



Analysing Finnish Cybersecurity Thesis Topics Using Taxonomic Frameworks

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

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

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

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

Index Terms—Cybersecurity, Education, Thesis, NICE Framework

I. INTRODUCTION

A. Cybersecurity as a Field of Education

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

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

B. Government Decrees on the Universities

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

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

C. Our contribution

This research categorizes the thesis topics from two Finnish universities according to taxonomic frameworks. This is done to map the topics to industry and workforce needs and gain insight into how well the educational outcomes correspond to the frameworks. This is a rarely studied topic, especially within the context of the Finnish educational system.

II. LITERATURE AND FRAMEWORKS

A. Degree Levels

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

Learning outcomes can be mapped as Bachelor’s degree for level 6 (EQF) and Master’s degree for level 7 (EQF and

ISCED) [11] [12], for older ISCED 1997 model the corresponding leveling would be 5A-medium and 5A-long/very long programmes.

B. NICE Framework

National Initiative for Cybersecurity Education (NICE) describes the Workforce Framework for Cybersecurity (NICE Framework or NCWF). The main idea is to map certain skills and knowledge into a task. The most common use case of the NICE Framework is to assign those into a Work Role. [13] The work roles and building blocks are illustrated in Figure 1.

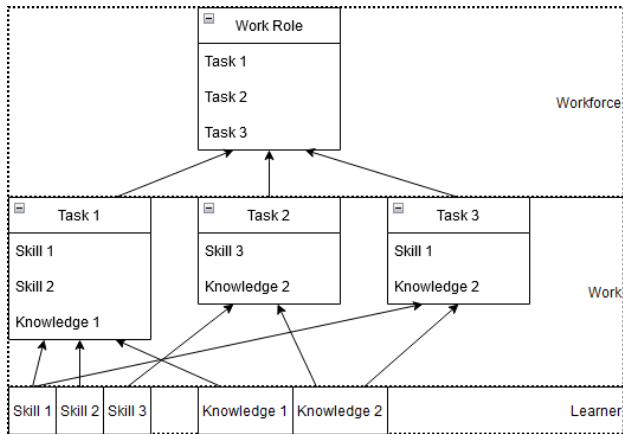


Fig. 1. Work roles' relationship to building blocks.

As the Framework evolved and got more attention, the National Institute of Standards and Technology (NIST) has updated the Framework and mapped work roles into 7 categories. Each of these categories is composed of Specialty Areas that contain one or more work roles. The work roles contain KSAs and Tasks, see Figure 2 and list below. [13]

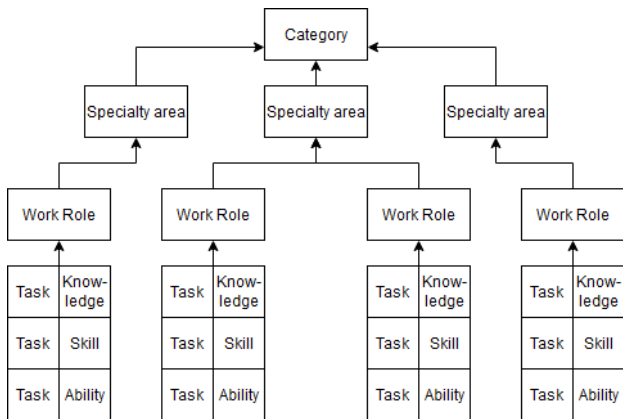


Fig. 2. Relationships among NICE framework components.

- Securely Provision (SP)
Build secure, conceptualized, procures, designs information technology (IT) systems. Includes specialty areas such as *Technology R&D, Risk Management, Systems Architecture, etc.*

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

Work roles are not listed here, but a few examples are given as examples to get the idea what is the meaning of a work role: “Security Architect”, “System Administrator”, “Exploitation Analyst”, “Cyber Crime Investigator”. A single Work Role (e.g., Software Developer) could cover multiple actual job titles (e.g., software engineer, coder, application developer). A combination of roles could also be used to form a job description.

There are no definitions for proficiency levels (e.g., Basic, Intermediate, Advanced) in the NICE Framework. Proficiency levels and attributes describing how a learner performs Tasks, are covered by other models and resources.

NICE Framework has the following parts:

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

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

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

C. The European Cybersecurity Taxonomy

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

The goal of the taxonomy is to support the mapping of the European cybersecurity competencies available. However, the taxonomy is not meant for cybersecurity products, services or processes, including operational activities.

Cybersecurity is a complex and multifaceted discipline, which leads to the need to cluster it meaningfully. The taxonomy is structured as a multi-dimensional representation of the core and traditional research domains. At the same time, it tries to take into account impacted sectors and application.

This taxonomy is proposed as three-dimensional taxonomy:

- **Research domains** represent areas of knowledge, including human, legal, ethical and technological aspects.
- **Sectors** for scenarios, such as energy, transport or financial sector.
- **Technologies and Use Cases** are the technological enablers to enhance the development of the sectors.

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

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

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

- Audiovisual and media
- Defence
- Digital Services and Platforms
- Energy
- Financial

- Food and drink
- Government
- Health
- Manufacturing and Supply Chain
- Telecomm Infrastructure

Technologies and Use Cases Dimensions relates to these topics in the dimensions. Many sectors use these technologies, as there are total of 23 listed items, but we are listing only sectors which had at least one hit within this research:

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

III. DATASET, SCOPING & RESEARCH METHOD

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

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

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

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

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

IV. ANALYSIS

A. NICE Categories

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

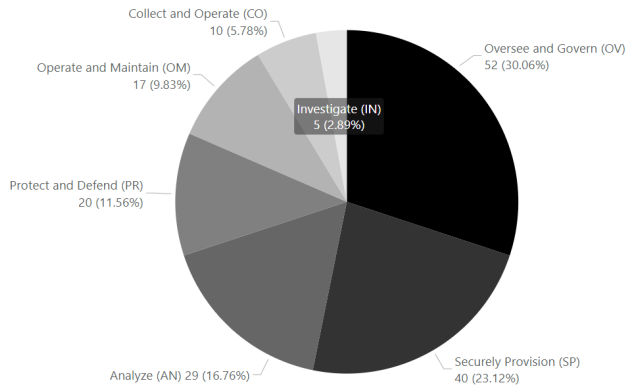


Fig. 3. Theses per NICE category.

