Researching Graduated Cyber Security Students: Reflecting Employment and job Responsibilities Through NICE Framework

Karo Saharinen, Jarmo Viinikanoja and Jouni Huotari
JAMK University of Applied Sciences, Jyväskylä, Finland
karo.saharinen@jamk.fi
jarmo.viinikanoja@jamk.fi
jouni.huotari@jamk.fi

Abstract: Most research and development on Cyber Security education is currently focusing on what should be taught, how much, and where within the degree programmes. Different Cyber Security frameworks are currently evolving to include Cyber Security education parallel to older paradigms of Computing Education, existing alongside with such as "*Information Technology"* and "*Software Engineering"*. Different Cyber Security specialisations or even whole degree programmes have started within universities before the frameworks have been defined into standardised degree structures. This is mainly the result of a dire industry need of well-educated cyber security personnel, a phenomenon affecting the industry globally. Our research concentrates on Finnish alumni students who have already graduated from a bachelor's degree programme in Information Technology with a specialisation in Cyber Security in Finland. Within our gathered research data, we analysed what is the industry sector where their current job resides, and what are the cyber security responsibilities in their current work. The questionnaire also contained an after-reflection section where the graduated students could choose what they would study were they about to start and plan their studies again. The results verify that Cyber Security is still the most favoured specialisation within the former Cyber Security alumni students. Slight variation is evident from the data, which in the authors' perspective, verifies the multifaceted nature of Cyber Security. When analysing alumni students' job responsibilities, the main category of work resides in the "*Protect and Defend"* category of the NICE Framework, which in the terms of the conference, relates to Critical Infrastructure Protection being the main subject of employment for fresh graduates. These results give insight to other education organisations on how to develop their curricula to further emphasise the employment of students or to offer modules which are of interest for newly employed Cyber Security professionals. In addition, it gives an insight of industry demand for freshly graduated students within the target group.

Keywords: cyber security, degree programme, cybersecurity skills

1. Introduction

Cyber Security capability building is a world-wide phenomenon where different nations are either gathering or developing tools, training people (Catota et al, 2019) and perfecting their processes to an extent that some might even call a cyber arms race (Limnéll, 2016). This paper concentrates on researching the training of cyber security professionals through the education systems of a country. An undertaking which is simultaneously answering to an evident workforce need of a functioning industry (Jaurimaa et al, 2020) and the national cyber resilience levels of a country (Whyte, 2020). Both of which are targeted by threats coming from the cyber domain affecting e.g. the critical infrastructure of a country or the information security of a nation.

To answer this need of cyber security professionals, degree programmes fully dedicated to Cyber Security are being established in the Higher Education institutions of different countries. European Union Agency for Cybersecurity (ENISA) established Cybersecurity Higher Education Database (CyberHEAD) to map these degree programmes (Zan De & Di Franco, 2019). Criteria for degree programme approval were:

- 25 percent of *cyber security topics* for bachelor's degrees
- 40 percent of *cyber security topics* for master's degrees
- and research on *cyber security topics* for PhD students

At the time of writing this paper, there are 139 programmes in 25 countries that are approved in CyberHEAD (ENISA, 2021). Within these 139 programmes the word cyber security appeared in the title of 13 out of 23 bachelor's degrees, 56 out of 105 master's degrees and in none of the three PhD programmes (and 0 out of 8 specialiation postgraduate courses). This emphasises that almost half of the degrees are titled and focused on other areas of Computing. However, they contain the percentage required in *cyber security topics* to be a part of CyberHEAD.

2. Literature review

As described by the introduction chapter, the *cyber security topics* in use at CyberHEAD were defined by ENISA (Zan De & Di Franco, 2019) to be aligned with Joint Task Force on Cybersecurity Education called CSEC2017 (Associate for Computing Machinery, 2017), which is published by the Association for Computing Machinery (ACM) in their collection of curricula recommendations (Associate for Computing Machinery, n.d.). These recommendations were published to emphasise Cyber Security as a paradigm of Global Computing Education. An aspect which was lacking in the ACM Curricula Recommendations of 2005 (Shackelford et al, 2005). ACM recently published their Curricula Recommendations 2020 (CC2020 Task Force, 2020), which stabilised the presence of Cybersecurity as a full paradigm of computing next to older topics such as *"Information Technology*" and *"Software Engineering"* to name a few.

Alongside these developments the National Institute of Science and Technology (NIST) released National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework in 2017 (Newhouse et al, 2017), which described the knowledge, skills and tasks in different categories and workroles within Cyber Security. The framework aspired to partner academia, private and public sector to provide comprehensive material to improve workforce development in education and training within the United States of America. In the UK, as put forth by the UK Cyber Security Strategy (United Kingdom, 2016), The Cyber Security Body of Knowledge was released in 2019 by version 1.0 (Rashid et al, 2019) and 2021 with version 1.1.0 (Rashid et al, 2021) respectively. It is a simplification if stated that both are quite similar in their agendas and goals.

