Cybersecurity Education and Industry Demand: Insight from Norway

Diego Prestegård, Jon Harwiss, Mary Sánchez-Gordón and Selina Demi

Faculty of Computer Science, Engineering and Economics, Østfold University of Applied Sciences, Halden, Norway
{juan.d.prestegard, jon.p.harwiss, mary.sanchez-gordon, selina.demi}@hiof.no

Abstract. As the cybersecurity industry continues to grow, so does the demand for competent and skilled professionals. However, there is limited empirical evidence on the skills required by the Norwegian labor market and those included in the curricula of higher education institutions in Norway. This study aims to address this gap by examining the alignment between 77 job advertisements selected from a total of 253 postings collected from NAV and FINN, as well as curriculum data from six universities in Norway. Then, the collected data was manually categorized into the ACM Computing Classification System (ACM CCS) and the European Joint Commission Research Centre (JRC) taxonomies. The findings indicate that there is a partial gap between curricula and the cybersecurity labor market in Norway. Curricula tend to focus on theoretical aspects of cybersecurity, whereas there is demand for skills and competence within governance and applied technical security in the labor market.

Keywords: cybersecurity skills, cybersecurity curricula, cybersecurity labor market

1 Introduction

Digital infrastructure underpins economic activity, public services, and national security. As organizations grow more dependent on complex information systems, they are simultaneously exposed to a rapidly evolving cyber threat landscape. Moreover, continuous innovation leads to an increase in demand for skilled cybersecurity professionals capable of protecting assets against sophisticated threat actors. Consequently, there is a growing need to align cybersecurity education with the expectations and the needs of the labor market [1].

The relevance of this concern is further emphasized by the Nordic Financial CERT (NFCERT), reporting that the cyber threat level facing the Nordic financial sector remains high with organized crime groups, nation-state actors, malicious insiders, and supply chain attacks posing the most significant threats [2]. In contrast, hacktivism and artificial intelligence are currently assessed as having medium importance, with no major changes in their impact on the overall threat landscape. Moreover, the Norwegian

Police Security Service (PST) highlights how increased geopolitical tension and uncertainty drive foreign intelligence services to engage in activities such as recruitment, influence operations, sabotage, and economically motivated security threats [3]. These two reports illustrate a persistent and complex threat environment that demands continuously updated and relevant cybersecurity competence.

The National Cyber Security Strategy (NCSS) for Norway in 2019 identified as a key objective ensuring that "improved cybersecurity competence is aligned with the needs of society" [4]. However, NCSS also acknowledges that addressing all challenges and risks present in the cybersecurity space in Norway is a difficult task. The digital infrastructure and threat landscape carries on with rapid evolution, increasing the necessary competence required from professionals. In 2025, the strategy prioritizes total preparedness and acknowledges that "access to cyber security expertise is a prerequisite for developing cyber resilience" and "investigate establishing a national cyber security reserve with the private sector" [5].

The fast-paced development seems to be a consistent concern across literature. For instance, Goupil et al. [6] describe skill gaps as "highly dynamic", suggesting that even with a significant investment in cybersecurity skills, the landscape of information technology changes too fast for skills to fully mature. Although there are several studies that have examined employers' expectations within the cybersecurity job market, these studies have not focused on the Norwegian job market. Therefore, there are limited empirical insights into the cybersecurity skills included in the cybersecurity education in Norway and the current demands of the Norwegian labor market.

To address this gap, this exploratory study aims to identify cybersecurity skills demanded by the Norwegian cybersecurity labor market and skills included in the cybersecurity curriculum of Norwegian universities. Therefore, the following two research questions (RQ) are formulated:

RQ1: What cybersecurity skills are demanded by the Norwegian labor market?

RQ2: Is there a gap between skills required by Norwegian labor market and those included in the cybersecurity curricula?

To answer these RQs, this study collected and analyzed job ads data from two job portals and curriculum data from six Norwegian universities. The data was classified using two cybersecurity taxonomies and then potential gaps were identified.

The remaining sections were structured as follows: Section 2 presents related research in the topic. Section 3 provides an overview of our research approach. Section 4 reports the results while Section 5 discusses them. Finally, conclusions are presented in Section 6. To ensure transparency, supplementary material is provided and accessible online [7].

