Assessing Cyber Security Education through NICE Cybersecurity Workforce Framework

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Analyzing the results

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

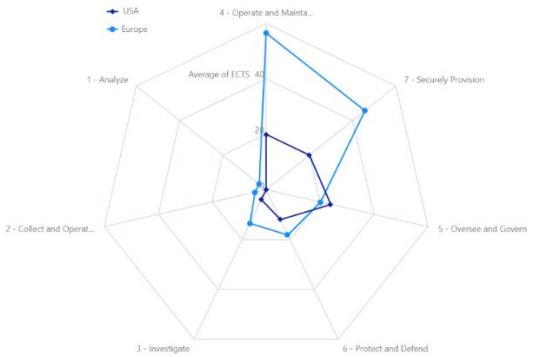
- Bachelor's Degree
  - 168 to 210 ECTS
  - 240 to 252 ECTS
- Master's Degree
  - 60 to 90 ECTS
  - 120 to 139 ECTS

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

3.1 Bachelor's Degree in Cyber Security

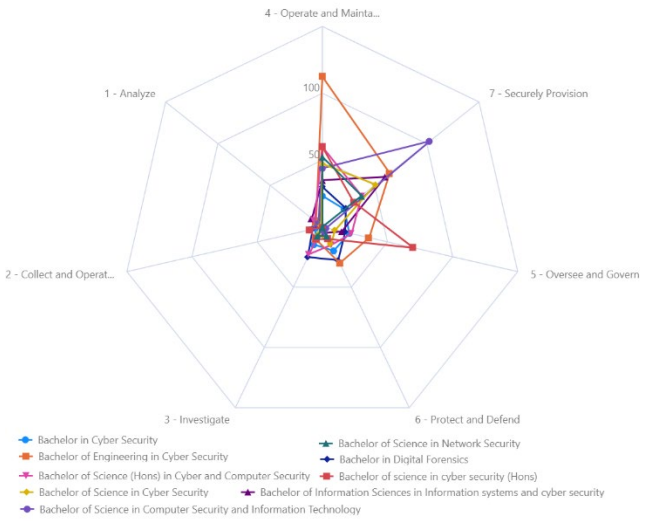
3.1.1 Bachelor's Degrees between 168 to 210 ECTS

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



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

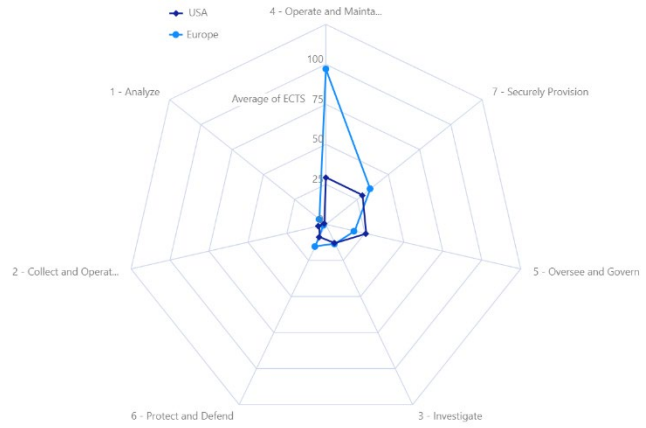
Figure 2 represents the same data when drawn of individual degree programmes of both geographic areas.



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

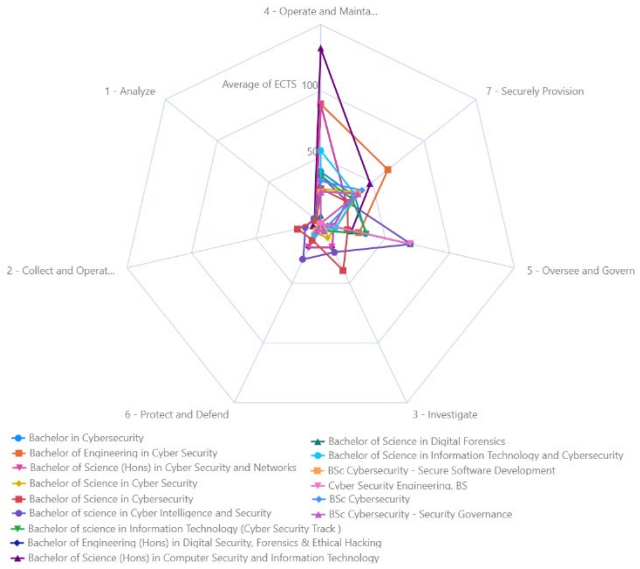
3.1.2 Bachelor's Degrees between 240 to 252 ECTS