Similar projects were conducted in the European Union in two different research and development projects; SPARTA and Cyber Security for Europe (CS4E). SPARTA released their "*Cybersecurity skills framework"* in 2020 (Piesarskas et al, 2020), but based a part of their work on the NICE framework. A very similar undertaking was developed under the Cyber Security for Europe (CS4E) project in Work Package 6 with a topic of Cybersecurity Skills & Capability Building. The work package released a Deliverable on "*Design of Education and Professional Framework*" in 2021 (Karinsalo et al, 2021).

Many skills framework documents were motivated by the worldwide need of Cybersecurity Workforce. This topic was declared as follows: *"The cybersecurity skills shortage and gap are well-documented issues that are currently having an impact on national labour markets worldwide*", a direct quote from a publication of ENISA released on 24th of November 2021 titled "Addresing Skills Shortage and Gap Through Higher Education" (Nurse et al, 2021), released just prior to writing this research paper. This shortage was referenced by seven different sources, divided regionally here to be from European Union, UK, North America, Central and South America, Asia and Australia. This emphasises the fact that there is a world wide need of Cyber Security Professionals. Even the newly published cyber security strategy of the European Union (European Comission, 2020) states this lack of professionals, but with fewer references. These parallelly generated frameworks, curriculum guides, and different publications prove an evident background and need of establishing cyber security focused education.

Finland published its first Cyber Security Strategy on 24 January 2013 as a government resolution (The Security Committee of Finland, 2013). The strategy declared different goals and operation models to meet the challenges of the cyber domain and ensure the fuctionality of the cyber domain. The first version of the strategy contained a sentence declaring *"The study of basic cyber security skills must be included at all levels of education"*. This was further enforced in the updated strategy (The Security Committee of Finland, 2019) that all cyber and information and communications technology (ICT) related training/degree programmes will be strengthened.

The first Finnish strategy can be seen as a clear point in time when Higher Education institutions in Finland began to start degree programmes purely dedicated to cyber security. JAMK University of Applied Sciences (JAMK) and University of Jyväskylä (JYU) both launched a master's degree programme on purely cyber security in 2013 (JAMK University of Applied Sciences, 2013) (University of Jyväskylä, 2013). JAMK also started a bachelor's degree with a cyber security specialisation in 2015 (JAMK University of Applied Sciences, 2015). Afterwards many other Universities of Applied Sciences and Universities in Finland followed with their own offering of Cyber Security, be it degree-oriented curricula (South-Eastern Finland University of Applied Sciences, 2021) or just specialisation studies for life-long learning with no official degree completion (Metropolia University of Applied Sciences, 2021). This timeline of frameworks and degree oriented higher education is further visualised in the Figure 1.

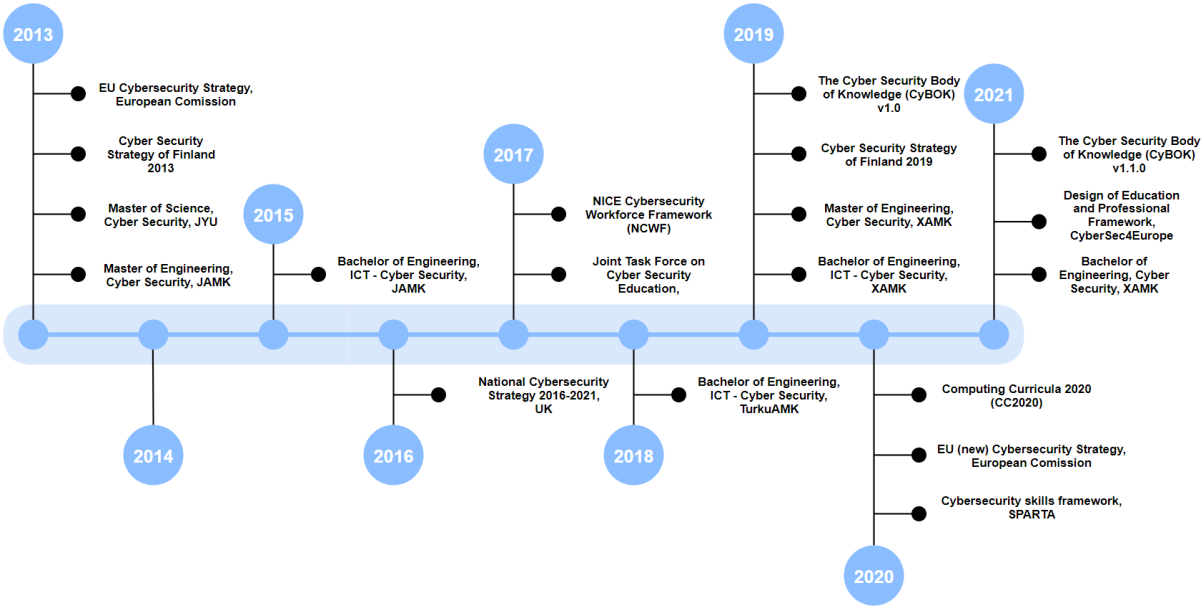

Figure 1: Timeline of cyber security frameworks, Finnish cyber security strategies and degree programmes

3. Survey research on graduated students

This research was scoped to concern graduated bachelor's degree students of JAMK University of Applied Sciences with a cyber security specialisation in their degree. The degree programme was started in 2015 and has a recommended length of 4 years (240 ECTS). Thus, the first students to graduate according to the recommended timetable should have been around 2019. Noteworthy is that these students were the first graduates within Finland to have a cyber security focus in their bachelor's degree.