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

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

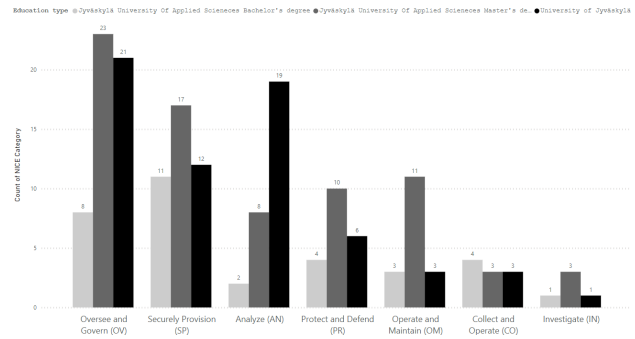


Fig. 4. Mapped categories by education type.

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

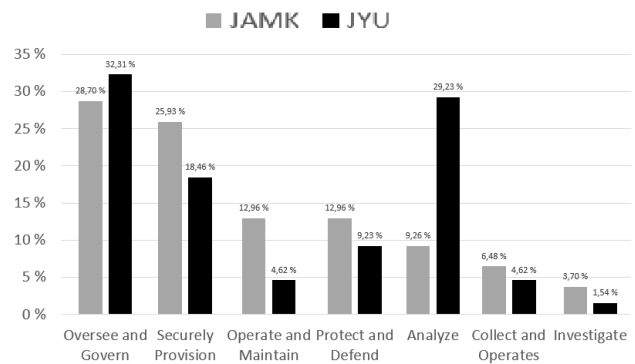


Fig. 5. Mapped categories by education type, total.

In table I we can see the more detailed amounts and percentages of these category mappings between each education type, these percentages 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) Research & Development Specialist, 18
- 3) Cyber Policy and Strategy Planner, 15
- 4) Vulnerability Assessment Analyst, 11
- 5) Privacy Officer/Privacy Compliance Manager, 8
- 6) Cyber Instructor, 7
- 7) Cyber Legal Advisor, 6
- 7) Security Architect, 6
- 9) Cyber Crime Investigator, 5
- 9) Cyber Instructional Curriculum Developer, 5
- 9) Cyber Workforce Developer and Manager, 5
- 9) Network Operations Specialist, 5
- 9) Security Control Assessor, 5
- 9) System Requirements Planner, 5
- 9) Systems Security Analyst, 5

These 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.

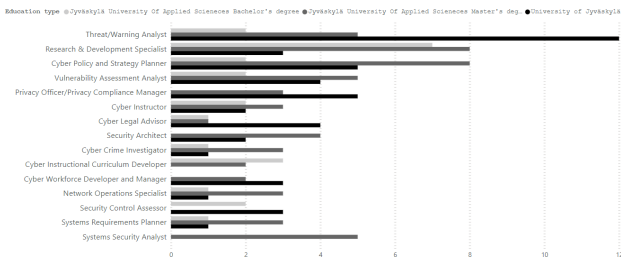


Fig. 6. Mapped work roles by education type.

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 Infrastructure” 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 sector 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%
- **Manufacturing 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.

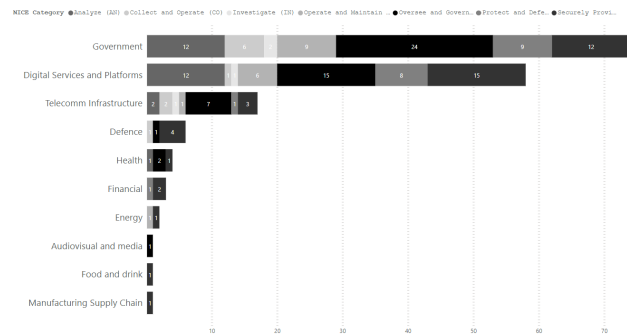


Fig. 7. European Taxonomy sectors mapped to NICE categories.

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 applicable 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 these 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. 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 were 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 comparable 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 definitely work roles that exists in the real world, while it is clear that these 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 definitely 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#Pdp446675200>
- [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](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-iscd-2011-en.pdf>
- [13] National Institute of Standards and Technology, “Workforce framework 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 Justice, "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 hospital was success," 2021, retrieved May 31, 2022. [Online]. Available: [https://www.sairaanova.fi/fi-FI/Ajankohtaista/Muutto_Sairaala_Novaan_sujui_erinomaises\(62659\)](https://www.sairaanova.fi/fi-FI/Ajankohtaista/Muutto_Sairaala_Novaan_sujui_erinomaises(62659))
- [23] —, "Organising and producing health and social services in central finland 2021-2023," 2021, retrieved May 31, 2022. [Online]. Available: [https://www.sairaanova.fi/fi-FI/Sairaanhoitopiiri/Terveystuolain_mukainen_jarjestamis\(62970\)](https://www.sairaanova.fi/fi-FI/Sairaanhoitopiiri/Terveystuolain_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/rtiepa/projekti.php?projektkoodi=S22466>