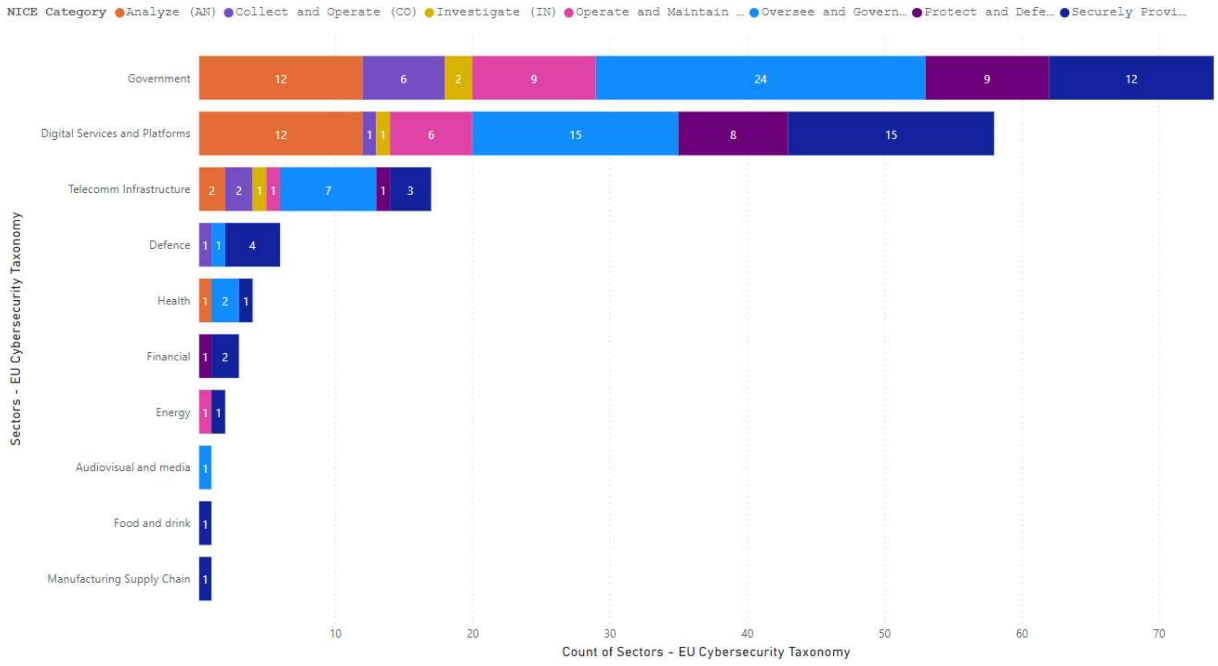

Figure 12 Colour duplicate of the European Cybersecurity Taxonomy industry sectors mapped with NICE Framework

3.4 Discussion

In the discussion part of the article reliability is taken into mind while also mentioned that the learner will be most likely to acquire multiple skillsets in many different work roles. NICE Framework also has an option to generate work roles, that is also one thing to keep in mind that this analysis only used the prefixed listed work roles. The amount of work roles is so wide that there is probably no employer so big in Finland which would have all the work roles in use.

3.4.1 Cybersecurity as a field

In the modern world, every industry sector is using more or less information technology connected to the public internet. Connectivity could be either user desktop computers, some embedded software unit, any kind of internet of things unit or anything. There is always room for human error in terms of connecting factory controlling devices for internet, just to control it from home due

COVID-19 pandemic or another reason. Yet there are lots of sectors missing from this study, we can guess that they might be purchasing cybersecurity as a service from some company on digital platforms, cloud computing, government, or something else.

3.4.2 Effects of the education level

Education level will most likely also affect the results of work roles in the theses mapped to. Since these theses were done in EQF levels six and seven, it is unlikely to have a thesis pointing to a work role, for example, an incident responder, which could be an entry level position and it will be led from upwards, mapping a thesis for this role would probably always point up to the management side of mentioned role. Workload of the thesis is also good to keep in mind since EQF level 6 thesis will be roughly 400 hours of workload and EQF level 7 thesis 800 hours of workload, it surely ramps up the thesis projection in the work role mapping. Differences between the universities were also mentioned in the article and they are opened in this thesis part 3.3.1.

3.4.3 NICE Framework

The article discusses the differences between education type hit frequency on categories. Points out that most mapped category “Oversee and Govern” suits greatly for this level of research, while most likely having not that many work roles available on the field.

On the work roles side, it was a surprise to have few clear leaders on the work roles. All top 4 roles “Threat/Warning Analyst, 19”, “Research & Development Specialist, 18”, “Cyber Policy and Strategy Planner, 15”, “Vulnerability Assessment Analyst, 11” had a high percentage of the total mapped works, being as high as 63/173 of all works, meaning ~36% as percentage.

4 Conclusion

Differences between target universities were expected, but it was unclear how large the difference is. Even when University of Jyväskylä is more of a research based, there is still lots of research done in Jamk University of Applied Sciences, the reason might be the scope of theses in terms of workload, but also the field of study might affect this.

Examining the original dataset and mapping it against given frameworks was a more difficult and longer task to do, when trying to be accurate in the mapping. Usually, it is not enough to read just the topic, the topic was quite often misleading on the context of the work. In most cases abstract was enough to get enough information from the work, but sometimes also table of contents and conclusion were needed to read with a thought.

Analysis part was the most interesting part to find all the relevant information by choosing different filters and different correlations between things. Definitely the chosen theory part supported the analysis planning. When chosen tools are flexible and the dataset is parsed good the analysis part is easy to execute and easy to find and test different correlations, sometimes experimenting with ideas could lead up to good analysis results.

Writing the article with tools and formatting that I was unfamiliar before was quite hard to do, but the article managed to be ready on the given deadline of the chosen conference, afterwards the conference gave more time for the articles, but that also resulted much more polished version of the article. LaTeX is powerful tool for article writing and, in this industry sector, it could be handy to teach and use it in the education also.

The chosen research questions were answered in the analysis part and this thesis was easy to assemble to support the article. A lot more was learned about the frameworks and education systems during thesis writing, since the length of the thesis was about four times longer.

The first research question asked how higher level education theses can be mapped using taxonomy frameworks. NICE Framework suits the task well, while not perfectly for mapping theses. Most theses could fit into more than one category, specialty area or work role than one, but to get a picture what the work is about the NICE Framework gives quite good overlook and describes the nature of the work.

The second research question inspected how reliable this kind of mapping towards the work role or job title would be. Reliability is somewhat questionable according to facts just described. However, I could guess that differences with a different mapper would not be that great after all, my best guess would be around 85-95% similarity, but that could be one of the future research topics.

Writing these kinds of articles just to fit in three to eight pages is quite restricting comparing to thesis project. Having tech talks about theses also could give more to the field than narrow articles.

Future research could be done by comparing NICE Framework with European Cybersecurity Taxonomy on the parts they most overlap being: domains and specialty areas. Also, another region or other datasets could be taken into consideration. Reflecting the results to current educational curriculum decree is a good future research project on this topic. Can the course pool be adjusted to match the needs of the workforce, is there something that might not be requested, but still on the course pool?

References

Amir T. (2020). *Developing cyber security competences using NICE KSAs in cyber ranges.* [Bachelor's Thesis, LAUREA University of Applied Sciences]. Theseus. https://urn.fi/URN:NBN:fi:amk-2020121728905

Arene ry. (n.d.) *Database for theses from Universities of Applied Sciences in Finland*. Theseus. https://www.theseus.fi/

Bologna Process (n.d.) *How does the bologna process work?* European Higher Education Area website. Retrieved June 7, 2022, from http://www.ehea.info/page-how-does-the-bologna-process-work

Burley D., Bishop M., Kaza S., Gibson D., Hawthorne E. & Buck S. (2017). ACM Joint Task Force on Cybersecurity Education. In *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education (SIGCSE '17)* (pp. 683-684). ACM. https://doi.org/10.1145/3017680.3017811

Cabaj K., Domingos D., Kotulski Z. & Respício A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security, 75*. https://doi.org/10.1016/j.cose.2018.01.015

CAE Documents Library. (n.d.) *National Centers of Academic Excellence in Cybersecurity (NCAE-C) CAE Documents Library*. Department of Defence Cyber Exchange website. https://public.cyber.mil/ncae-c/documents-library/

Council of the European Union. (2017). *32017h0615(01)* (OJ C 189). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv%3AOJ.C_.2017.189.01.0015.01.ENG

Crick T., Davenport J., Irons A. & Prickett T. (2019). A UK Case Study on Cybersecurity Education and Accreditation. *IEEE Frontiers in Education Conference (FIE)*. https://doi.org/10.1109/FIE43999.2019.9028407

EHEA Finland. (n.d.) *Page-Finland*. European Higher Education Area website. Retrieved June 7, 2022, from http://www.ehea.info/page-finland

EHEA Report. (2003). *National Report Finland 2003*. European Higher Education Area website. http://www.ehea.info/Upload/document/members/finland/National_Report_Finland_2003_576352.pdf

European Commission. (2017). Directorate-General for Education and Culture, *ECTS users' guide 2015*, Publications Office, 2017. https://data.europa.eu/doi/10.2766/87192

European Qualifications Framework. European Commission. (2018). *The European Qualifications Framework: supporting learning, work and cross-border mobility*. Publications Office of the European Union. https://www.oph.fi/sites/default/files/documents/eqf-10-years-guide.pdf

Finnish Education System. (n.d.) *The Finnish education system*. Ministry of Education and Culture website. Retrieved June 8, 2022, from https://okm.fi/en/education-system

Finnish Higher Education Evaluation Council, Niemelä, J. & Teichler, U. (2012). *Evaluation of the Bologna process implementation in Finland: Part I, Evaluation of the degree reform. Part II, The implementation of the Bologna reforms in Finland from an international perspective*. Finnish Higher Education Evaluation Council.

IEEE Conferences. (n.d.) *Conferences page*. IEEE. Retrieved June 2, 2022, from https://www.ieee.org/conferences/

IEEE Templates. (n.d.) *Manuscript Templates for Conference Proceedings*. IEEE. Retrieved June 3, 2022, from https://www.ieee.org/conferences/publishing/templates.html

ISCED 2011. (2012). *International Standard Classification of Education ISCED 2011*. UNESCO Institute for Statistics. http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

Lehto M. (2015). Cyber security competencies: cyber security education and research in Finnish universities. In *proceeding of the 14th European Conference on Cyber Warfare & Security, ser. ECCWS 2015* (pp. 179–188). Academic Conferences and Publishing International Limited. http://urn.fi/URN:NBN:fi:jyu-201507092560

Merriam-Webster. (n.d.) Taxonomy. In *Merriam-Webster.com dictionary*. Retrieved June 16, 2022, from https://www.merriam-webster.com/dictionary/taxonomy

Microsoft Power BI. (n.d.) *Power Bi page.* Microsoft website. Retrieved June 16, 2022, from https://powerbi.microsoft.com

Ministry of Education and Culture. (2014). *Covernment Decree on Universities of Applied Sciences*. https://finlex.fi/en/laki/kaannokset/2014/en20141129.pdf

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

Newhouse W., Keith S., Scribner B. & Witte G. (2017). NIST Special Publication 800-181. *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-181

NICE Website. (n.d.) *Homepage of National initiative for cybersecurity education (NICE)*. National Institute of Standards and Technology Website. Retrieved June 3, 2022, from https://www.nist.gov/itl/applied-cybersecurity/nice

Ovaska, J. Saharinen, K. & Sipola, T. (2022). *Analysing Finnish Cybersecurity Thesis Topics Using Taxonomic Frameworks*. [Manuscript submitted for publication]. Institute of Information Technology. Jamk University of Applied Sciences.