The research was designed to directly involve the university in contacting the students, however it proved to be a troublesome task. Cyber Security students, by the nature of their studies presumably, had marked that their contact information should not be used for research purposes, nor should they be contacted later by the university. Thus, the research permission process of the university granted no results for student contact information.

This result of the permission process forced the researchers of this paper to contact the students through different social media platforms; asking the students publicly to inform of their willingness for the research by contacting the researchers personally. Luckily few active students could be found which then forwarded the request to attend the research to more specific and limited messaging groups of the students. To increase the reliability of the research, one aspect was that the questionnaire was handed only to graduated students who had directly contacted the researchers and been identified as former students. This resulted in 19 respondents out of 68 graduated, thus sample size from the total possible participants was 27.94%.

The research method used was a survey containing mostly quantitative measurements of the participants. Research ethics were used design the questionnaire in a way that would give the researchers the necessary information, and then the replies were generalised (e.g., specific company to be "private/public company") so that no singular student could be identifiable from the data.

As the literature review stated, there are multiple frameworks possible of data categorisation/analyzation. In this research the NICE Framework was chosen to categorise and analyse the work roles of researched participants. The Framework has descriptive terminology on each work responsibility assigned to each work role. Because of this, the NICE framework was something that the students were requested to examine, if they had doubt in selecting what work role described their profession the best.

4. Survey results and analysis

This chapter divides into two different sections; place of employment answers the research question "Where are graduated students employed?" and type of work answering, "What kind of work responsibilities do the students have?".

4.1 Place of employment

First question concerned the student's starting year and graduation year to get a glimpse of the length of their studies. This is visualised in the Figure 2 in which the darker color shows the total count of started degree studies of each year, and the lighter color represents the total count of graduations of each year within our sample group.

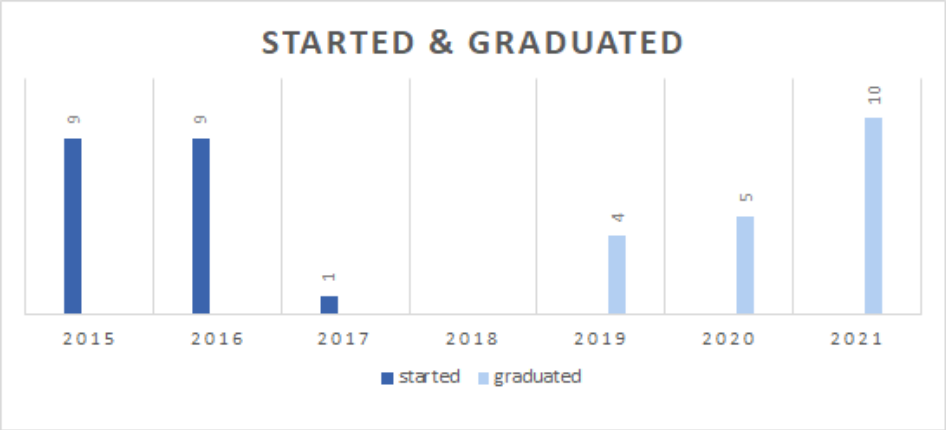

Figure 2: Starting year compared to graduation year

It is evident that even though almost half of the respondents started their studies in 2015, still many graduated behind schedule in 2020 and 2021. The authors interpret this could be the result of e.g. fast employment during studies as ICT degrees do not need to be finished to start working in the industry which results to delaying the graduation of a student. Although other reasons might be as plausible as proved by other research (Willoughby et al, 2021). Unfortunately, within our research this reason of delay was not a separate question.

One of the main research objectives was to find out where the bachelor's degree students get employed, which industry sector and company size. These are apparent in the data gathered and visualised in the Figure 3.