2 Related Works

Previous literature has explored the cybersecurity job market and cybersecurity curricula. For instance, a study conducted by Graham & Lu [8] conducted semantic network analysis of 17,929 cybersecurity job advertisements to identify critical soft skills required by cybersecurity employers. The results revealed three main categories

of required soft skills in cybersecurity: knowledge management and systems, big data analytical skills, and teamwork. Recently, Ullah et al. [9] conducted a study to understand the skills needed for cybersecurity professionals. The data was collected from 12,161 job ads and 49,002 Stack Overflow posts, The analysis of the data suggested that communication skills and project management skills are the most important soft skills, while the demand for technical skills varies across different cyber roles, with Java being the most used programming language. Moreover, Erickson and Kim [10] reviewed several industry security certifications and governing bodies to compare the domains and use that information to provide recommendations for building better cybersecurity curricula. According to the authors, well-recognized security certifications and relevant subject domains should be incorporated within cybersecurity programs, given that those align with minimum requirements for entry-level cybersecurity job postings.

Previous literature has also raised concerns related to the teaching methods applied in educational programs through which cybersecurity skills are attained. Aaltola et al. [11] found that many programs rely on traditional, theory heavy approaches, offering limited opportunities for practical application. This can hinder students' ability to gain a good understanding of key concepts and skills, making the transition from graduate to workforce challenging. Innovative technologies, such as generative AI can be leveraged to improve both cybersecurity curricula and teaching methods. As recommended in [12], the incorporation of generative AI related use cases aligned with learning outcomes into cybersecurity curricula could bridge the gap between theoretical cybersecurity knowledge and practical skills needed to face real-world cybersecurity challenges.

3 Methods

Based on the main research objective, this study conducted a thematic analysis to examine data from job advertisements and curricula. The data was categorized using established cybersecurity taxonomies.

3.1 Data Collection

The following two processes were adopted to collect relevant data for this study.

Job Advertisements. Data was manually gathered from FINN AS (https://www.finn.no) and NAV (https://arbeidsplassen.nav.no) by using the search terms *"cybersecurity"* and *"cybersikkerhet"*. The selected keyword was a result of an iterative process where the keywords were chosen and refined based on the relevance and amount of hits. For each website, we then refined to show results not by relevance, but by date. Although, the original intention was to gather job advertisement data through automated-scraping, due to restrictions, automated data collection from these jobs portals was not feasible. Therefore, a manual process was defined to gather job

advertisements into Excel. The job advertisements included in this study were chosen based on the following criteria:

- The term *"Cybersecurity"* or *"Cybersikkerhet"* is mentioned in the job title or in the job qualifications.
- Cybersecurity relevant skills and responsibilities are described as part of the job description.
- The job advertisement must be within the Norwegian labor market.

The collection of job advertisement data was conducted in April 2026, with a total of 253 records. The search term got 222 hits on FINN, and 31 hits on NAV. Each job advertisement was then analyzed to determine whether they fit our inclusion criteria, resulting in 77 relevant advertisements (see the complete list in [7]). These were recorded in an Excel sheet, along with a unique identifier (ID: 1-77), and information about the job title, organization, qualifications, responsibilities, and where available, desired personal qualities.

In order to assess the validity of the gathered data, a random sample of 16 job advertisements (around 20% of the dataset of 77) was checked for accuracy. All sampled entries matched the original ads.

Higher Education Curricula. The university curricula data focused on public universities part of the 2025 Norwegian University Ranking (https://www.unirank.org). Given the manual nature of the data extraction process, the study was limited to the six top ranked higher education institutions: Universitetet i Oslo (UiO), Norges teknisk-naturvitenskapelige Universitet (NTNU), Universitetet i Bergen (UiB), UiT Norges arktiske universitet (UiT), Oslo Met, and Høgskolen i Østfold (HiØ).

Each institutional website was reviewed to identify the courses relevant to the computer science area, specifically the ones related to cybersecurity. The relevance was determined based on the course description along with expected learning outcomes. These were selected as they were common informational traits with the same structure and format among all the individual courses and different universities. As a result, 96 courses were identified: UiO (25), NTNU (20), UiB (12), UiT (22), OsloMet (10), and HiØ (7).

3.2 Data Extraction and Analysis

The data extraction and analysis process was conducted based on two established taxonomies, as explained in the following section.

Skill Categories (ACM CCS and JRC). The findings were systematically categorized using two established taxonomies. One of the taxonomies was developed by the Association for Computing Machinery (ACM), i.e., the ACM Computing Classification System (ACM CCS), and the other by the European Commission Joint Research Centre (JRC). These taxonomies were selected because they are well-recognized and provide a clear set of areas to use for grouping different learning outcomes from higher education and skills needed in professional jobs, giving them clear classifications [6].

ACM CCS consists of several broader computing classifications that follow a hierarchical structure spanning several levels in-depth, each with their own additional categories/nodes. In this study, one of the initial categories catered towards cybersecurity, “Security and privacy”, was used for our predefined scheme. JRC taxonomy follows a similar structure, where only the first level was used and all categories are catered towards cybersecurity.