Pelkonen, A., Ahlqvist, T., Leinonen, A., Nieminen, M., Salonen, J., Savola, R., Savolainen, P., Suominen, A., Toivanen, H., Kyheröinen, J., & Remes, J. (2016). *Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen* (Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2015). Valtioneuvoston kanslia. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79562/Kyberosaaminen%20Suomessa.pdf

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

Reference spreadsheet. (2020). *Reference spreadsheet*. National Institute of Standards and Technology website. Retrieved June 21, 2022, from https://www.nist.gov/document/supplementnicespecialtyareasandworkroleksasandtasksxlsx

Saharinen K., Backlund J. & Nevala J. (2020). Assessing Cyber Security Education through NICE Cybersecurity Workforce Framework. In *2020 12th International Conference on Education Technology and Computers (ICETC'20)* (pp. 172-176). ACM. https://doi.org/10.1145/3436756.3437041

Saharinen K., Karjalainen M. & Kokkonen T. (2019). A design model for a degree programme in cyber security. In *Proceedings of the 2019 11th International Conference on Education Technology and Computers (ICETC 2019)* (pp. 3-7). ACM. https://doi.org/10.1145/3369255.3369266

Savola R. (2017). Current level of cybersecurity competence and future development: case Finland. In *Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings, ser. ECSA'17* (pp. 121-124). https://doi.org/10.1145/3129790.3129804

Seppänen-Järvelä R., Åkerblad L. & Haapakoski K. (2019). Monimenetelmällisen tutkimuksen integroivat strategiat. *Yhteiskuntapolitiikka*, 84(3), 332-339. http://urn.fi/URN:NBN:fi-fe2019061220179

Shoemaker D., Kohnke A. & Sigler K. (2016). *A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)*. Taylor & Francis Group.

Stange M., Tucker C., Tang C., Servin C. & Geissler M. (2020). Pre-Bachelor's Curricular Guidance For Cybersecurity Programs. In *Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE '20).* ACM. https://doi.org/10.1145/3341525.3393973

Švábenský V., Vykopal J. & Čeleda P. (2020). What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. In *proceedings of the 51st ACM Technical Symposium on Computer Science Education* (pp. 2-8). ACM. https://doi.org/10.1145/3328778.3366816

The LaTeX Project. (n.d.) Website at The LaTeX Project homepage. Retrieved June 16, 2022, from https://www.latex-project.org

The Security Committee. (2013). *Program for the implementation of the national cybersecurity strategy* (pp. 47–48). https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Kyberturvallisuusstrategian-toimeenpano-ohjelma.pdf

Unesco Institute of Statistics. (2011). *International Standard Classification of Education ISCED 2011*. https://web.archive.org/web/20170106011231/https://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

University law. (2009). *University law regulation*. FINLEX. https://www.finlex.fi/fi/laki/ajantasa/2009/20090558

University of Jyväskylä. (n.d.) *Jyväskylä University Digital Repository*. https://jyx.jyu.fi/?locale-attribute=en

What is cybersecurity? (2019). Article. *Cybersecurity & Infrastructure Security Agency (CISA) website*. Retrieved June 2, 2022, from https://www.cisa.gov/uscert/ncas/tips/ST04-001

Wikipedia contributors. (2022, July 3). LaTeX. In Wikipedia, The Free Encyclopedia. Retrieved July 5, 2022, from https://en.wikipedia.org/w/index.php?title=LaTeX&oldid=1096218960

Appendices

Appendix 1. Article LaTeX source code (without comments):

```
\documentclass[conference]{IEEEtran}
\IEEEoverridecommandlockouts
\usepackage{cite}
\usepackage{amsmath,amssymb,amsfonts}
\usepackage{algorithmic}
\usepackage{graphicx}
\usepackage{textcomp}
\usepackage{xcolor}
\usepackage{url}
\usepackage{booktabs}
\usepackage{float}
\usepackage{arydshln}
\usepackage{flushend}
\def\BibTeX{{\rm B\kern-.05em{\sc i\kern-.025em b}\kern-.08em
    T\kern-.1667em\lower.7ex\hbox{E}\kern-.125emX}}
\begin{document}

\title{Analysing Finnish Cybersecurity Thesis Topics Using Taxonomic Frameworks}

\author{\IEEEauthorblockN{Joonatan Ovaska}
\IEEEauthorblockA{\textit{Institute of Information Technology} \\
\textit{Jamk University of Applied Sciences}\\
Jyväskylä, Finland \\
joonatan.ovaska@jamk.fi}
\and
\IEEEauthorblockN{Karo Saharinen}
\IEEEauthorblockA{\textit{Institute of Information Technology} \\
\textit{Jamk University of Applied Sciences}\\
Jyväskylä, Finland \\
karo.saharinen@jamk.fi}
\and
\IEEEauthorblockN{Tuomo Sipola}
\IEEEauthorblockA{\textit{Institute of Information Technology} \\
\textit{Jamk University of Applied Sciences}\\
Jyväskylä, Finland \\
tuomo.sipola@jamk.fi}
}

\maketitle

\begin{abstract}
This paper presents an analysis of Bachelor's and Master's cybersecurity theses in
Jyväskylä, Finland.
The theses were gathered from publicly available publishing platforms of Finnish
universities and were analysed using the NICE Cybersecurity Workforce Framework
```

(NCWF) categories and European Cyber Security Organization's (ECSO) The European Cybersecurity Taxonomy.
The aim of this research was to find whether there clearly were emphasis on certain framework categories or work roles. Similarly, industry sectors about which cybersecurity theses were done were of interest. The results can be used by education providers to align and plan their education based on regional needs, and cybersecurity students, before starting their thesis project, can use this information to deliberate suitable work sectors in which theses are lacking.
As our research results point out, there is a clear emphasis on certain NICE categories and work roles that are more common within the dataset. However, it is prudent to take into account the scope of the dataset, which was specific to one region in Finland.
While this research presents findings about this one region, researchers from around the world can consider using the same research methods on a similar datasets gathered from their respective regions.
\end{abstract}

\begin{IEEEkeywords}
Cybersecurity, Education, Thesis, NICE Framework
\end{IEEEkeywords}

\section{Introduction}

\subsection{Cybersecurity as a Field of Education}

Already in 2018, a study in the field of cybersecurity education reviewed and analysed 21 cybersecurity master's programmes with a content, structure, requirements, duration, etc. \cite{cabaj2018}. A UK case study about cybersecurity education and accreditation analysed this subject in the scope of UK, which was compared to the US \cite{crick2019}.

The security committee of Finland was established in 2012 and released a program for the implementation of the national cybersecurity strategy \cite{seccom2013} in March 2013. One point of the implementation was to establish cybersecurity education on all levels of the Finnish educational system. Both organisations at the higher education institution (HEI) level in Jyväskylä, Jamk University of Applied Sciences (JAMK) and University of Jyväskylä (JYU), started their master's degrees in cybersecurity around 2013 \cite{jyu,jamk}. JAMK established a bachelor's degree in 2015. Within the decade more and more HEIs in Finland started to establish courses or full degrees in cybersecurity as Lehto and Niemelä point out~\cite{lehto2019}.

\subsection{Government Decrees on the Universities}\label{chap:legislation}

The HEIs are regulated by Government Decree on Universities of Applied Sciences \cite{minedu2014} and Decree on Universities \cite{finlextutkinnot,finlexyo}.
The mission of the scientific universities of Finland, by law, is to freely further scientific research, provide scientific education and civilise artistically and \emph{\textit{interact with the society}}~. The mission of the universities of applied sci-

```
ences, by law, is to \emph{practice research, development, innovation and artistic
actions to improve working life and regional development}~\cite{minedu2014}.

Ministry of Education and Culture in Finland has written down that studies must
have certain structure which includes a thesis project~\cite{minedu2014}. Each pro-
gramme leading either to a Bachelor's degree or Master's degree must have a thesis,
this also applies to the field of all universities. Theses for this analysis are
gathered from programmes in this category and only from publicly available sources.
Bachelor's theses are worth of 15 European Credit Transfer and Accumulation System
(ECTS) credits and Master's theses from both JAMK and JYU are worth of 30 (ECTS)
\cite{eu2015}.

\section{Literature and Frameworks}

\subsection{Degree Levels}

For measuring the degree levels of the analysed theses, we can use European Quali-
fications Framework (EQF) and International Standard Classification of Education
(ISCED) for a similar International level system. Leveling system for (EQF) goes
from level 1 up to level 8 and (ISCED) from level 0 up to level 8, where level 8 is
concidered to be highest level. Level 8 would map to Ph.D. studies while the lowest
level 1 is concidered as just only a basic general knowledge. In this paper we con-
centrate on levels 6 \& 7.

Learning outcomes can be mapped as Bachelor's degree for level 6 (EQF) and Master's
degree for level 7 (EQF and ISCED) \cite{eu2017}\cite{unesco2011}, for older ISCED
1997 model the corresponding leveling would be 5A-medium and 5A-long/very long pro-
grammes.

\subsection{NICE Framework}

National Initiative for Cybersecurity Education (NICE) describes the Workforce
Framework for Cybersecurity (NICE Framework or NCWF). The main idea is to map cer-
tain skills and knowledge into a task. The most common use case of the NICE Frame-
work is to assign those into a Work Role. \cite{nist2020}

\begin{figure}[h!]
    \centering

\includegraphics[width=0.45\textwidth]{NICE_framework_workroles.drawio_diagrams.net
.png}
    \caption{Work roles' relationship to building blocks.}
    \label{fig_1}
\end{figure}

As the Framework evolved and got more attention, the National Institute of Stand-
ards and Technology (NIST) has updated the Framework and mapped work roles into 7
categories. Each of these categories is composed of Specialty Areas, each of which
is composed of one or more work roles. Each work role, in turn, includes KSAs and
Tasks, see fig 2 and list below. \cite{nist2020}
```

```
\begin{figure}[h!]
    \centering
    \includegraphics[width=0.45\textwidth]{NICE_categories.png}
    \caption{Relationships among NICE framework components.}
    \label{fig_2}
\end{figure}

\begin{itemize}
    \item Securely Provision (SP)

    Build secure, conceptualized, procures, designs information technology (IT)
systems.
    Includes specialty areas such as \emph{*Technology R\&D, Risk Management, Sys-
tems Architecture, etc.*}

    \item Operate and Maintain (OM)

    Provides the support, maintance and administration for efficient and effective
    information technology (IT) system performance and security. Includes specialty
    areas such as \emph{*Network Services, Data Administration, Systems Administra-
tion, etc.*}

    \item Oversee and Govern (OV)

    Provides direction, leadership, management or development and advocacy for
    organisation effective conduct cybersecurity work. Includes specialty areas
such as
    \emph{*Strategic Planning and Policy, Legal Advice and Advocacy, Training, Edu-
cation and Awareness, etc.*}

    \item Protect and Defend (PR)

    Analyses, mitigates and identifies threats to internal information technology
(IT)
    systems and/or networks. Includes specialty areas such as \emph{*Vulnerability
Assessment and Management,
    Cybersecurity Defence Infrastructure Support, Cybersecurity Defence Analysis,
etc.*}

    \item Analyze (AN)

    Performs specialized review and evaluation of incoming cybersecurity infor-
mation
    to determine its usefulness for intelligence. Includes specialty areas such as
\emph{*Threat Analysis, All-Source Analysis,
    Exploitation Analysis, etc.*}

    \item Collect and Operate (CO)
```

```
    Provides specialized deception and collection and denial of cybersecurity in-
formation
    that may be used to develop intelligence. Includes specialty areas
    \emph{Cyber Operational Planning, Cyber Operations, Collection Operations}

    \item Investigate (IN)

    Investigates cybersecurity crimes and/or events related to information technol-
ogy
    (IT) systems, digital evidence, and networks. Includes specialty areas
    \emph{Cyber Investigation, Digital Forensics}

\end{itemize}

Work roles are not listed here, but for an example here's few given to get the idea
what is the meaning of a work role. ``Security Architect'', ``System Administra-
tor'', ``Exploitation Analyst'', ``Cyber Crime Investigator''. A single Work Role
(e.g., Software Developer) may apply to those with many varying job titles (e.g.,
Software engineer, coder, application developer). Conversely, mulitple roles could
be combined to create a particular job.

The NICE Framework does not define proficiency levels (e.g., Basic, Intermediate,
Advanced). Such attributes, and those regarding the proficiency with which a learn-
er performs Tasks, are left to other models and resources.

\begin{itemize}
    \item 7 Cyber Security Workforce Categories
    \item 33 Specialty Areas
    \item 52 Work Roles
\end{itemize}

Framework itself provides freedom of either using existing work roles or creating a
new work roles, but this analysis is limited to use only existing work roles within
the framework.

Mapping NICE Framework with EQF table can be used to generate a design model for a
degree programme within field of cybersecurity. \cite{saharinen2019}

\subsection{The European Cybersecurity Taxonomy}

The European Cybersecurity Taxonomy has reformed to complete more aspects and de-
tails than compiting similar Frameworks such as NICE Framework. It covers the most
sources compared to other Frameworks as contributions to Cybersecurity Taxonomy.
\cite{eu2019}

The goal of the taxonomy is supporting the mapping of the European cybersecurity
competencies available. The goal of the taxonomy is not to support the maping of
cybersecurity products, services, or processes including oprational activities.
```