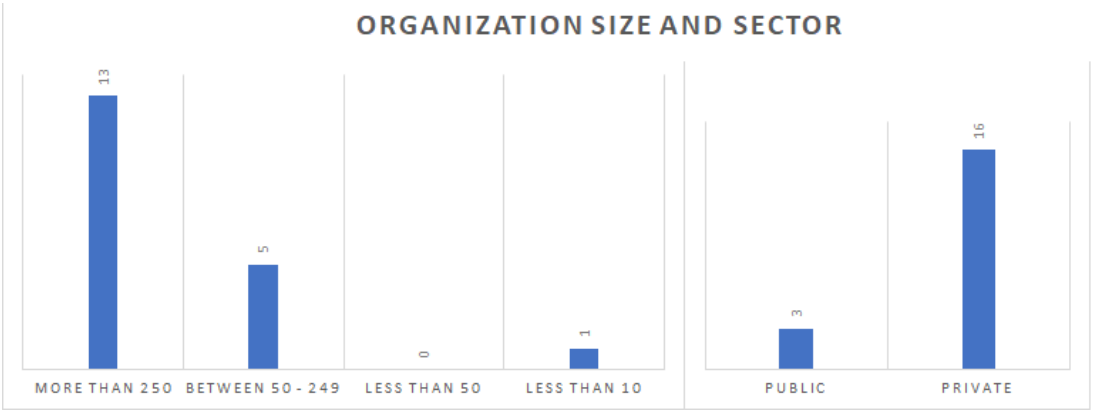

Figure 3: Organisation size and sector

Within these results, neither the employment sector nor company size surprised the authors. In Finland, the growing cyber security sector seems to follow the same footsteps as the global phenomenon. The European Cyber Security Strategy (European Comission, 2020) states that *"Over two-thirds of companies, in particular Small to Medium Enterprises (SMEs) are considered 'novices' in cyber security…"*. This stated need for protection can be witnessed from the service offering of private cyber security companies in Finland. These provided services need workforce behind them and thus, graduated bachelor's degree students get employed.

Given the employment, these companies can be dissected further based on their industry sector. A proposal for a European Cybersecurity Taxonomy (Nai Fovino et al, 2019) declared industry sectors which were utilised in the data categorisation of this research. Students' employment information was translated into these sectors as represented by figure 4.

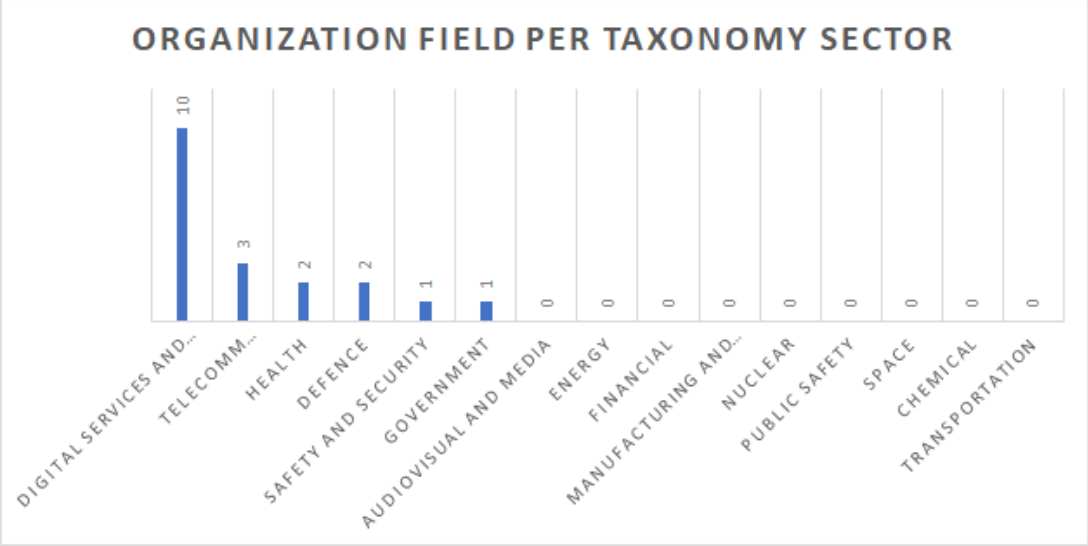

Figure 4: Employment sector of students based on a proposal for a European cybersecurity taxonomy

Out of these sectors, the business to business (B2B) companies were most apparent. Most of them categorising under the "*Digital services and platforms"* sector of the taxonomy. "*Telecomm infrastructure*" had significant Internet Service Providers (ISPs) of Finland recruiting some students, but for reliability sake it is worth metioning that some of the "*digital services and platforms*" were subsidiary organisations of the previously mentioned ISPs. Thus, based on analysis interpretation of the organisations, these two were the largest employers. "*Health"* and "*Defence"* sectors have employed two students both with "*Defence"* being the majority of public organisation employers. *"Government"* and *"Safety and Security"* sectors followed, but there are no results of other sectors within this survey scope.

4.2 Type of work

As for the following results, we asked the students to place emphasis on the question of "what work role of the NICE framework describe their work the most?". As the quantitative grading scheme, we asked them to place the work roles in 1st to 5th order where the 1st being the most descriptive work role for their current work and 2nd being the second most descriptive work role etc. Figure 5 shows a graph of the whole data.