It is worth noting that the relationship between the ACM CCS (10) / JRC taxonomies (53), and the job advertisements and university curriculums is not always one-to-one. In practice, each job advertisement and curriculum could be categorized into more than one category depending on the context (see the complete list of ACM CCS and JRC in [7]).

Extraction of Skill Categories. Both ACM CCS and JRC were used as defined codes and were assigned to the data using each sentence as the unit of analysis. To ensure consistency throughout the classification process, each category in both taxonomies must be clearly defined. These definitions were based both on ACM CCS and JRC official sources but were also supplemented with third-party definitions where needed.

The collected data was then manually categorized according to these definitions. To ensure consistency and reliability, each categorization of job and curriculum data was cross-checked by each of the authors.

Each course description and job advertisement were manually assigned to the relevant ACM CCS L2 nodes and JRC L1 nodes. The categorization of the JRC skill categories was limited to L1, as it was descriptive enough for the purpose of this study. Deeper nodes were taken into consideration to more accurately match the extracted skills and learning outcomes of the specific course.

Other Categories. The job advertisements gathered were also categorized by the applicants’ desired qualifications, such as experience with certain standards and frameworks, desired certifications and education.

4 Results

In total, 77 job advertisements fit the inclusion criteria, and were included in this study. Furthermore, 96 unique courses from the universities were found to be cybersecurity relevant. The coded data were analyzed to identify trends and patterns context (see details in [7]).

4.1 Labor Market Requirements (RQ1)

The results provide an overview of the desired skills in the Norwegian cybersecurity labor market based on jobs ads collected from NAV (21 %) and FINN (79%).

Desired Skill Categories in the Labor Market. The results of the ACM CCS classification is shown in Figure 1. Regarding ACM CCS skill categories, the results

showed that *Systems security* (72) was the most represented skill category. The second most represented category was *Formal methods and theory of security* (56), followed by *Human and societal aspects of security and privacy* (42), *Security services* (40), *Intrusion/anomaly detection and malware mitigation* (37), *Network security* (28), and *Software and application security* (25). Finally, *Database and storage security* and *Cryptography* were represented with 2 instances each.

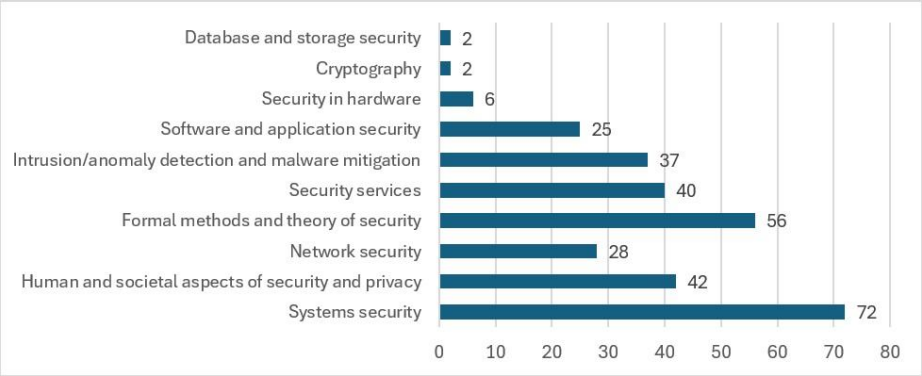

Fig. 1. Job Advertisement ACM CCS

By categorizing desired skills according to JRC taxonomy, Figure 2 depicts that *Security Management and Governance* (53) is the most represented category in the cybersecurity labor market. *Network and Distributed Systems* (34), and *Software and Hardware Security Engineering* (27) are the second and third most represented categories. *Data Security and Privacy* (19), *Incident Handling and Digital Forensics* (19), and *Assurance, Audit and Certification* (18) are similarly represented. *Cloud, Edge and Virtualisation* (15), *Education and Training* (14), *Security Measurements* (11), and *Information systems* (10) are also similarly represented. The remaining categories were limited in their representation, but they all varied from between 1 to 5 instances.