Taxonomy is trying to cluster a complex and multifaceted discipline as cybersecurity needs to be structed on multiple dimensions, capturing not only the core and traditional research domains, but also impacted sectors and application.

This taxonomy is proposed as three-dimensional taxonomy, based on:

\begin{itemize}
    \item \textbf{**Research domains**} represent areas of knowledge, inluding human, legal, ethical and technological aspects.
    \item \textbf{**Sectors**} proposed to highlight in scenarios, such as energy, transport or financial sector.
    \item \textbf{**Tehnologies and Use Cases**} represent the technological enablers to enchance the development of the different sectors.
\end{itemize}

European cybersecurity taxonomy can be mapped to 15 Cybersecurity Domains which each have respective subdomains (e.g., Domain Cryptology has total of 14 subdomains such as ``Asymmetric cryptography'', ``Symmetric cryptography'', ``Hash functions'', ``Random number generation'', etc.). Here's full list of main domains:

\begin{itemize}
    \item Assurance, Audit, and Certification
    \item Cryptology (Cryptography and Cryptanalysis)
    \item Data Security and Privacy
    \item Education and Training
    \item Human Aspects
    \item Identity Management
    \item Incident Handling and Digital Forensics
    \item Legal Aspects
    \item Network and Distributed Systems
    \item Security Management and Governance
    \item Security Measurements
    \item Software and Hardware Security Engineering
    \item Steganography, Steganalysis and Watermarking
    \item Theoretical Foundations
    \item Trust Management and Accountability
\end{itemize}

The European cybersecurity taxonomy maps also different sectors which are described further in the documentation. (e.g., Defence describes as ``This sector embraces the activities and infrastructure required for protecting citizen, including the use of aeronautics, space, electronices, land or telecommunication systems''.) There are total of 15 sectors, but we are listing only those which had hits within this research:

\begin{itemize}
    \item Audiovisual and media
    \item Defence
    \item Digital Services and Platforms
    \item Energy

```
    \item Financial
    \item Food and drink
    \item Government
    \item Health
    \item Manufacturing and Supply Chain
    \item Telecomm Infrastructure
\end{itemize}

Technologies and Use Cases Dimensions relates to the technologies and uses cases in
dimensions. These technologies are used across multiple sectors, there are total of
23 listed items, but we are listing only sectors which had at least one hit within
this research:

\begin{itemize}
    \item Artificial intelligence
    \item Big Data
    \item Blockchain and Distributed Ledger Technology (DLT)
    \item Cloud, Edge and Virtualisation
    \item Critical Infrastructure Protection (CIP)
    \item Disaster resilience and crisis management
    \item Fight against crime and terrorism
    \item Border and external security
    \item Local/wide area observation and surveillance
    \item Hardware technology (RFID, chips, sensors, networking, etc.
    \item Information Systems
    \item Internet of Things, embedded systems, pervasive systems
    \item Mobile Devices
    \item Operating Systems
    \item Vehicular Systems (e.g. autonomous vehicles)
\end{itemize}

\section{Dataset, Scoping \& Research Method}

For the research scope the authors targeted theses done in Central Finland that
were publicly available/released over several years which proved to be an big
enough dataset to reflect findings. Regional developer scoping was chosen, Jyväsky-
lä is a major player in Finland when it comes to cybersecurity training and educa-
tion \cite{savola2017} \cite{lehto2015}. In Jyväskylä there are 2 Universities
which provide cybersecurity education: University of Jyväskylä and Jamk University
of Applied Sciences. University of Jyväskylä provides Master's students more theo-
rical approach for cybersecurity. Jamk University of Applied Sciences has ICT engi-
neering programs for both Bachelor's and Master's class Applied Sciences for cyber-
security \cite{minedund}.

Theses done for Jamk University of Applied Sciences can be found publicly from the-
seus \cite{arenend} site and use search terms for keywords such as cybersecurity.
For University of Jyväskylä theses called pro-gradu, can be found from their system
called JYX \cite{jyujyx}, where these theses are also publicly available. Some of
the theses contained appendixes or even whole main thesis as restricted access or
hidden based on the Act of the Openness of Government Activities which allows Uni-
```

```
versities of Applied Sciences and University of Jyväskylä to have thesis which may
contain hidden appendixes due research permission for confidential data
\cite{mineduopen}. Those which has not been scoped out has been determined by the
abstract and topic of the thesis.

Theseus is a service for Universities of Applied Sciences for storing and sharing
published theses. JYX is a digital archive which collect and display parts of JYX
materials including theses from (JYU).

Used research method is mixed methods, quantity of the total scope is 173 theses,
which has been qualified to match against the described Frameworks and analysed
afterwards. Dataset from JAMK is from 2013 to 2020 and the dataset from JYU from
2018 to 2020. The reasoning for the scope is that this dataset was pregathered for
investigation, only some theses were dropped from that dataset for not hitting the
scope of cybersecurity field (e.g. Cybersecurity was only mentioned as a future
research, while not being part of thesis itself). The counted total of 173 theses
does not  include these mentioned unscoped theses.

Most of the theses dataset could have been mapped very differently during the map-
ping phase these theses are tried to tied only to the category which it fits the
most or is the main part of that specific thesis. Same applies for each other map-
ping done for work role and industry sectors also, when not specified on the order-
er side.

\section{Analysis}

\subsection{NICE Categories}

Based on all the collected theses by the dataset, within fig.~\ref{fig_3} we can
see the distribution of theses in NICE categories.

\begin{figure}[H]
    \centering
    \includegraphics[width=0.45\textwidth]{Categories-Pie.png}
    \caption{Theses per NICE category.}
    \label{fig_3}
\end{figure}

Mapping of the we can see that over half of the mapped theses were done for ``Over-
see and Govern'' and ``Securely Provision'' while categories ``Investigate'' and
``Collect and Operate'' were total of less than 10\% of the works.

The authors also wanted to compare the differences on each levels of education and
education organisation. Thus, we also mapped the weights of each category based on
those attributes. This is visualized in fig 4.

\begin{figure}[H]
    \centering
    \includegraphics[width=0.45\textwidth]{categories-education.png}
    \caption{Mapped categories by education type.}
```

```
    \label{fig_4}
\end{figure}

In figure 5 we can see the detailed precentages of category mappings between target
universities to highlight the differences and mission between the education types
as described by chapter~\ref{chap:legislation}. These precentages are compared to-
wards the total number of theses in the corresponding university.

\begin{figure}[H]
    \centering
    \includegraphics[width=0.45\textwidth]{NICE_Category_university_compare.png}
    \caption{Mapped categories by education type, total.}
    \label{fig_5}
\end{figure}

In table~\ref{mapping_table} we can see the more detailed amounts and precentages
of these category mappings between each education type, these precentages are com-
pared to total number of theses.

\begin{table}[H]
    \renewcommand{\arraystretch}{1.3}
    \caption{Categories Mapping Table}
    \centering
    \begin{tabular}{p{1,9cm} p{1,1cm} p{1,1cm} p{1,1cm} p{1,1cm}}
    \toprule
    \textbf{Categories}                & Bachelor's (JAMK) & Master's (JAMK) & Mas-
ter's (JYU) & Total        \\
    \midrule
    Oversee and Govern (OV)   & 8  (24.24\%)      & 23 (30.67\%)    & 21 (32.31\%)
  & 52 (30.06\%) \\
    \hdashline
    Securely Provision (SP)   & 11 (33.33\%)      & 17 (22.26\%)    & 12 (18.46\%)
  & 40 (23.12\%) \\
    \hdashline
    Analyze (AN)              & 2  (6.06\%)       & 8  (10.67\%)    & 19 (29.23\%)
  & 29 (16.76\%) \\
    \hdashline
    Protect and Defend (PR)   & 4  (12.12\%)      & 10 (13.33\%)    & 6  (9.23\%)
 & 20 (11.56\%) \\
    \hdashline
    Operate and Maintain (OM) & 3  (9.09\%)       & 11 (14.67\%)    & 3  (4.62\%)
 & 17 (9.83\%)  \\
    \hdashline
    Collect and Operate (CO)  & 4  (12.12\%)      & 3  (4\%)        & 3  (4.62\%)
 & 10 (5.78\%)  \\
    \hdashline
    Investigate (IN)          & 1  (3.03\%)       & 3  (4\%)        & 1  (1.54\%)
 & 5  (2.89\%)  \\
    \hdashline
```

```
    Total                    & 33 (19.08\%)      & 75 (43.35\%)    & 65 (37.57\%)
  & 173 (100\%)  \\
    \bottomrule
    \end{tabular}
    \label{mapping_table}
\end{table}

\subsection{NICE Work Roles}

One objective was to map each thesis towards a work role of the framework that was
exactly or close to that thesis topic. Total of 37 work roles were present within
the analysis. However, only top 15 had five or more hits each. There was also many
work roles with only one hit. Here is the top 15 listed provided with the count of
mapped roles:

\begin{enumerate}
    \item Threat/Warning Analyst, 19
    \item Reasearch \& Development Specialist, 18
    \item Cyber Policy and Strategy Planner, 15
    \item Vulnerability Assessment Analyst, 11
    \item Privacy Officer/Privacy Compliance Manager, 8
    \item Cyber Instructor, 7
    \item Cyber Legal Advisor, 6
    \setcounter{enumi}{6}
    \item Security Architect, 6
    \setcounter{enumi}{8}
    \item Cyber Crime Investigator, 5
    \setcounter{enumi}{8}
    \item Cyber Instructional Curriculum Developer, 5
    \setcounter{enumi}{8}
    \item Cyber Workforce Developer and Manager, 5
    \setcounter{enumi}{8}
    \item Network Operations Specialist,5
    \setcounter{enumi}{8}
    \item Security Control Assessor, 5
    \setcounter{enumi}{8}
    \item System Requirements Planner, 5
    \setcounter{enumi}{8}
    \item Systems Security Analyst, 5
\end{enumerate}

These top 15 work roles cover 72.25\% of all works. Remaining 27.75\% were distrib-
uted between other work roles. For mapping each of these top 15 work roles for each
education type we can get graph to show us the results as visualized by fig-
ure~\ref{fig_6}.

\begin{figure}[H]
    \centering
    \includegraphics[width=0.45\textwidth]{work_role_education_analysis.png}
    \caption{Mapped work roles by education type.}
```

```
    \label{fig_6}
\end{figure}

As the figure shows there is much alteration between education types when mapping
into work roles.

\subsection{European Taxonomy, Industry Sectors}

Theses done within University of Applied Sciences most of the time have a thesis
orderer within the description page and in Scientific Universities this orderer
might appear in the contents of the thesis. Given the theses where the orderer ap-
peared, the NICE category thesis can be mapped to an industry sector e.g. telecomm
company as an order would map it into ``Telecomm Infrasturcture'' and most of the
institution orders are mapped into ``Government''.

Theses from University of Jyväskylä are mostly research based, there will be more
of mapping with the feeling which industry would be the most relevant for the the-
sis, while most works would of course map to multiple sectors.

These sectors can indicate where cybersecurity play roles in current life span,
obviously the most common sectors are the sectory which are heavily related to in-
formation communications technologies and government. Sector mapping listed here:

\begin{itemize}
    \item \textbf{Government} 74, 44.31\%
    \item \textbf{Digital Services and Platforms} 58, 34.73\%
    \item \textbf{Telecomm Infrastructure} 17, 10.08\%
    \item \textbf{Defence} 6, 3.59\%
    \item \textbf{Health} 4, 2.4\%
    \item \textbf{Financial} 3, 1.8\%
    \item \textbf{Energy} 2, 1.2\%
    \item \textbf{Audiovisual and media} 1, 0.6\%
    \item \textbf{Food and drink} 1, 0.6\%
    \item \textbf{Manufactruing Supply Chain} 1, 0.6\%
\end{itemize}

Sectors can be also mapped to NICE categories as shown on the figure~\ref{fig_7}.
For the minor sectors most commonly the work was done in ``Securely Provision'',
while the ``Oversee and Govern'' was on top of the more common sectors.

\begin{figure}[H]
    \centering
    \includegraphics[width=0.45\textwidth]{taxonomy_sectors.png}
    \caption{European Taxonomy sectors mapped to NICE categories.}
    \label{fig_7}
\end{figure}

Theses around very high level of concepts or not a clear way nor order to define
sector remained unmapped or has been mapped to most applyable sector.
```