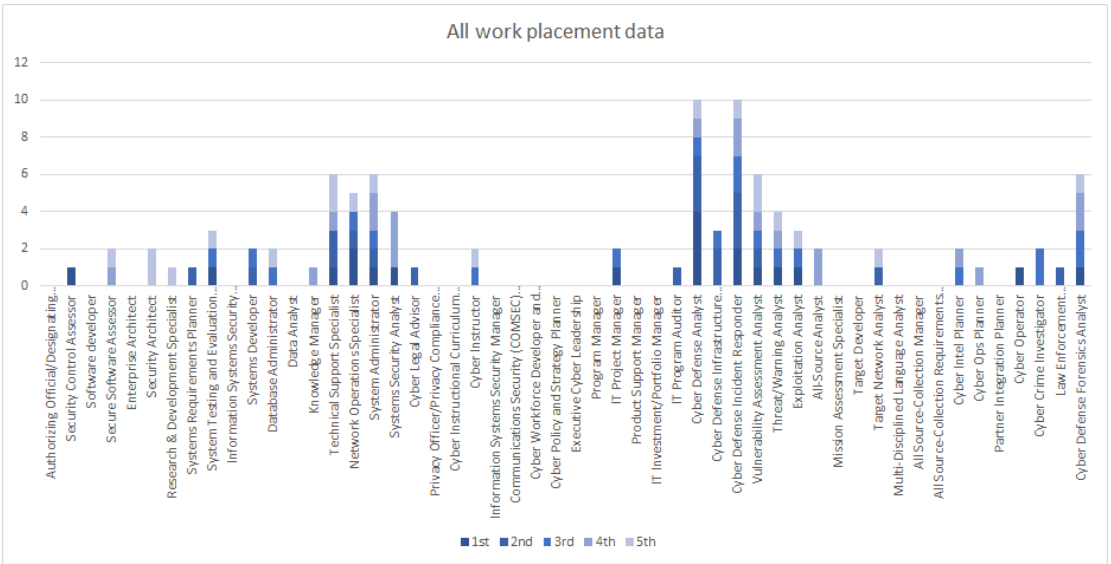

Figure 5: Top NICE categories based on what best fit their work

As there are 52 work roles described by the NICE Framework, Figure 5 is quite extensive or even hard to differentiate, but clear emphasises can already be observed from the visualization. To illustrate the work responsibilities more informatively, we used the frameworks categories to further delve into the data and order it from the most hit category (up top) and the least hit category (on bottom) as visualised in the Figure 6.

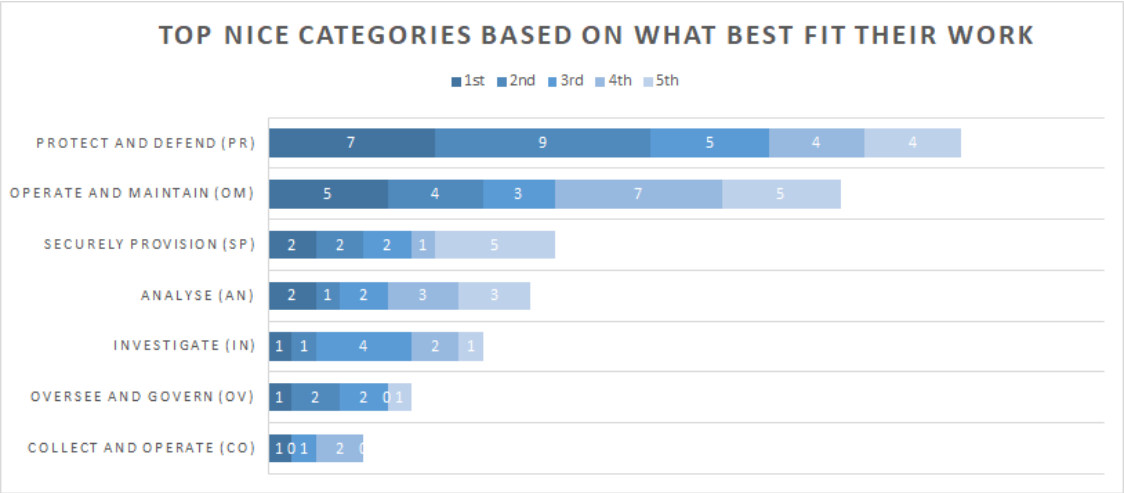

Figure 6: Top NICE categories based on what best fit their work

With this analysis of the data one can see that the bachelor's degree students are clearly employed in the "*Protect and Defend"* and "*Operate and Maintain"* categories with "*Securely Provision"* category closely behind them. "*Investigate"* and "*Analyse"* are categories that closely tie in with one another, thus they are quite similarly represented in the data. "*Oversee and Govern"* is quite administrative or managerial category with executive work roles; thus, the authors are not surprised that the bachelor's degree students do not work in that category immediately at the end of their studies. "*Collect and Operate"* category has described as intelligence gathering and offensive operations performed within the cyber domain, and as such it was the lowest category to receive answers.

To get a better view of the most frequent work roles we filtered 3rd to 5th selections from the data (still visible in figure 5) to get an understanding of what are the primary work roles of the respondents. This visualization can be seen in figure 7.