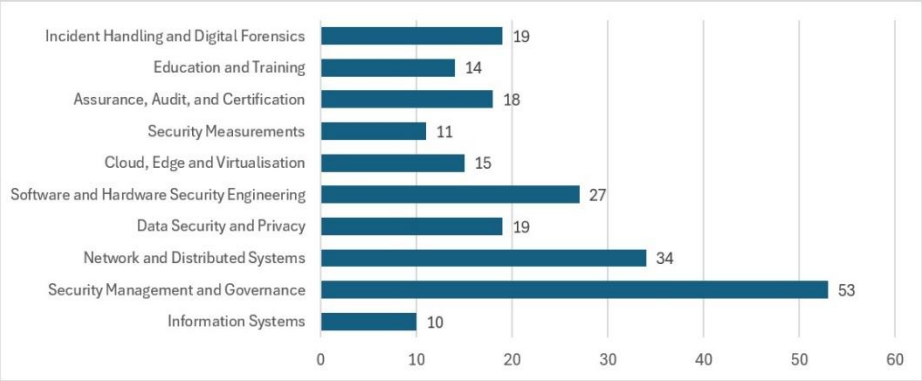

Fig. 2. Job Advertisement JRC

Standards and Frameworks in the labor market. Most job ads (48; 62%) did not specify experience with any standard or framework. Figure 3 shows that among those that did, there was a clear preference towards experience with ISO (*International Organization for Standardization)* standards (21). Of these, 14 advertisements specifically requested experience with or knowledge of *ISO/IEC 27001,* while *ISA/IEC 62443* was mentioned four times. Other advertisements referred to regulatory frameworks and legislation, including the *Sikkerhetsloven (Security Act)* (12), *General Data Protection Regulation (GDPR)* (8) and *NIS 2* (1).

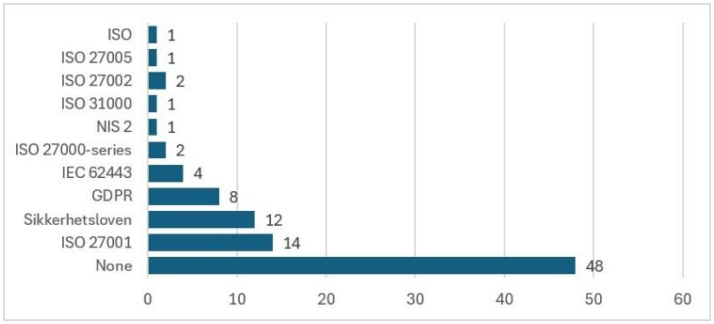

Fig. 3. Job Advertisement Standards, Regulatory frameworks and Legislation

Jobs requiring experience and/or knowledge of approaches are shown in Figure 4. Among these jobs, the *NSM Grunnprinsipper (NSM ICT Security Principles)* (9) was the most requested approach. Other approaches included the *Information Technology Infrastructure Library (ITIL)* (6), *Zero Trust frameworks* (4) and *NIST* (4).

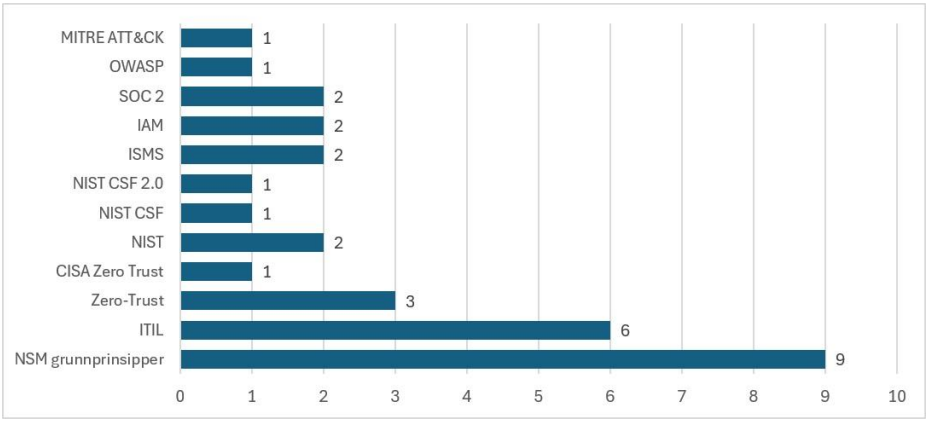

Fig. 4. Job Advertisement Frameworks

Education and experience requirements in the labor market. The results presented in Figure 5 indicated that both *Master* (32) and *Bachelor* (26) degrees are the most represented categories. Around a quarter of the job advertisements only specify *Higher*

Education (20) without indicating the education level required. In addition, 15 job ads do not mention any requirements. *Degree certificate* (4) and *PhD* (3) are required in a few instances. Note that education counts exceed the total number of job ads, due to multiple categories being related to a single advertisement, e.g., bachelor and master.