\subsection{Other Analysis}

Used frameworks could lead for more potential findings using different correlations with different options of European Cybersecurity Taxonomy domains, industries or sectors. Instead of mapping to NICE category and NICE work roles, we could map and see how they map into European Taxonomy and compare that result between two different frameworks or just to find the domains under different taxonomy.

\section{Discussion}

Before making any conclusions the first observation is that neither of these chosen frameworks suits perfectly to this type of analysis. Within the dataset there was a minimal number of theses which suited to just one category of the NICE framework or just one specialty area nor one work role, as already mentioned also in the original NIST documentation.

Comparing to the European Taxonomy proposal, there are more domains in use, however in the opinion of the authors they also overlap, maybe even more than NICE categories do, therefore the NICE categories was chosen as the main target for this study. Also the European Taxonomy offers much in names of technology and sectors, while those sectors might be quite far from the main area of cybersecurity, there could be a connection that those sectors might prefer to purchase these cybersecurity services from another company. This connection is hard to detect as typically theses were done to companies providing these \emph{*digital services and platforms*} and thus were the assigned orderer of the thesis.

Frameworks are relevant to categorise different fields together and to analyse certain trends that could be emphasised and communicated to interested parties. In case of the work roles, it gives an idea what to study in order to get the work that learner is interested of, however at the same time it is quite common that students should acquire multiple skillsets in many different work roles. There are not many employers, in Finland, that can have a cybersecurity teams big enough to include each of these work roles within one company.

\subsection{Cybersecurity as a Field}

In modern world there is no sector or field that could be totally unplugged or irrelevant to the Internet which leads to the point that in every field there is a need for at least some cybersecurity. More and more devices from IoT and any other embedded system will be connected to Internet if not already. Even the industrial factories where the common ideology has been that each of the factory controlling device is plugged offline there is always a part when someone with a lack of understanding or just by accident could attach this unit to public Internet. Sometimes it could be a worker who wants to work from home fex. Covid-19 issues or maybe a business fusion with another company which has joined to the same area network.

While cybersecurity as a field is growing fast, in terms of student theses and research, this growth is not apparent in all industry sectors. However, the trend can be seen from the researched dataset already, cybersecurity is not anymore just for

the most obvious sectors as in ICT, government, digital platforms, cloud computing, but it is for all.

\section{Conclusion}

\subsection{Effects of the Education Level}

Since the theses were pointing to EQF levels 6 \& 7, there is an effect that can be seen from the results and should be noted when making conclusions. For example basic cybersecurity work incident responder role didn't get a single match in this analysis, while it might be a common work role in the industry for lower level of education (EQF levels 4 \& 5). Meanwhile, there wer many theses which related to incident response as a concept, but the thesis had more of a planning or developing nature, therefore there a different work role was selected.

Not only the level of education is pushing these results to aim higher or more advanced levels, but also the workload of the thesis project. EQF level 6 studies has approximately 400 hours workload and EQF level 7 studies has approximately 800 hours of workload for thesis project of chosen research study that could be pure research or combination of doing implementation for chosen topic. This will effect the targeted work role as the workload is not too small the project is often pushed towards the mapping of higher hierarchy workforce.

\subsection{Differences Between the Universities}

For the chosen fields and subjects there could be seen trends between the two universities. JAMK students more often related their work, that could be at least somewhat correlated, to provided courses. Meanwhile, JYU theses more often included analytical research than implementations.

As figure 5 shows JAMK theses are more often towards categories ``Securely Provision'', ``Operate and Maintain'', ``Protect and Defend'', while JYU theses maps more often towards ``Oversee and Govern'' and ``Analyze''.

\subsection{NICE Categories}

While the dataset has least amount of data from Bachelor's degree theses they still pointed out to be much more focused on implementations by having a comperable high amount of works for ``Securely Provision'' and ``Protect and Defend'', also the third biggest total category analyze had only 2 works from Bachelor's level, mean while it was huge in (JYU) Master's theses, while not the first one, which was Oversee and Govern, which is somewhat same nature with the analysis category.

Investigate category has only 3 work roles and 2 specialty areas in it, and that could be also seen from these works that it's more rare to thesis land in this area, also there could be much of work loads which is not a good idea to give for a thesis project, being criminal investigation etc. Meanwhile there is definately work roles that exists in the real world, while it is clear that theses aren't done within these lines of work based on our research data.

The most mapped category, ``Oversee and Govern'', suits probably the best to these levels of research, I wouldn't say that there is not that much of work roles in work life as there was mapped theses for that category. Meanwhile there definately is work roles, it might not just be as big of a field that these statistics are providing.

\subsection{NICE Work Roles}

Surprisingly, there was one work role that stood clearly, with four (4) as clear leaders. ``Threat/Warning analyst'' was clearly the most mapped work role, while also ``Research \& Development Specialist'' was the 2nd most mapped work role in this analysis. ``Cyber Policy and Strategy Planner'' and ``Vulnerability Assessment Analyst'' were both mapped over 10 times. Theses from JYU were clearly most mapped to ``Threat/Warning Analyst'', while Bachelor's theses' most common mapping was ``Research \& Development Specialist''. Other top 4 work roles were quite even among different education types. Something to mention outside the top 4 is that all 5 works mapped to ``Systems Security Analyst'' were exclusively from the University of Applied Sciences Master's thesis.

Another interesting finding was that while University of Jyväskylä concentrated more on works around research fields, there were no mappings for ``Cyber Instructional Curriculum Developer'' work role. However, this might reflect the fact that these theses were extracted from the IT field including Cybersecurity as a search parameter and those works might be done for different fields of studies, e.g., Teacher Education.

\subsection{European Taxonomy Industry Sectors}

European Taxonomy Industry Sectors had hits only for about half of the industries. Meanwhile, multiple sectors had one hit in the complete dataset. In the rare cases they were mostly ``Securely Provision'' hits, which are more often implementation or system requirement based hits. If we would look the non-top 3 hits without ``Securely Provision'' works included, the amount of works and industries would cut lower than 50\%.

The methodology in the University of Applied Sciences on thesis projects encourages to find a commissioner for the thesis, therefore the mappings to rare industries were because of these commissioners. The other two industries that gained considerable amount of theses were from Health and Financials in the data from University of Jyväskylä. Health as an industry and as a regional determiner play a big role when looking at the location of Jyväskylä in Central Finland. There is a new hospital built recently and opened in early 2021 \cite{kssp2021} \cite{kssp2021org}. These theses were done before that time, but could be related to that project.

\subsection{Other Observations}

NICE Framework is suitable for obtaining data when asking where the work is and what kind of work orders have been given. Also, the courses and the nature of studies played a role in the thesis categories. This dataset scope can be used for re-

gional education development while it also gives an example for future research and possibilities in other geographic locations.

While the framework makes this mapping possible, there is room for subjective evaluation: another person could map some of the works differently by weighting the main topic differently, while it could be technically possible to map same works with multiple attributes. The authors considered the possibility, but concluded to go with only one category per thesis.
More advanced mathematical analysis methods could be used to investigate the dataset. However, the authors could draw up relevant conclusions with the analysis methods used in this paper.

\subsection{Future Research}

This data could be used to improve regional focus of education. This could be achieved by developing courses towards the work roles, categories and industries that were found during this work. These findings can also be used internationally to reflect the current state and to compare to other regions or perform similar research as an inspiration. With this dataset there are possibilities to look at other aspects concerning the topic or carry out research around European Taxonomy Domains mapping analysis.