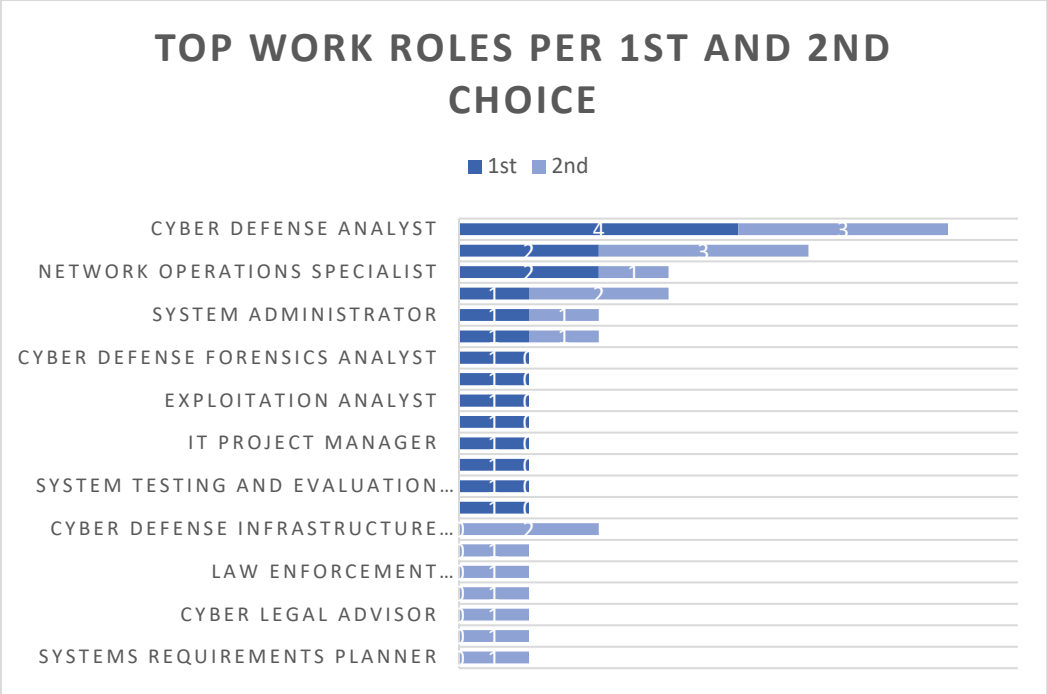

Figure 7: Top NICE categories based on what best fit their work

Almost all the data was either in "*Cyber Defense Analyst"* or "*Cyber Defense Incident Responder"* work roles with both belonging to "*Protect and Defend*" category. The authors would assume these two work roles of NICE Framework to be essential parts of the current establishment of Security Operations Centres (SOCs) within Finland (Carson, 2014), a growing private and public sector functionality within the field of Cyber Security (Jauhiainen, 2021). The newly graduated would most probably be workforce to create, upkeep or provide this service.

4.3 Cyber security specialisation in retrospective

At the end of the survey, the hindsight of the students is asked; "How would you choose your specialisation modules nowadays, with all the knowledge of your current work occupation and your hindsight of the studies". The student could choose two 30 ECTS modules but not the same module twice.

Noteworthy is that the module selection is available at the University of Applied Sciences they graduated from, but from a newly updated curriculum (JAMK University of Applied Sciences, 2021). The students were asked to familiarise themselves with the updated curriculum and then make their module selections. One central theme of the curriculum is to divide the modules into the *"DevSecOps"* ideology (Sánchez-Gordón & Colomo-Palacios, 2020) within ICT; the acronym standing for *"Dev"* being developers, *"Sec"* meaning (cyber) security and *"Ops"* as Operations. Results from the student answers are visualised in the Figure 8.