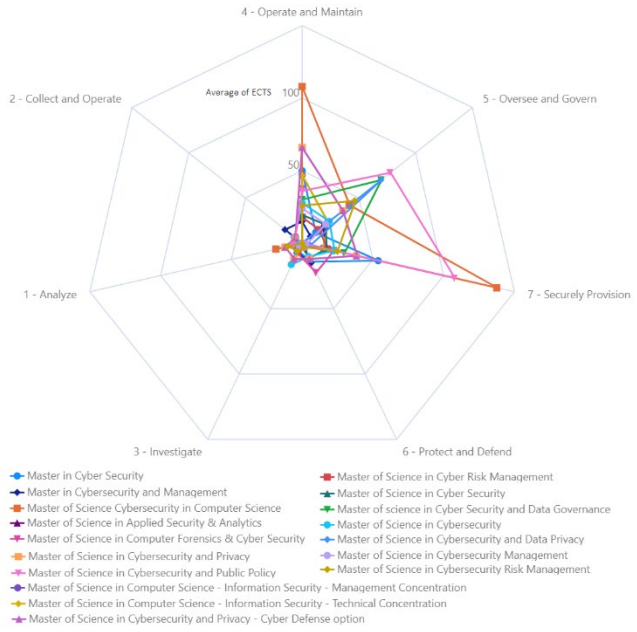
Figure 3 visualizes the average distribution by geographical area, but in bachelor's degree programmes between 240 to 252 ECTS.



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

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



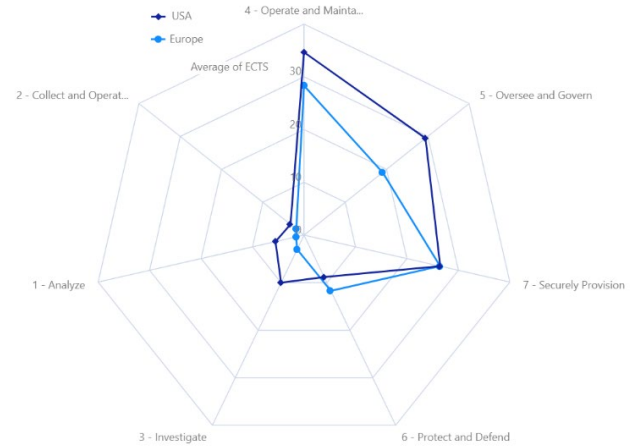


Few bachelor's degrees focus heavily on *Oversee and Govern*, but most are emphasizing *Operate and Maintain* with *Securely Provision*.

3.2 Master's Degree in Cyber Security

3.2.1 Master's Degree between 60 to 90 ECTS

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

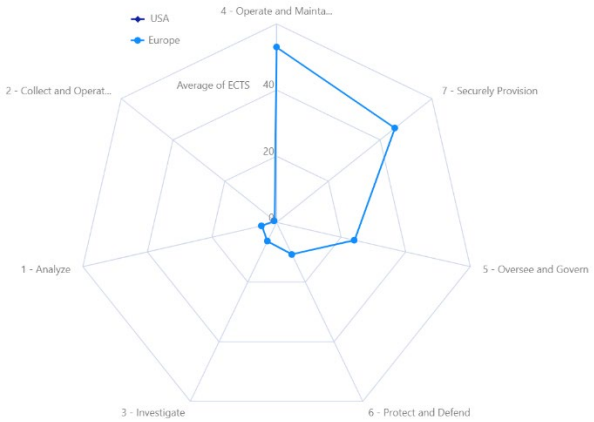


In this segment, *Operate and Maintain* is the highest, however *Oversee and Govern* is higher than *Securely Provision*. In this segment the degree programmes are often specializing to some area. Cyber Security Management and Regulation fall under *Oversee and Govern* category, thus it shows when at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

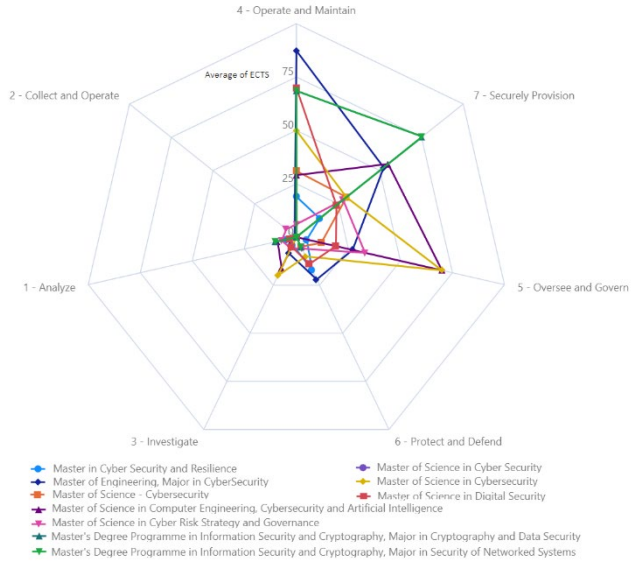
In the visualization above we come across the problem of large course offering of a degree programme. This gives room for selection; however, it causes certain averages to be above the degree length. It still emphasizes the NCWF category offering of the degree programme, while simultaenously it causes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

3.2.2 Master's Degree between 120 to 180 ECTS

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



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



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

4. CONCLUSIONS & FUTURE RESEARCH

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

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

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

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

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

5. ACKNOWLEDGMENTS

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

6. REFERENCES

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

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

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

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

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

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

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

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

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

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