\section*{Acknowledgment}

This research was supported by European Social Fund 2021–2023 as part of the LIPPA research and development project which is supporting smooth transitions from ICT studies to work life~\cite{lippa}.

\bibliographystyle{IEEEtran}
\bibliography{refs}

\end{document}

Appendix 2. NICE Framework refernce spreasheet

Full description can be found from NICE website from (Reference spreadsheet, 2020).

- Securely Provision (SP)
  - Risk Management (RSK)
    - Authorizing Official/Designating Representative
    - Security Control Assessor
  - Software Development (DEV)
    - Software Developer
    - Secure Software Assessor
  - Systems Architecture (ARC)
    - Enterprise Architect
    - Security Architect
  - Technology R&D (TRD)
    - Research & Development Specialist
  - Systems Requirements Planning (SPR)
    - Systems Requirements Planner
  - Test and Evaluation (TST)
    - System Testing and Evaluation Specialist
  - Systems Development (SYS)
    - Information Systems Security Developer
    - Systems Developer
- Operate and Maintain (OM)
  - Data Administration (DTA)
    - Database Administrator
    - Data Analyst
  - Knowledge Management (KMG)
    - Knowledge Manager
  - Customer Service and Technical Support (STS)
    - Technical Support Specialist
  - Network Services (NET)
    - Network Operations Specialist
  - System Administration (ADM)
    - System Administrator
  - Systems Analysis (ANA)
    - Systems Security Analyst
- Oversee and Govern (OV)
  - Legal Advice and Advocacy (LGA)
    - Cyber Legal Adviser
    - Privacy Officer/Privacy Compliance Manager
  - Training, Education, and Awareness (TEA)
    - Cyber Instructional Curriculum Developer
    - Cyber Instructor
  - Cybersecurity Management (MGT)
    - Information Systems Security Manager
    - Communication Security (COMSEC) Manager
  - Strategic Planning and Policy (SPP)
    - Cyber Workforce Developer and Manager
    - Cyber Policy and Strategy Planner
  - Executive Cyber Leadership (EXL)

        - Executive Cyber Leadership
    - Program/Project Management (PMA) and Acquisition
        - Program Manager
        - IT Project Manager
        - Product Support Manager
        - IT Investment/Portfolio Manager
        - IT Program Auditor
- Protect and Defend (PR)
    - Cybersecurity Defence Analysis (CDA)
        - Cyber Defence Analyst
    - Cybersecurity Defence Infrastructure Support (INF)
        - Cyber Defence Infrastructure Support Specialist
    - Incident Response (CIR)
        - Cyber Incident Responder
    - Vulnerability Assessment and Management (VAM)
        - Vulnerability Assessment Analyst
- Analyze (AN)
    - Threat Analysis (TWA)
        - Threat/Warning Analyst
    - Exploitation Analysis (EXP)
        - Exploitation Analyst
    - All-Source Analysis (ASA)
        - All-Source Analyst
        - Mission Assessment Specialist
    - Targets (TGT)
        - Targets Developer
        - Target Network Analyst
    - Language Analysis (LNG)
        - Multi-Disciplined Language Analyst
- Collect And Operate (CO)
    - Collection Operations (CLO)
        - All Source-Collection Manager
        - All Source-Collection Requirements Manager
    - Cyber Operational Planning (OPL)
        - Cyber Intel Planner
        - Cyber Ops Planner
        - Partner Integration Planner
    - Cyber Operations (OPS)
        - Cyber Operator
- Investigate (IN)
    - Cyber Investigation (INV)
        - Cyber Crime Investigator
    - Digital Forensics (FOR)
        - Law Enforcement/Counter-Intelligence Forensics Analyst
        - Cyber Defence Forensics Analyst

Appendix 3. European Cybersecurity Taxonomy

Full descriptions can be found from European Cybersecurity Taxonomy (Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M., Lazari, A., 2019).

- Assurance, Audit and Certification
  - Assurance
  - Audit
  - Assessment
  - Certification
- Cryptology (Cryptography and Cryptanalysis)
  - Asymmetric cryptography
  - Symmetric cryptography
  - Cryptanalysis methodologies, techniques and tools
  - Functional encryption
  - Mathematical foundations of cryptography
  - Crypto material management (e.g. key management, PKI)
  - Secure multi-party computation
  - Random number generation
  - Digital signatures
  - Hash functions
  - Message authentication
  - Quantum cryptograph
  - Post-quantum cryptography
  - Homomorphic encryption
- Data Security and Privacy
  - Privacy requirements for data management systems
  - Design, implementation, and operation of data management systems that include
  - security and privacy functions
  - Anonymity, pseudonymity, unlinkability, undetectability, or unobservability
  - Data integrity
  - Privacy Enhancing Technologies (PET)
  - Digital Rights Management (DRM)
  - Risk analysis and attacks with respect to de-anonymization or data re-identification (e.g. inference attack)
  - Eavesdropping techniques (e.g. via electromagnetic radiation, visual observation of blinking LEDs, acoustic via keyboard typing noise)
  - Data usage control
- Education and Training
  - Higher Education
  - Professional training
  - Cybersecurity-aware culture (e.g. including children education)
  - Cyber ranges, Capture the Flag, exercises, simulation platforms, educational/training tools, cybersecurity awareness
  - Education methodology
  - Vocational training
- Human Aspects
  - Accessibility
  - Usability
  - Human-related risks/threats (social engineering, insider misuse, etc.)

  - Socio-technical security
  - Enhancing risk perception
  - Psychological models and cognitive processes
  - Forensic cyberpsychology
  - User acceptance of security policies and technologies
  - Automating security functionality
  - Non-intrusive security
  - Privacy concerns, behaviours, and practices
  - Computer ethics and security
  - Transparent security
  - Cybersecurity profiling
  - Cyberpsychology
  - Security visualization
  - Gamification
  - Human aspects of trust
  - Human perception of cybersecurity
  - History of cybersecurity
- Identity Management
  - Identity and attribute management models, frameworks, applications, technologies, and tools (e.g. PKI, RFID, SSO, attribute-based credentials, federated IdM etc.)
  - Protocols and frameworks for authentication, authorization, and rights management
  - Privacy and identity management (e.g. privacy-preserving authentication)
  - Identity management quality assurance
  - Optical and electronic document security
  - Legal aspects of identity management
  - Biometric methods, technologies and tools
- Incident Handling and Digital Forensics
  - Incident analysis, communication, documentation, forecasting (intelligence based), response, and reporting
  - Theories, techniques and tools for the identification, collection, attribution, acquisition, analysis and preservation of digital evidence (e.g. code authorship and attacker identification, provenance assurance, digital evidence correlation, digital evidence triage)
  - Vulnerability analysis and response
  - Digital forensic processes and workflow models
  - Digital forensic case studies
  - Policy issues related to digital forensics
  - Resilience aspects
  - Anti-forensics and malware analytics
  - Citizen cooperation and reporting
  - Coordination and information sharing in the context of cross-border/organizational incidents
- Legal Aspects
  - Cybercrime prosecution and law enforcement
  - Intellectual property rights
  - Cybersecurity regulation analysis and design
  - Investigations of computer crime (cybercrime) and security violations
  - Legal and societal issues in information security (e.g. identity management, digital forensics, cybersecurity litigation)
- Network and Distributed Systems
  - Network security (principles, methods, protocols, algorithms and technologies)
  - Distributed systems security
  - Managerial, procedural and technical aspects of network security
  - Requirements for network security

  - Protocols and frameworks for secure distributed computing
  - Network layer attacks and mitigation techniques
  - Network attack propagation analysis
  - Distributed systems security analysis and simulation
  - Distributed consensus techniques
  - Fault tolerant models
  - Secure distributed computations
  - Network interoperability
  - Secure system interconnection
  - Privacy-friendly communication architectures and services (e.g. Mix-networks, broadcast protocols, and anonymous communication)
  - Network steganography
- Security Management and Governance
  - Risk management, including modelling, assessment, analysis and mitigations
  - Modelling of cross-sectoral interdependencies and cascading effects
  - Threats and vulnerabilities modelling
  - Attack modelling, techniques, and countermeasures (e.g. adversary machine learning)
  - Managerial aspects concerning information security
  - Assessment of information security effectiveness and degrees of control
  - Identification of the impact of hardware and software changes on the management of Information Security
  - Standards for Information Security
  - Governance aspects of incident management, disaster recovery, business continuity
  - Techniques to ensure business continuity/disaster recovery
  - Compliance with information security and privacy policies, procedures, and regulations
  - Economic aspects of the cybersecurity ecosystem
  - Privacy impact assessment and risk management
  - Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling)
  - Capability maturity models (e.g. assessment of capacities and capabilities)
- Security Measurements
  - Security analytics and visualization
  - Security metrics, key performance indicators, and benchmarks
  - Validation and comparison frameworks for security metrics
  - Measurement and assessment of security levels
- Software and Hardware Security Engineering
  - Security requirements engineering with emphasis on identity, privacy, accountability, and trust
  - Security and risk analysis of components compositions
  - Secure software architectures and design (security by design)
  - Security design patterns
  - Secure programming principles and best practices
  - Security support in programming environments
  - Security documentation
  - Refinement and verification of security management policy models
  - Runtime security verification and enforcement
  - Security testing and validation
  - Vulnerability discovery and penetration testing
  - Quantitative security for assurance
  - Intrusion detection and honeypots
  - Malware analysis including adversarial learning of malware
  - Model-driven security and domain-specific modelling languages
  - Self-* including self-healing, self-protecting, self-configuration systems

    - Attack techniques (e.g. side channel attacks, power attacks, stealth attacks, advanced persistent attacks, rowhammer attacks)
    - Fault injection testing and analysis
    - Cybersecurity and cyber-safety co-engineering
    - Privacy by design
- Steganography, Steganalysis and Watermarking
    - Steganography
    - Steganalysis
    - Digital watermarking
- Theoretical Foundations
    - Formal specification of various aspects of security (e.g properties, threat models, etc.)
    - Formal specification, analysis, and verification of software and hardware
    - Information flow modelling and its application to confidentiality policies, composition of systems, and covert channel analysis
    - New theoretically-based techniques for the formal analysis and design of cryptographic protocols and their applications
    - Formal verification of security assurance
    - Cybersecurity uncertainty models
    - Cybersecurity concepts, definitions, ontologies, taxonomies, foundational aspects
- Trust Management and Accountability
    - Semantics and models for security, accountability, privacy, and trust
    - Trust management architectures, mechanisms and policies
    - Trust and privacy
    - Identity and trust management
    - Trust in securing digital as well as physical assets
    - Trust in decision making algorithms
    - Trust and reputation of social and mainstream media
    - Social aspects of trust
    - Reputation models
    - Trusted computing
    - Algorithmic auditability and accountability (e.g. explainable AI)

Appendix 4. Submitted article as pdf

Analysing Finnish Cybersecurity Thesis Topics Using Taxonomic Frameworks

Joonatan Ovaska
Institute of Information Technology
Jamk University of Applied Sciences
Jyväskylä, Finland
joonatan.ovaska@jamk.fi

Karo Saharinen
Institute of Information Technology
Jamk University of Applied Sciences
Jyväskylä, Finland
karo.saharinen@jamk.fi

Tuomo Sipola
Institute of Information Technology
Jamk University of Applied Sciences
Jyväskylä, Finland
tuomo.sipola@jamk.fi

***Abstract*—This paper presents an analysis of Bachelor's and Master's cybersecurity theses in Jyväskylä, Finland. The theses were gathered from publicly available publishing platforms of Finnish universities and were analysed using the NICE Cybersecurity Workforce Framework (NCWF) categories and European Cyber Security Organization's (ECSO) The European Cybersecurity Taxonomy. The aim of this research was to find whether there clearly were emphasis on certain framework categories or work roles. Similarly, industry sectors about which cybersecurity theses were done were of interest. The results can be used by education providers to align and plan their education based on regional needs, and cybersecurity students, before starting their thesis project, can use this information to deliberate suitable work sectors in which theses are lacking. As our research results point out, there is a clear emphasis on certain NICE categories and work roles that are more common within the dataset. However, it is prudent to take into account the scope of the dataset, which was specific to one region in Finland. While this research presents findings about this one region, researchers from around the world can consider using the same research methods on a similar datasets gathered from their respective regions.**

***Index Terms*—Cybersecurity, Education, Thesis, NICE Framework**

I. Introduction

A. Cybersecurity as a Field of Education

Already in 2018, a study in the field of cybersecurity education reviewed and analysed 21 cybersecurity master's programmes with a content, structure, requirements, duration, etc. [1]. A UK case study about cybersecurity education and accreditation analysed this subject in the scope of UK, which was compared to the US [2].