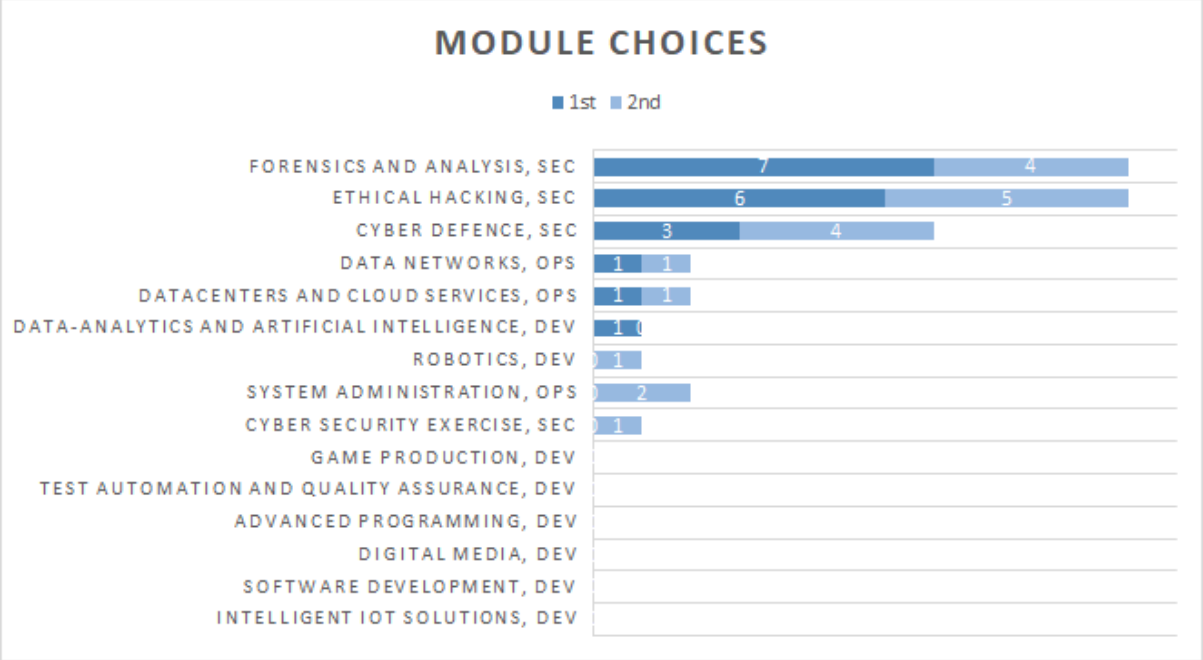

Figure 8: Specialisation modules of the bachelor's degree

An encouraging result from the survey data is that the module choices would still focus on Cyber Security. These top three modules are considered by the ICT degree programme coordinators to be a part of Cyber Security specialisation. The following two choices *"Data Networks"* and *"Datacentres and Cloud Services"* are more in the Operations section of the curriculum but noticeably related to some students' current work. This ties well with the results in Figure 6 as *"Operate and Maintain"* category was the second most descriptive category of their work.

One misstep of the authors was that we did not ask the alumni students about what modules they already had studied. Without this information it is impossible trace back Figure 8 data as being a new selection of the participants or did they just confirm that they would choose the same module they did once again, supposing they were freshly started students. Still, it would indicate the trend, that they wish to further emphasise their studies in Cyber Security. And as an education organisation it would give a confirmation to the university that these specialisation studies should be offered to the industry as a part of life-long learning.

5. Conclusion

Given the results and analysis, one can conclude that the cyber security students graduate and get employed to "*Protect and Defend"* the Critical Infrastructure through ISPs and work with the safety of "*Digital Services and Platforms"* in Finland. Our research data can be interpreted to prove that students are employed to be ensuring the functionality of the Finnish Cyber Domain as the Cyber Security Strategy of Finland stated. Through our research the education organizers (at JAMK) can now have a better understanding of the work placements of their former students in the field of Cyber Security. Adjustments of the curriculum can be based on researched data. By researching the education landscape (Saharinen et al, 2020), industry need (Jaurimaa et al, 2020) and student employment and satisfaction data the degree programme coordinators can verify their curricula to be up to date, have an ongoing discussion with the industry and provide current students of the degree programme information about their module choices. The timeline of the different, parallel cyber security frameworks gives a view of the evolving atmosphere around cyber security education. Different frameworks have varying amount of scientific research behind them, and this is typically stated in publication of the framework. The authors of this paper would like to conclude that all additions are of course an enrichment of the field, but for an education organisation; it would be preferrable to establish a basis of education on one of the frameworks (Saharinen et al, 2019) and proceed with the chosen framework consistently throughout the curriculum.

6. Discussion

The lifespan of a bachelor's degrees varies from three to four years in the Finnish education system (Ministery of Education and Culture - Finland, 2021). Given the degree completion length of the participating students in the research, there are six different cyber security frameworks published as visualized in Figure 1. The authors would assume that many of these Finnish cyber security degree programmes were started purely to respond to an industry need, however, also to meet this governmental resolution in Finland. Their formation might have come from an earlier information security orientation degree background, rather than a guiding cyber security framework or a governmental guidance, enforcing a clear degree structure and content. Thus, education organizations are trying to hit a moving target with their module and course structures within their curricula, that should be publicly available as mandated by the ECTS Users' Guide (European Comission, 2015). Finland has a national graduands feedback questionnaire system (Rectors' Conference of Finnish Universities of Applied Science, 2021) in place; however, the questionnaire is generalised to cover all education fields in the Universities of Applied Sciences. Although it gives useful data to the educating organisations, it rarely has relevant data on a certain degree field. The data is aggregated to Finland's Ministry of Education specific "Fields of Steering" and thus it does not even mention a specialisation of the degree, such as Cyber Security in ICT. Our research in this paper could and should be replicated to various universities to gain a better understanding of the graduands of cyber security.

Acknowledgements

This work has been done in Jyväskylä University of Applied Sciences (JAMK) which is participating in LIPPA - project – Quality to ICT Education from Industry and Education collaboration (project code S22466) funded by European Social Fund.

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

References

Associate for Computing Machinery. (2017) *Cybersecurity Curricula 2017 - Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity.* New York: Associate for Computing Machinery.

Associate for Computing Machinery, n.d. *Curricula Recommendations.* [online] https://www.acm.org/education/curricula-recommendations

Carson, Z. (2014) *Ten Strategies of a World-Class Cybersecurity Operations Center.* s.l.:The MITRE Corporation.