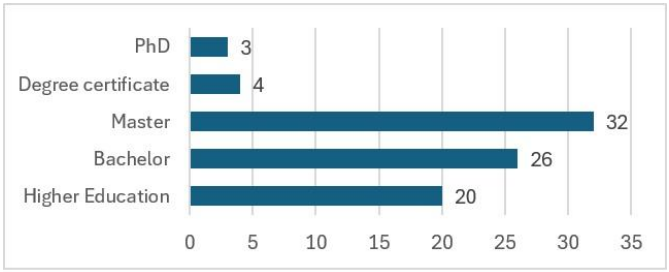

Fig. 5. Level of Education

The results in Figure 6 show that with regards to job levels, the position most in demand is *Junior* (39), followed by *Senior* (26), with *Mid-level* (10) positions being less frequent. Additionally, there were two specific positions related to research at the PhD level.

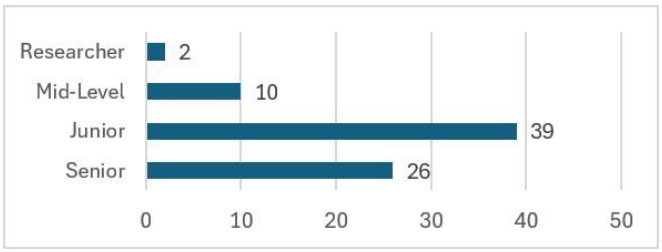

Fig. 6. Junior, Mid-level, Senior Counts

4.2 Curriculum and Job Advertisement Comparisons (RQ2)

This section takes previous job advertisement results and compares them with the university curriculum data.

Skill Categories. The results in Figure 7 show similarities and differences between job and curriculum data. The categories *Systems security* and *Formal methods and theory of security* were the most represented in both datasets. Further similar patterns were observed in *Human and societal aspects of security and privacy*, *Security services*, *Software and application security*, *Intrusion/anomaly detection and malware mitigation* and *Network security*. These categories were represented at similar levels in both the job and curriculum data, with only minor differences.

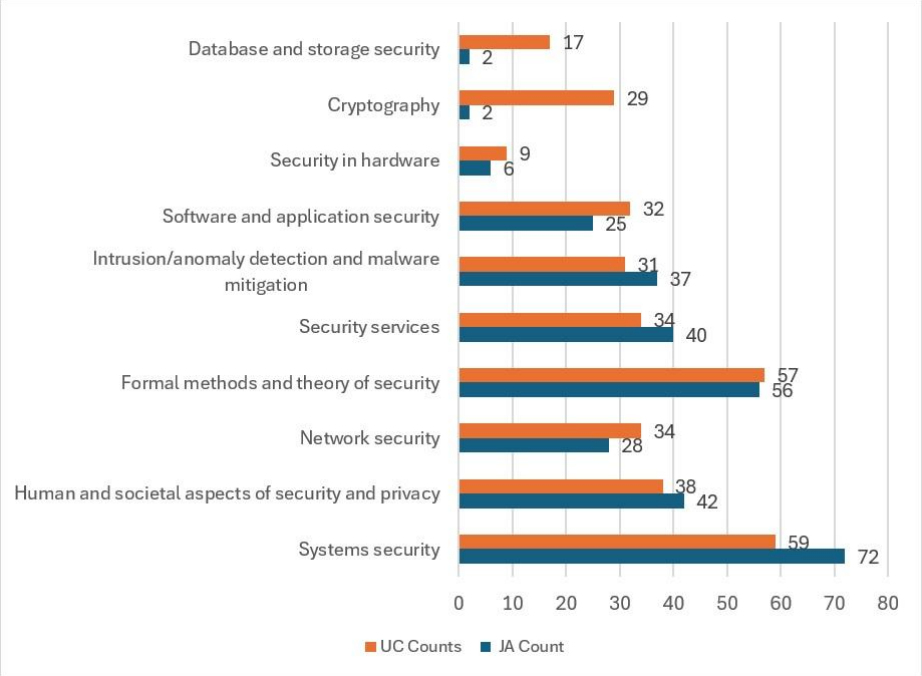

Fig. 7. Curriculum (UC) & Job Advertisement (JA) ACM CCS Comparison

The results also revealed differences between the job and curriculum data. *Cryptography* (29) and *Database and storage security (17)* were identified more often in the curriculum data compared to 2 instances in the job data. Another difference was found in the *Security in hardware* category, with 6 instances in the job data, and 9 in the curriculum data.

The results in Figure 8 show a continued overlap between JRC categories for both job advertisements and curriculum data. These include *Incident and Management Handling*, *Security Measurements*, *Network and Distributed Systems*, and *Security Management and Governance*. Meanwhile categories such as *Education and training*, *Assurance, Audit, and Certification*, *Cloud, Edge and Virtualisation, Information systems* are more visible in job advertisement data. Meanwhile categories such as *Theoretical Foundations*, *Legal Aspects*, *Cryptology*, *Software and Hardware Security Engineering*, and *Data Security and Privacy* are more represented by university curricula data rather than job advertisements.