The security committee of Finland was established in 2012 and released a program for the implementation of the national cybersecurity strategy [3] in March 2013. One point of the implementation was to establish cybersecurity education on all levels of the Finnish educational system. Both organisations at the higher education institution (HEI) level in Jyväskylä, Jamk University of Applied Sciences (JAMK) and University of Jyväskylä (JYU), started their master's degrees in cybersecurity around 2013 [4], [5]. JAMK established a bachelor's degree in 2015. Within the decade more and more HEIs in Finland started to establish courses or full degrees in cybersecurity as Lehto and Niemelä point out [6].

B. Government Decrees on the Universities

The HEIs are regulated by Government Decree on Universities of Applied Sciences [7] and Decree on Universities [8], [9]. The mission of the scientific universities of Finland, by law, is to freely further scientific research, provide scientific education and civilise artistically and *interact with the society* . The mission of the universities of applied sciences, by law, is to *practice research, development, innovation and artistic actions to improve working life and regional development* [7].

Ministry of Education and Culture in Finland has written down that studies must have certain structure which includes a thesis project [7]. Each programme leading either to a Bachelor's degree or Master's degree must have a thesis, this also applies to the field of all universities. Theses for this analysis are gathered from programmes in this category and only from publicly available sources. Bachelor's theses are worth of 15 European Credit Transfer and Accumulation System (ECTS) credits and Master's theses from both JAMK and JYU are worth of 30 (ECTS) [10].

II. Literature and Frameworks

A. Degree Levels

For measuring the degree levels of the analysed theses, we can use European Qualifications Framework (EQF) and International Standard Classification of Education (ISCED) for a similar International level system. Leveling system for (EQF) goes from level 1 up to level 8 and (ISCED) from level 0 up to level 8, where level 8 is concidered to be highest level. Level 8 would map to Ph.D. studies while the lowest level 1 is concidered as just only a basic general knowledge. In this paper we concentrate on levels 6 & 7.

Learning outcomes can be mapped as Bachelor's degree for level 6 (EQF) and Master's degree for level 7 (EQF and ISCED) [11] [12], for older ISCED 1997 model the corresponding leveling would be 5A-medium and 5A-long/very long programmes.

B. NICE Framework

National Initiative for Cybersecurity Education (NICE) describes the Workforce Framework for Cybersecurity (NICE Framework or NCWF). The main idea is to map certain skills

and knowledge into a task. The most common use case of the NICE Framework is to assign those into a Work Role. [13]

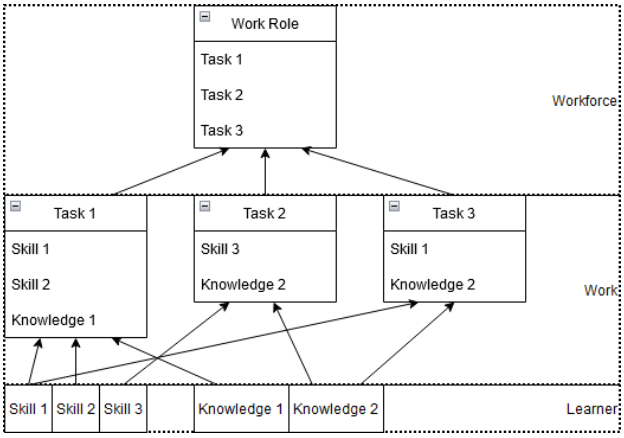

Fig. 1. Work roles' relationship to building blocks.

As the Framework evolved and got more attention, the National Institute of Standards and Technology (NIST) has updated the Framework and mapped work roles into 7 categories. Each of these categories is composed of Specialty Areas, each of which is composed of one or more work roles. Each work role, in turn, includes KSAs and Tasks, see fig 2 and list below. [13]

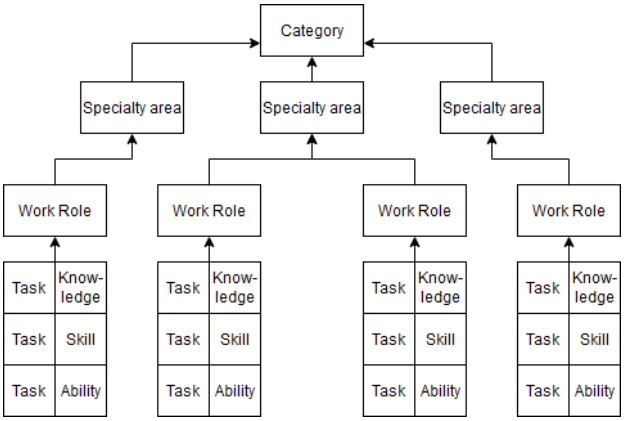

Fig. 2. Relationships among NICE framework components.

- Securely Provision (SP)
  Build secure, conceptualized, procures, designs information technology (IT) systems. Includes specialty areas such as *Technology R&D, Risk Management, Systems Architecture, etc.*
- Operate and Maintain (OM)
  Provides the support, maintance and administration for efficient and effective information technology (IT) system performance and security. Includes specialty areas such as *Network Services, Data Administration, Systems Administration, etc.*
- Oversee and Govern (OV)
  Provides direction, leadership, management or development and advocacy for organisation effective conduct cybersecurity work. Includes specialty areas such as *Strategic Planning and Policy, Legal Advice and Advocacy, Training, Education and Awareness, etc.*
- Protect and Defend (PR)
  Analyses, mitigates and identifies threats to internal information technology (IT) systems and/or networks. Includes specialty areas such as *Vulnerability Assessment and Management, Cybersecurity Defence Infrastructure Support, Cybersecurity Defence Analysis, etc.*
- Analyze (AN)
  Performs specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence. Includes specialty areas such as *Threat Analysis, All-Source Analysis, Exploitation Analysis, etc.*
- Collect and Operate (CO)
  Provides specialized deception and collection and denial of cybersecurity information that may be used to develop intelligence. Includes specialty areas *Cyber Operational Planning, Cyber Operations, Collection Operations*
- Investigate (IN)
  Investigates cybersecurity crimes and/or events related to information technology (IT) systems, digital evidence, and networks. Includes specialty areas *Cyber Investigation, Digital Forensics*

Work roles are not listed here, but for an example here's few given to get the idea what is the meaning of a work role. "Security Architect", "System Administrator", "Exploitation Analyst", "Cyber Crime Investigator". A single Work Role (e.g., Software Developer) may apply to those with many varying job titles (e.g., Software engineer, coder, application developer). Conversely, mulitple roles could be combined to create a particular job.

The NICE Framework does not define proficiency levels (e.g., Basic, Intermediate, Advanced). Such attributes, and those regarding the proficiency with which a learner performs Tasks, are left to other models and resources.

- 7 Cyber Security Workforce Categories
- 33 Specialty Areas
- 52 Work Roles

Framework itself provides freedom of either using existing work roles or creating a new work roles, but this analysis is limited to use only existing work roles within the framework.

Mapping NICE Framework with EQF table can be used to generate a design model for a degree programme within field of cybersecurity. [14]

C. The European Cybersecurity Taxonomy

The European Cybersecurity Taxonomy has reformed to complete more aspects and details than compiting similar Frameworks such as NICE Framework. It covers the most sources compared to other Frameworks as contributions to Cybersecurity Taxonomy. [15]

The goal of the taxonomy is supporting the mapping of the European cybersecurity competencies available. The goal of the taxonomy is not to support the maping of cybersecurity products, services, or processes including oprational activities.

Taxonomy is trying to cluster a complex and multifaceted discipline as cybersecurity needs to be structed on multiple dimensions, capturing not only the core and traditional research domains, but also impacted sectors and application.

This taxonomy is proposed as three-dimensional taxonomy, based on:

- **Research domains** represent areas of knowledge, inluding human, legal, ethical and technological aspects.
- **Sectors** proposed to highlight in scenarios, such as energy, transport or financial sector.
- **Tehnologies and Use Cases** represent the technological enablers to enchance the development of the different sectors.

European cybersecurity taxonomy can be mapped to 15 Cybersecurity Domains which each have respective subdomains (e.g., Domain Cryptology has total of 14 subdomains such as "Asymmetric cryptography", "Symmetric cryptography", "Hash functions", "Random number generation", etc.). Here's full list of main domains:

- Assurance, Audit, and Certification
- Cryptology (Cryptography and Cryptanalysis)
- Data Security and Privacy
- Education and Training
- Human Aspects
- Identity Management
- Incident Handling and Digital Forensics
- Legal Aspects
- Network and Distributed Systems
- Security Management and Governance
- Security Measurements
- Software and Hardware Security Engineering
- Steganography, Steganalysis and Watermarking
- Theoretical Foundations
- Trust Management and Accountability

The European cybersecurity taxonomy maps also different sectors which are described further in the documentation. (e.g., Defence describes as "This sector embraces the activities and infrastructure required for protecting citizen, including the use of aeronautics, space, electronices, land or telecommunication systems".) There are total of 15 sectors, but we are listing only those which had hits within this research:

- Audiovisual and media
- Defence
- Digital Services and Platforms
- Energy
- Financial
- Food and drink
- Government
- Health
- Manufacturing and Supply Chain
- Telecomm Infrastructure

Technologies and Use Cases Dimensions relates to the technologies and uses cases in dimensions. These technologies are used across multiple sectors, there are total of 23 listed items, but we are listing only sectors which had at least one hit within this research:

- Artificial intelligence
- Big Data
- Blockchain and Distributed Ledger Technology (DLT)
- Cloud, Edge and Virtualisation
- Critical Infrastructure Protection (CIP)
- Disaster resilience and crisis management
- Fight against crime and terrorism
- Border and external security
- Local/wide area observation and surveillance
- Hardware technology (RFID, chips, sensors, networking, etc.
- Information Systems
- Internet of Things, embedded systems, pervasive systems
- Mobile Devices
- Operating Systems
- Vehicular Systems (e.g. autonomous vehicles)

III. Dataset, Scoping & Research Method

For the research scope the authors targeted theses done in Central Finland that were publicly available/released over several years which proved to be an big enough dataset to reflect findings. Regional developer scoping was chosen, Jyväskylä is a major player in Finland when it comes to cybersecurity training and education [16] [17]. In Jyväskylä there are 2 Universities which provide cybersecurity education: University of Jyväskylä and Jamk University of Applied Sciences. University of Jyväskylä provides Master's students more theorical approach for cybersecurity. Jamk University of Applied Sciences has ICT engineering programs for both Bachelor's and Master's class Applied Sciences for cybersecurity [18].