CC2020 Task Force, 2020. *Computing Curricula 2020: Paradigms for Global Computing Education.* s.l.:Association for Computing Machinery.

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

ENISA (2021) *CYBERHEAD - Cybersecurity Higher Education Database.* [online] https://www.enisa.europa.eu/topics/cybersecurity-education/education-map

European Comission, 2015. *ECTS Users' Guide.* [online] https://ec.europa.eu/assets/eac/education/ects/users-guide/docs/ects-users-guide_en.pdf

European Comission, (2020) *The EU's Cybersecurity Strategy for the Digital Decade.* [online] Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

JAMK University of Applied Sciences. (2013) *Cyber Security, Master of Engineering.* [online] https://www.jamk.fi/en/Education/Technology-and-Transport/Cyber-Security-Masters-Degree/

JAMK University of Applied Sciences. (2015) *Bachelor of Engineering, Information and Communications Technology.* [online] https://www.jamk.fi/en/Education/Technology-and-Transport/information-and-communication-technology-bachelor-of-engineering/

JAMK University of Applied Sciences. (2021) *Bachelor's Degree Programme in Information and Communications Technology.* [online] https://opetussuunnitelmat.peppi.jamk.fi/en/48/en/5290/TTV2021SS/year/2021

Jauhiainen, J. (2021) *List of SOC service providers.* [online] https://csoc.fi/

Jaurimaa, J., Saharinen, K. and Kotikoski, S. (2021) Critical Infrastructure Protection: Employer Expectations for Cyber Security Education in Finland, in *Proceedings of the 2021 20th European Conference on Cyber Warfare and Security*. *European Conference on Cyber Warfare and Security*, United Kingdoms: Academic Conferences International Limited. doi:10.34190/EWS.21.015.

Karinsalo, A. et al. (2021) [online] Available at: https://cybersec4europe.eu/wp-content/uploads/2021/06/D6_3_Design-of-Education-and-Professional-Frame-work_Final.pdf

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

Metropolia University of Applied Sciences (2021) *Cyber Security specialization studies.* [online] https://www.metropolia.fi/fi/opiskelu-metropoliassa/osaamisen-taydentaminen/erikoistumiskoulutukset/kyberturvallisuus

Ministery of Education and Culture - Finland (2021) *Finnish Education System.* [online] https://okm.fi/en/education-system

Nai Fovino, I. et al. (2019) *A Proposal for a European Cybersecurity Taxonomy.* [online] https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

Newhouse et al. (2017) *National.* s.l.:National Institute of Science and Technology.

Nurse, J. R. et al. (2021) [online] https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education/@@download/fullReport

Piesarskas, E. et al. (2020) [online] https://sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf

Rashid, A. et al. (2019) *The Cyber Security Body of Knowledge.* [online] https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf

Rashid, A. et al. (2021) *The Cyber Security Body of Knowledge.* [online] https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

Rectors' Conference of Finnish Universities of Applied Science, 2021. *University of Applied Sciences Graduand Feedback Questionnaire.* [online] https://avop.fi/en

Saharinen, K., Backlund, J. & Nevala, J. (2020) *Assessing Cyber Security Education through NICE Cybersecurity Workforce Framework.* New York, NY, USA, Association for Computing Machinery, p. 172–176.

Saharinen, K., Karjalainen, M. & Kokkonen, T. (2019) *A Design Model for a Degree Programme in Cyber Security.* New York, NY, USA, Association for Computing Machinery, p. 3–7.

Sánchez-Gordón, M. & Colomo-Palacios, R. (2020) *Security as Culture: A Systematic Literature Review of DevSecOps.* New York, NY, USA, Association for Computing Machinery, p. 266–269.

Shackelford, R. et al. (2005) In: *Computing Curricula 2015.* s.l.:The Association for Computing Machinery (ACM); The Association for Information Systems (AIS); The Computer Society (IEEE-CS).

South-Eastern Finland University of Applied Sciences (2021) *Bachelor of Engineering, cyber security.* [online] https://www.xamk.fi/koulutukset/insinoori-amk-kyberturvallisuus/

The Security Committee of Finland (2013) *Finland's Cyber security Strategy.* [online] https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

The Security Committee of Finland, 2019. *Finland's Cyber security Strategy 2019.* [online] https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

United Kingdom (2016) *National Cyber Security Strategy 2016-2021.* [online] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

University of Jyväskylä (2013) *Cyber Security, Master of Philosophy.* [online] https://www.jyu.fi/it/fi/opiskelu/maisteriohjelmat/kyberturvallisuus

Whyte, C. (2020) Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare, *Journal of Cybersecurity*, 6(1), p. tyaa013. doi:10.1093/cybsec/tyaa013.

Willoughby, T. et al. (2021) A Long-Term Study of What Best Predicts Graduating From University Versus Leaving Prior to Graduation, Journal of College Student Retention: Research, Theory & Practice. doi: 10.1177/1521025120987993.

Zan De, T. & Di Franco, F. (2019) *Cybersecurity Skills Development in the EU.* [online] https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/@@download/fullReport