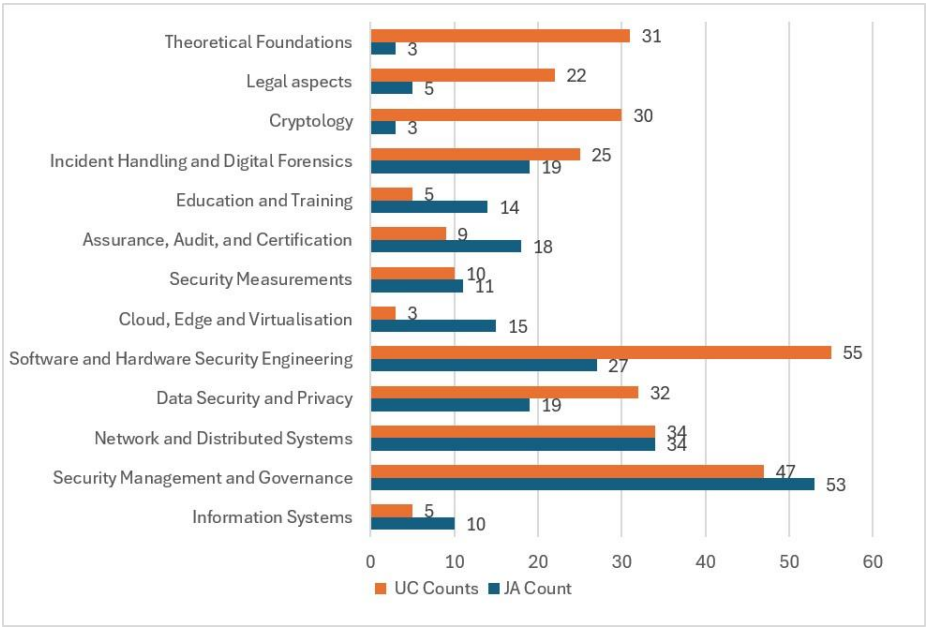

Fig. 8. Curriculum (UC) & Job Advertisement (JA) JRC Comparison

Curriculum Standards and Frameworks. The results for standards and frameworks in the curriculum showed a negligible representation. Large portions of the curriculum generally mention the concept of frameworks and standards in the course description, but not specifically by name. However, among the universities only HiØ and NTNU mention a cybersecurity standard or framework by its specific name.

5 Discussion

The results for the ACM CCS categories indicated that employers in the Norwegian cybersecurity labor market value skills and competencies within the frameworks of the *Systems security* and *Formal methods and theory of security* categories, as these were by far the most represented categories in the job advertisements. These findings align with how cybersecurity professionals go from IT-centric roles into management-focused roles [13, 14]. Other categories, such as *Human and societal aspects of security and privacy*, *Security services*, and *Intrusion/anomaly detection and malware mitigation* are also quite desired in the labor market. These competencies are therefore very much desired in the labor market and could indicate that employers value a combination of technical, organizational and operational skills.

In contrast, other categories such as *Cryptography* and *Database and storage security* had a few instances of representation in the data. Although these categories are relevant to cybersecurity, they appear to be of less interest to employers. However, it is important to note that skills and experience in these categories could still be relevant to

specialized roles. With a larger sample size of job advertisements, we could see a significant increase of underrepresented categories.

The results for the JRC categories show that employers value skills and experience in categories such as *Security Management and Governance, Network and Distributed Systems,* and *Software and Hardware Security Engineering*, as these are the three most represented categories in the job data. The results may indicate that employers value both technical skills, such as security engineering and network configuration, as well as skills in management and governance. The results may also indicate that skills within management and governance, networks and security engineering could make employees more attractive in the labor market.

Other categories had a relatively low representation in comparison, with many categories receiving between 1 and 10 representations in the job data. This indicates that there is a vast variety of specializations in the labor market, and that skills within these categories could still be valuable to employees. This may also be a consequence of the small sample size of job advertisements, as categories could receive more representation with a larger sample size.

Furthermore, the results revealed that few jobs required any specific knowledge or experience with any standard or framework. Among the few job ads that did, *ISO/IEC 27001* was the most represented standard. Other standards and frameworks included *NSM grunnprinsipper*, *GDPR*, *ITIL*, *NIST* and *Zero Trust*. The low amount of representation of jobs requiring experience with standards and frameworks may suggest that employers may expect this implicitly rather than stating it directly in the job ads. It may also suggest that employers do not value experience with standard and frameworks above practical and technical skills.