Theses done for Jamk University of Applied Sciences can be found publicly from theseus [19] site and use search terms for keywords such as cybersecurity. For University of Jyväskylä theses called pro-gradu, can be found from their system called JYX [20], where these theses are also publicly available. Some of the theses contained appendixes or even whole main thesis as restricted access or hidden based on the Act of the Openness of Government Activities which allows Universities of Applied Sciences and University of Jyväskylä to have thesis which may contain hidden appendixes due research permission for confidential data [21]. Those which has not been scoped out has been determined by the abstract and topic of the thesis.

Theseus is a service for Universities of Applied Sciences for storing and sharing published theses. JYX is a digital archive which collect and display parts of JYX materials including theses from (JYU).

Used research method is mixed methods, quantity of the total scope is 173 theses, which has been qualified to match against the described Frameworks and analysed afterwards. Dataset from JAMK is from 2013 to 2020 and the dataset from JYU from 2018 to 2020. The reasoning for the scope is that this dataset was pregathered for investigation, only some theses were dropped from that dataset for not hitting the scope

of cybersecurity field (e.g. Cybersecurity was only mentioned as a future research, while not being part of thesis itself). The counted total of 173 theses does not include these mentioned unscoped theses.

Most of the theses dataset could have been mapped very differently during the mapping phase these theses are tried to tied only to the category which it fits the most or is the main part of that specific thesis. Same applies for each other mapping done for work role and industry sectors also, when not specified on the orderer side.

IV. Analysis

A. NICE Categories

Based on all the collected theses by the dataset, within fig. 3 we can see the distribution of theses in NICE categories.

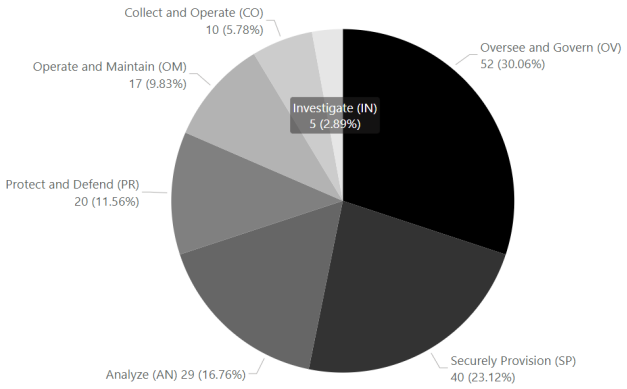

Fig. 3. Theses per NICE category.

Mapping of the we can see that over half of the mapped theses were done for “Oversee and Govern” and “Securely Provision” while categories “Investigate” and “Collect and Operate” were total of less than 10% of the works.

The authors also wanted to compare the differences on each levels of education and education organisation. Thus, we also mapped the weights of each category based on those attributes. This is visualized in fig 4.

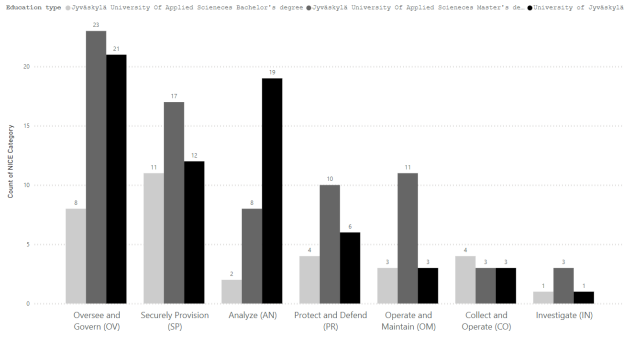

Fig. 4. Mapped categories by education type.

In figure 5 we can see the detailed precentages of category mappings between target universities to highlight the differences and mission between the education types as described by chapter I-B. These precentages are compared towards the total number of theses in the corresponding university.

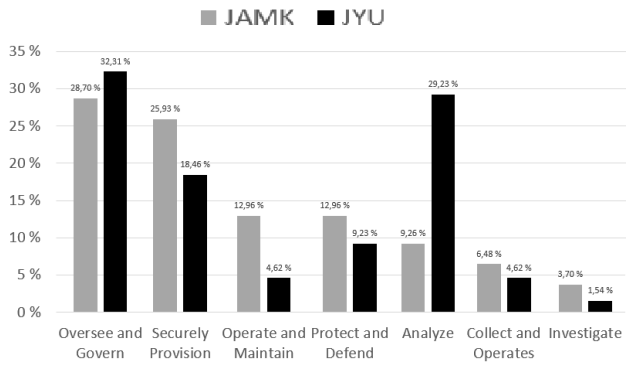

Fig. 5. Mapped categories by education type, total.

In table I we can see the more detailed amounts and precentages of these category mappings between each education type, these precentages are compared to total number of theses.

TABLE I
Categories Mapping Table

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

B. NICE Work Roles

One objective was to map each thesis towards a work role of the framework that was exactly or close to that thesis topic. Total of 37 work roles were present within the analysis. However, only top 15 had five or more hits each. There was also many work roles with only one hit. Here is the top 15 listed provided with the count of mapped roles:

1) Threat/Warning Analyst, 19
2) Reasearch & Development Specialist, 18
3) Cyber Policy and Strategy Planner, 15
4) Vulnerability Assessment Analyst, 11
5) Privacy Officer/Privacy Compliance Manager, 8
6) Cyber Instructor, 7
7) Cyber Legal Advisor, 6

7) Security Architect, 6
9) Cyber Crime Investigator, 5
9) Cyber Instructional Curriculum Developer, 5
9) Cyber Workforce Developer and Manager, 5
9) Network Operations Specialist,5
9) Security Control Assessor, 5
9) System Requirements Planner, 5
9) Systems Security Analyst, 5

These top 15 work roles cover 72.25% of all works. Remaining 27.75% were distributed between other work roles. For mapping each of these top 15 work roles for each education type we can get graph to show us the results as visualized by figure 6.

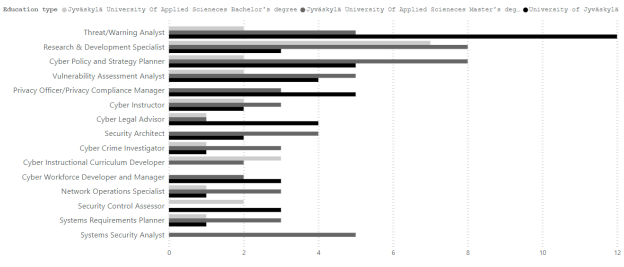

Fig. 6. Mapped work roles by education type.

As the figure shows there is much alteration between education types when mapping into work roles.

C. European Taxonomy, Industry Sectors

Theses done within University of Applied Sciences most of the time have a thesis orderer within the description page and in Scientific Universities this orderer might appear in the contents of the thesis. Given the theses where the orderer appeared, the NICE category thesis can be mapped to an industry sector e.g. telecomm company as an order would map it into "Telecomm Infrasturcture" and most of the institution orders are mapped into "Government".

Theses from University of Jyväskylä are mostly research based, there will be more of mapping with the feeling which industry would be the most relevant for the thesis, while most works would of course map to multiple sectors.

These sectors can indicate where cybersecurity play roles in current life span, obviously the most common sectors are the sectory which are heavily related to information communications technologies and government. Sector mapping listed here:

- **Government** 74, 44.31%
- **Digital Services and Platforms** 58, 34.73%
- **Telecomm Infrastructure** 17, 10.08%
- **Defence** 6, 3.59%
- **Health** 4, 2.4%
- **Financial** 3, 1.8%
- **Energy** 2, 1.2%
- **Audiovisual and media** 1, 0.6%
- **Food and drink** 1, 0.6%
- **Manufactruing Supply Chain** 1, 0.6%

Sectors can be also mapped to NICE categories as shown on the figure 7. For the minor sectors most commonly the work was done in "Securely Provision", while the "Oversee and Govern" was on top of the more common sectors.

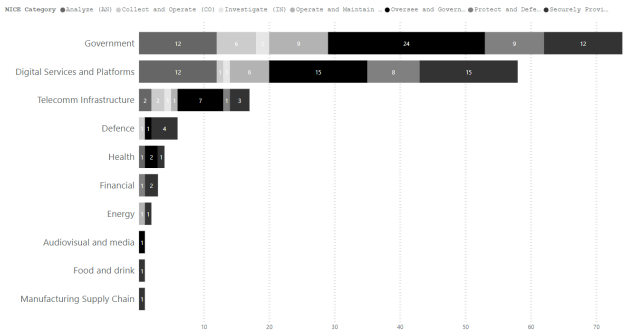

Fig. 7. European Taxonomy sectors mapped to NICE categories.

Theses around very high level of concepts or not a clear way nor order to define sector remained unmapped or has been mapped to most applyable sector.

D. Other Analysis

Used frameworks could lead for more potential findings using different correlations with different options of European Cybersecurity Taxonomy domains, industries or sectors. Instead of mapping to NICE category and NICE work roles, we could map and see how they map into European Taxonomy and compare that result between two different frameworks or just to find the domains under different taxonomy.

V. Discussion

Before making any conclusions the first observation is that neither of these chosen frameworks suits perfectly to this type of analysis. Within the dataset there was a minimal number of theses which suited to just one category of the NICE framework or just one specialty area nor one work role, as already mentioned also in the original NIST documentation.

Comparing to the European Taxonomy proposal, there are more domains in use, however in the opinion of the authors they also overlap, maybe even more than NICE categories do, therefore the NICE categories was chosen as the main target for this study. Also the European Taxonomy offers much in names of technology and sectors, while those sectors might be quite far from the main area of cybersecurity, there could be a connection that those sectors might prefer to purchase these cybersecurity services from another company. This connection is hard to detect as typically theses were done to companies providing these *digital services and platforms* and thus were the assigned orderer of the thesis.

Frameworks are relevant to categorise different fields together and to analyse certain trends that could be emphasised and communicated to interested parties. In case of the work roles, it gives an idea what to study in order to get the work that learner is interested of, however at the same time it is quite common that students should acquire multiple skillsets

in many different work roles. There are not many employers, in Finland, that can have a cybersecurity teams big enough to include each of these work roles within one company.