Previous research argue that certifications should be more systematically integrated into academic programs, however empirical evidence remains scarce [10]. Our results support that education is important for employers, although several job advertisements indicate that adequate experience may compensate for a lack of education. Bachelor's and master's degrees are in high demand, which suggests that employers are looking for employees with an academic background.

There is also a high demand for juniors in the labor market, as they are the most represented group in the job ads, followed by seniors and mid-level positions. This suggests that there is an increasing demand for newly educated employees. The strong representation of seniors could also suggest that employers are interested in experienced employees to handle complex responsibilities. However, it is worth noting that this could also be a consequence of the small sample size, and that in reality, more positions may look for a mid-level or a senior employee.

Results indicated a partial gap between higher education curriculum and the desired skills in the Norwegian cybersecurity labor market, but this gap is not uniform across categories. A level of alignment can be observed between various categories, such as *Systems security*, *Formal methods and theory of security*, *Security Management and Governance*, and *Network and Distributed Systems*.

However, some differences were observed. For instance, categories such as *Cryptography*, *Database and storage security*, *Cryptology*, and *Theoretical Foundations* are more represented in curriculum data. This may suggest that curricula

places a higher emphasis on traditional and theoretical cybersecurity topics than what is requested in sampled job advertisements. This may contribute to a shortage in applied and practical skills in newly graduated students as the curriculum has placed too much emphasis on the theory rather than the practical.

Another observation can be made in categories such as *Assurance, Audit and Certification* and *Education and Training,* being more visible in job advertisement data over curriculum data. This may create challenges for students transitioning into cybersecurity professional roles, as the curriculum may have placed too much emphasis on theoretical principles. This focus on theory may also be necessary, as students with no background in cybersecurity would benefit greatly from theoretical foundations.

Ultimately, there appears to be a partial gap between curriculum content and labor market demand. The gaps are observed in specific categories, rather than the whole cybersecurity education. Curriculum data appears to be somewhat more focused on theoretical and traditional security topics, while job advertisements place more emphasis on governance, operational, and applied security competencies. This could have implications for students, universities and the labor market as a misalignment between the curricula and the labor market could lead to a skill gap in the cybersecurity workforce. It may also lead to a decline in enrolment at certain universities as students may prefer to study at universities with curricula that are closely aligned with the demands of the labor market.

Findings in this study show both similarities and differences compared to Goupil et al. [6]. Similar to their study, results suggest that some categories for both ACM CCS and JRC are more strongly represented across curricula than in job advertisements as this paper's findings. This is more visible with *Cryptography*, which appears more strongly represented in curricula. However, in contrast with Goupil et al. [6], the present study finds a less pronounced gap for industry-oriented categories. This may be explained due to the sample size, as well as a focus in the Norwegian sector in this study.

Limitations and Threats to Validity. The main threat to this study is the small sample size of data regarding job advertisements. Initially, the data gathering and category extraction were planned to be an automated process, enabled by webscrapers and other analysis tools. However, due to restrictions in the data gathering process, we had to gather and analyze data manually. This meant that the process of gathering data and extracting information took longer than initially planned and led to a limited amount of job advertisement data, due to time restrictions. It is also noteworthy that only two search terms were used to collect job advertisements. Excluding similar terms, such as *IT-sikkerhet* or *informasjonssikkerhet* might have led to the exclusion of relevant job positions. Therefore, although the small sample size provides a good overview of the topic, representation is limited.

To ensure validity of the gathered job ads, samples were selected at random and verified with the original source. This does not prove that the full dataset is entirely error-free but provides support for reliability in the manual extraction process. A potential challenge that can hinder the process relates to those job advertisements that no longer appear active on FINN and may be deleted.

Manual processing and categorization of data can lead to human error, so measurements to combat this were therefore taken. These include taking advantage of our background in cybersecurity, verifying that each category of data is correct by re-examining it, and comparing them to the developed defined codes for ACM CCS and JRC with examples on how it should be categorized. It should be noted that our interpretations of ACM CCS and JRC might differ from other researchers.

The universities used to gather curricula data presented course descriptions in different ways. This could lead to variations in the process of how we refined and presented the data. For example, most universities described concepts such as frameworks and standards in courses but did not specify which of them would be used in a given course. From our selected universities, only HiØ and NTNU had specified the standards and frameworks used in their curriculum. This was also the case for a number of job descriptions. There might also be courses that include standards and frameworks without naming them in their public descriptions. Ultimately, the results could also benefit from including more universities.

6 Conclusion

This study explored the specific skills desired in the Norwegian cybersecurity labor market, and the alignment between the labor market demands and the cybersecurity curricula taught to students in Norway's top six universities. By gathering and analyzing job advertisements and cybersecurity relevant courses, we were able to categorize them into the ACM CCS and JRC cybersecurity taxonomies, identify desirable skills in the labor market and explore the alignment between today's cybersecurity labor market and university curricula. The findings indicate that the labor market values the combination of technical, organizational and operational skills and competencies, as categories such as *Security Management and Governance, Systems Security* and *Network and Distributed Systems* are highly represented in the job advertisement data. There also seems to be a demand for skills and competency within the ACM CCS category *Formal Methods and Theory of Security* as it is also highly represented.

The findings also indicate that there is a potential gap between what is being taught in cybersecurity courses and the expectations in the labor market. Although several categories in both the ACM CCS and JRC taxonomies show significant alignment, there are still significant differences. As seen in the JRC results, curricula data put a stronger emphasis on theoretical aspects, which may lead to challenges related to students' transition into cybersecurity professional roles. This focus may however be necessary, as students may have limited foundational knowledge about cybersecurity. Results in the ACM CCS data also showed that many job advertisements valued theoretical knowledge.

Overall, the study suggests that there is a gap and need for alignment between what is being taught in universities and skills required in the labor market. Future research would benefit from larger datasets and automated work processes to increase the sample

size and eliminate human error and bias, in order to gain a more comprehensive overview of the desired skills.

Acknowledgments. The authors thank Tim Didrik Asbjørnsen Sandmark and Robin Kristiansen Enerhaugen for their contributions to conducting this study.

References

1. Sechi, F., Chockalingam, S.: A Framework for Multi-University Cybersecurity Curriculum Gap Analysis. Norsk IKT-konferanse for forskning og utdanning. 37, (2025). https://doi.org/10.5324/ksmqtr77.
2. Nordic Financial CERT: The Nordic Cyber Threat Landscape (CTL) 2026 report, https://www.nfcert.org/nfcert-2026-ctl-the-expanding-web-of-cyber-threats-supply-chains-insiders-and-the-state-crime-nexus-in-2026/, (2026).
3. Norwegian Police Security Service (PST): National Threat Assessment 2026. (2026).
4. Norwegian Ministeries: National Cyber Security Strategy for Norway. , Norway (2019).
5. Norwegian Ministry of Justice and Public Security: Total preparedness. (2025).
6. Goupil, F., Laskov, P., Pekaric, I., Felderer, M., Dürr, A., Thiesse, F.: Towards Understanding the Skill Gap in Cybersecurity. In: Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education Vol. 1. pp. 477–483. Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3502718.3524807.
7. Diego Prestegård, Jon Harwiss, Mary Sánchez-Gordón, Selina Demi: Online appendix: Understanding Industry Expectations for Cybersecurity Professionals in Norway, (2026). https://doi.org/10.6084/m9.figshare.33098708.
8. Graham, C.M., Lu, Y.: Skills Expectations in Cybersecurity: Semantic Network Analysis of Job Advertisements. Journal of Computer Information Systems. 63, 937–949 (2023). https://doi.org/10.1080/08874417.2022.2115954.
9. Ullah, F., Ye, X., Fatima, U., Akhtar, Z., Wu, Y., Ahmad, H.: What Skills Do Cyber Security Professionals Need? (2025). https://doi.org/10.48550/arXiv.2502.13658.
10. Mathew Erickson, Philip Kim: Designing cybersecurity curriculum: Exploring the need for industry certifications and experiential learning. IIS. 22, 9–20 (2021). https://doi.org/10.48009/4_iis_2021_9-21.
11. Aaltola, K., Ruoslahti, H., Heinonen, J.: Desired cybersecurity skills and skills acquisition methods in the organizations. eccws. 21, 1–9 (2022). https://doi.org/10.34190/eccws.21.1.293.
12. Demi, S., Guttormsen, B., Reinaas, K.F., Hansen, M., Sand, S.: Advancing Cybersecurity Education in the Era of Generative AI. Norsk IKT-konferanse for forskning og utdanning. 37, (2025). https://doi.org/10.5324/42gawg86.
13. Ramezan, C.A.: Understanding the chief information security officer: Qualifications and responsibilities for cybersecurity leadership. Computers & Security. 152, 104363 (2025). https://doi.org/10.1016/j.cose.2025.104363.
14. Blažič, B.J.: Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? Educ Inf Technol. 27, 3011–3036 (2022). https://doi.org/10.1007/s10639-021-10704-y.