A. Cybersecurity as a Field

In modern world there is no sector or field that could be totally unplugged or irrelevant to the Internet which leads to the point that in every field there is a need for at least some cybersecurity. More and more devices from IoT and any other embedded system will be connected to Internet if not already. Even the industrial factories where the common ideology has been that each of the factory controlling device is plugged offline there is always a part when someone with a lack of understanding or just by accident could attach this unit to public Internet. Sometimes it could be a worker who wants to work from home fex. Covid-19 issues or maybe a business fusion with another company which has joined to the same area network.

While cybersecurity as a field is growing fast, in terms of student theses and research, this growth is not apparent in all industry sectors. However, the trend can be seen from the researched dataset already, cybersecurity is not anymore just for the most obvious sectors as in ICT, government, digital platforms, cloud computing, but it is for all.

VI. Conclusion

A. Effects of the Education Level

Since the theses were pointing to EQF levels 6 & 7, there is an effect that can be seen from the results and should be noted when making conclusions. For example basic cybersecurity work incident responder role didn't get a single match in this analysis, while it might be a common work role in the industry for lower level of education (EQF levels 4 & 5). Meanwhile, there wer many theses which related to incident response as a concept, but the thesis had more of a planning or developing nature, therefore there a different work role was selected.

Not only the level of education is pushing these results to aim higher or more advanced levels, but also the workload of the thesis project. EQF level 6 studies has approximately 400 hours workload and EQF level 7 studies has approximately 800 hours of workload for thesis project of chosen research study that could be pure research or combination of doing implementation for chosen topic. This will effect the targeted work role as the workload is not too small the project is often pushed towards the mapping of higher hierarchy workforce.

B. Differences Between the Universities

For the chosen fields and subjects there could be seen trends between the two universities. JAMK students more often related their work, that could be at least somewhat correlated, to provided courses. Meanwhile, JYU theses more often included analytical research than implementations.

As figure 5 shows JAMK theses are more often towards categories "Securely Provision", "Operate and Maintain", "Protect and Defend", while JYU theses maps more often towards "Oversee and Govern" and "Analyze".

C. NICE Categories

While the dataset has least amount of data from Bachelor's degree theses they still pointed out to be much more focused on implementations by having a comperable high amount of works for "Securely Provision" and "Protect and Defend", also the third biggest total category analyze had only 2 works from Bachelor's level, mean while it was huge in (JYU) Master's theses, while not the first one, which was Oversee and Govern, which is somewhat same nature with the analysis category.

Investigate category has only 3 work roles and 2 specialty areas in it, and that could be also seen from these works that it's more rare to thesis land in this area, also there could be much of work loads which is not a good idea to give for a thesis project, being criminal investigation etc. Meanwhile there is definately work roles that exists in the real world, while it is clear that theses aren't done within these lines of work based on our research data.

The most mapped category, "Oversee and Govern", suits probably the best to these levels of research, I wouldn't say that there is not that much of work roles in work life as there was mapped theses for that category. Meanwhile there definately is work roles, it might not just be as big of a field that these statistics are providing.

D. NICE Work Roles

Surprisingly, there was one work role that stood clearly, with four (4) as clear leaders. "Threat/Warning analyst" was clearly the most mapped work role, while also "Research & Development Specialist" was the 2nd most mapped work role in this analysis. "Cyber Policy and Strategy Planner" and "Vulnerability Assessment Analyst" were both mapped over 10 times. Theses from JYU were clearly most mapped to "Threat/Warning Analyst", while Bachelor's theses' most common mapping was "Research & Development Specialist". Other top 4 work roles were quite even among different education types. Something to mention outside the top 4 is that all 5 works mapped to "Systems Security Analyst" were exclusively from the University of Applied Sciences Master's thesis.

Another interesting finding was that while University of Jyväskylä concentrated more on works around research fields, there were no mappings for "Cyber Instructional Curriculum Developer" work role. However, this might reflect the fact that these theses were extracted from the IT field including Cybersecurity as a search parameter and those works might be done for different fields of studies, e.g., Teacher Education.

E. European Taxonomy Industry Sectors

European Taxonomy Industry Sectors had hits only for about half of the industries. Meanwhile, multiple sectors had one hit in the complete dataset. In the rare cases they were mostly "Securely Provision" hits, which are more often implementation or system requirement based hits. If we would look the non-top 3 hits without "Securely Provision" works included, the amount of works and industries would cut lower than 50%.

The methodology in the University of Applied Sciences on thesis projects encourages to find a commissioner for the thesis, therefore the mappings to rare industries were because of these commissioners. The other two industries that gained considerable amount of theses were from Health and Financials in the data from University of Jyväskylä. Health as an industry and as a regional determiner play a big role when looking at the location of Jyväskylä in Central Finland. There is a new hospital built recently and opened in early 2021 [22] [23]. These theses were done before that time, but could be related to that project.

F. Other Observations

NICE Framework is suitable for obtaining data when asking where the work is and what kind of work orders have been given. Also, the courses and the nature of studies played a role in the thesis categories. This dataset scope can be used for regional education development while it also gives an example for future research and possibilities in other geographic locations.

While the framework makes this mapping possible, there is room for subjective evaluation: another person could map some of the works differently by weighting the main topic differently, while it could be technically possible to map same works with multiple attributes. The authors considered the possibility, but concluded to go with only one category per thesis. More advanced mathematical analysis methods could be used to investigate the dataset. However, the authors could draw up relevant conclusions with the analysis methods used in this paper.

G. Future Research

This data could be used to improve regional focus of education. This could be achieved by developing courses towards the work roles, categories and industries that were found during this work. These findings can also be used internationally to reflect the current state and to compare to other regions or perform similar research as an inspiration. With this dataset there are possibilities to look at other aspects concerning the topic or carry out research around European Taxonomy Domains mapping analysis.

ACKNOWLEDGMENT

This research was supported by European Social Fund 2021–2023 as part of the LIPPA research and development project which is supporting smooth transitions from ICT studies to work life [24].

REFERENCES

[1] K. Cabaj, D. Domingos, Z. Kotulski, and A. Respício, "Cybersecurity education: Evolution of the discipline and analysis of master programs," *Computers & Security*, vol. 75, pp. 24–35, 2018.

[2] T. Crick, J. H. Davenport, A. Irons, and T. Prickett, "A uk case study on cybersecurity education and accreditation," in *2019 IEEE Frontiers in Education Conference (FIE)*, 2019, pp. 1–9.

[3] The Security Committee, "Implementation programme for Finland's cyber security strategy," pp. 47–48, 2014, (in Finnish), retrieved May 21, 2022. [Online]. Available: https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Kyberturvallisuusstrategian-toimeenpano-ohjelma.pdf

[4] University of Jyväskylä, "MSc cyber security," n.d., retrieved June 3, 2022. [Online]. Available: https://www.jyu.fi/it/fi/opiskelu/maisteriohjelmat/kyberturvallisuus/masters-degree-programme-in-cyber-security

[5] JAMK University of Applied Sciences, "Educate yourself to be a cyber security professional," n.d., retrieved May 31, 2022. [Online]. Available: https://www.jamk.fi/en/Apply-to-Jamk/masters-degree/educate-yourself-to-be-a-cyber-security-professional

[6] M. Lehto and J. Niemelä, *Kyberalan tutkimus ja koulutus Suomessa 2019*, ser. Informaatioteknologian tiedekunnan julkaisuja, P. Neittaanmäki, Ed. Jyväskylä: University of Jyväskylä, 2019, no. 83/2019, retrieved May 30, 2022. [Online]. Available: https://www.jyu.fi/it/fi/tutkimus/julkaisut/it-julkaisut/kyberalan_koulutus_suomessa_verkkoversio.pdf

[7] Ministry of Education and Culture, "Government decree on universities of applied sciences," 2014, retrieved May 21, 2022. [Online]. Available: https://finlex.fi/en/laki/kaannokset/2014/en20141129.pdf

[8] "Valtioneuvoston asetus yliopistojen tutkinnoista," 2004, 794/2004, retrieved May 30, 2022. [Online]. Available: https://www.finlex.fi/fi/laki/alkup/2004/20040794#Pidp446675200

[9] "Yliopistolaki," 2004, 24.7.2009/558, retrieved May 30, 2022. [Online]. Available: https://www.finlex.fi/fi/laki/ajantasa/2009/20090558

[10] E. Commission, "Ects users' guide 2015," p. 11, 2015, retrieved May 25, 2022. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/da7467e6-8450-11e5-b8b7-01aa75ed71a1

[11] European Commission, "European qualifications framework," 2017, retrieved May 25, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017H0615(01)&qid=1552997420044&from=EN

[12] UNESCO Institute of Statistics, "International standard classification of education isced 2011," 2011, retrieved May 25, 2022. [Online]. Available: https://web.archive.org/web/20170106011231/https://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-isced-2011-en.pdf

[13] National Institute of Standards and Technology, "Workforce framtework for cybersecurity (NICE framework)," 2020, retrieved May 25, 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

[14] K. Saharinen, M. Karjalainen, and T. Kokkonen, "A design model for a degree programme in cyber security," in *Proceedings of the 2019 11th International Conference on Education Technology and Computers*, ser. ICETC 2019, 2019, pp. 3–7.

[15] European Commission, "A proposal for a european cybersecurity taxonomy," 2019, retrieved May 26, 2022. [Online]. Available: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

[16] R. M. Savola, "Current level of cybersecurity competence and future development: case Finland," in *Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings*, ser. ECSA '17, 2017, pp. 121–124.

[17] M. Lehto, "Cyber security competencies: cyber security education and research in finnish universities," in *Proceedings of the 14th European Conference on Cyber Warfare & Security*, ser. ECCWS 2015, 2015, pp. 179–188. [Online]. Available: http://urn.fi/URN:NBN:fi:jyu-201507092560

[18] Ministry of Education and Culture, "Agreements with universities of applied sciences," n.d., (in Finnish), retrieved May 31, 2022. [Online]. Available: https://okm.fi/ammattikorkeakoulut-sopimukset

[19] Arene ry, "Database for theses from universities of applied sciences in finland," n.d., retrieved May 31, 2022. [Online]. Available: https://www.theseus.fi/

[20] University of Jyväskylä, "Jyväskylä university digital repository," n.d., retrieved May 31, 2022. [Online]. Available: https://jyx.jyu.fi/?locale-attribute=en

[21] Ministry of Jucstice, "Act on the openness of government activities," 2015, 621/1999, amendments to 907/2015 included, retrieved May 31, 2022. [Online]. Available: https://www.finlex.fi/en/laki/kaannokset/1999/en19990621_20150907.pdf

[22] Keski-Suomen sairaanhoitopiiri, "Move to new hopital was success," 2021, retrieved May 31, 2022. [Online]. Available: https://www.sairaalanova.fi/fi-FI/Ajankohtaista/Muutto_Sairaala_Novaan_sujui_erinomaises(62659)

[23] ——, "Organising and producting health and social services in central finland 2021-2023," 2021, retrieved May 31, 2022.

[Online]. Available: https://www.sairaalanova.fi/fi-FI/Sairaanhoitopiiri/Terveydenhuoltolain_mukainen_jarjestamis(62970)
[24] Ministry of Employment and the Economy, “LIPPA quality for ICT studies from the working life interface,” 2021, retrieved May 31, 2022. [Online]. Available: https://www.eura2014.fi/rrtiepa/projekti.php?projektikoodi=S22466