



## OPEN ACCESS

### EDITED BY

Marta Moskal,  
University of Glasgow, United Kingdom

### REVIEWED BY

Hassan Abood,  
Republic of Iraq Ministry of Oil, Iraq  
Gede Saindra Santyadi Putra,  
Ganesha University of Education,  
Indonesia

### \*CORRESPONDENCE

Abdolrasoul Habibipour  
✉ [abdolrasoul.habibipour@ltu.se](mailto:abdolrasoul.habibipour@ltu.se)

RECEIVED 16 December 2025

REVISED 03 February 2026

ACCEPTED 06 February 2026

PUBLISHED 18 February 2026

### CITATION

Behzadi B and Habibipour A (2026)  
Aligning cybersecurity higher education  
with European skills frameworks:  
insights from master's programs in  
Sweden.

*Front. Educ.* 11:1769241.

doi: 10.3389/feduc.2026.1769241

### COPYRIGHT

© 2026 Behzadi and Habibipour. This is an open-access article distributed under the terms of the [Creative Commons Attribution License \(CC BY\)](https://creativecommons.org/licenses/by/4.0/). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

# Aligning cybersecurity higher education with European skills frameworks: insights from master's programs in Sweden

Bahareh Behzadi<sup>1</sup> and Abdolrasoul Habibipour<sup>2\*</sup>

<sup>1</sup>Hogskolan i Skövde, Skövde, Sweden, <sup>2</sup>Luleå University of Technology, Luleå, Sweden

**Introduction:** Cybersecurity education is expanding rapidly, yet universities face challenges in aligning curricula with evolving labour market needs and emerging domains such as artificial intelligence security and cloud security. This study examines how Swedish master's programmes align with the European Cybersecurity Skills Framework and how European skills frameworks are translated into curriculum practice.

**Methods:** A mixed-methods design combined document analysis of 91 compulsory courses across 12 master's programmes at 11 Swedish universities (Autumn 2024 intake) with semi-structured interviews with seven programme coordinators. Courses were mapped to European Cybersecurity Skills Framework role profiles using course titles, learning outcomes and the European Cybersecurity Education and Professional Training Minimum Reference Curriculum, and findings were interpreted through the European Cybersecurity Skills Framework based Cybersecurity Curriculum Alignment framework.

**Results:** Across the national set of programmes, all European Cybersecurity Skills Framework roles are covered, but depth and specialization vary substantially between programmes. Technical roles are strongly represented in some programmes, whereas others emphasise governance, risk and compliance roles. Emerging areas such as artificial intelligence security, machine learning security and cloud security are only marginally addressed in compulsory curricula, and programme coordinators report constraints related to staffing, time and slow institutional change processes.

**Discussion:** The findings suggest that national alignment to a European skills framework cannot be assessed only by counting covered roles, but must also consider programme design logics, curriculum content depth and institutional conditions for change. Stronger use of the European Cybersecurity Skills Framework in curriculum planning, clearer role oriented learning outcomes, increased industry collaboration and more structured practice based elements could improve graduates' readiness for cybersecurity careers.

### KEYWORDS

curriculum mapping, cybersecurity education, European Cybersecurity Skills Framework, higher education, skills frameworks

## Introduction

In today's digital landscape, information technologies (IT) have become a strategic asset, enabling organizations to adapt to situational changes and maintain competitiveness (Chakravarty et al., 2013). Consequently, information is increasingly regarded not merely as data but as a critical organizational asset requiring robust protection. Cybersecurity practices aim to safeguard information systems from unauthorized access, data breaches, and cyber

threats, preserving the confidentiality, integrity, and availability of sensitive information while maintaining competitive advantage.

The evolving threat landscape presents significant challenges. High-profile breaches, such as Yahoo!'s 3-billion-account compromise (Daswani and Elbayadi, 2021) and the Swedish Transport Agency incident in 2017 (Newlove-Eriksson et al., 2018), illustrate the severe consequences of inadequate protection. Organizations invest substantial resources in IT systems and cybersecurity measures to mitigate these risks (Parenty and Domet, 2020).

The growing complexity of technology ecosystems—including BYOD practices, IoT integration, and the proliferation of connected devices—expands potential vulnerabilities, demanding proactive management of cybersecurity risks (Joiner and Tutty, 2018). To address these challenges, specialized cybersecurity roles are essential, ensuring effective oversight, risk communication, and program execution (Auffret et al., 2017).

Education and training are fundamental to developing a skilled cybersecurity workforce. High-quality programs equip professionals with the knowledge and competencies required to navigate complex digital environments. Aligning curricula with evolving industry needs is critical to ensure that cybersecurity initiatives remain effective and graduates are prepared to meet the dynamic challenges of the field (Conklin et al., 2014; Triplett, 2022).

## Problem definition

Educational institutions face a critical challenge in preparing students for the cybersecurity workforce, particularly those offering dedicated cybersecurity programs or aspiring to achieve recognition as centers of academic excellence (Marquardson and Gomillion, 2018). The growing demand for qualified professionals in this dynamic field has prompted institutions to continually adapt curricula to equip students with relevant technical and professional skills.

A notable trend in cybersecurity education is the interdisciplinary integration of cybersecurity competencies across multiple academic and professional domains. This approach reflects the pervasive nature of cybersecurity challenges and emphasizes the need for individuals from diverse backgrounds to acquire foundational knowledge in cybersecurity. As McDuffie and Piotrowski (2014) note, essential cybersecurity skills span information technology, risk management, criminal justice, computer science, ethics, and policy development. Zorz (2018) further highlights the importance of technical expertise in programming languages, system architecture, administration, and certifications, while McGettrick (2013) underscores the relevance of soft skills, including effective communication.

The diversity of students' prior knowledge and professional experience presents additional challenges for curriculum design. Students entering cybersecurity programs often have varied IT and professional backgrounds, necessitating curriculum structures that provide foundational knowledge while supporting advanced learning and development. Evaluating the alignment between program content and industry needs is therefore essential to ensure graduates are prepared for the evolving demands of the workforce. Consequently, the study does not only describe current practice but also structures it analytically through the ECSF-based Cybersecurity Curriculum Alignment (ECCA) Framework and a taxonomy of program types.

Existing frameworks, such as the European Cybersecurity Skills Framework (ECSF) and the NICE Framework, provide structured approaches to identifying skills required for specific cybersecurity roles (Petersen et al., 2020; ENISA, 2024). This study adopts the ECSF due to its relevance in the European context, using it to analyze Swedish

cybersecurity programs and assess their effectiveness in fostering essential competencies. Additionally, perspectives from program coordinators were collected to identify challenges, opportunities, and evaluation practices, offering insights into the alignment between educational programs and workforce requirements. This research contributes to understanding and enhancing cybersecurity education in Swedish universities, ensuring graduates are equipped for diverse roles in a rapidly evolving field.

## Research question

This study investigates how curriculum content prepares students for effective roles in cybersecurity. By examining what is taught in Swedish cybersecurity programs, it aims to identify the key knowledge, skills, and competencies essential for success in the field. The central research question is:

- How do Swedish universities ensure their cybersecurity course content aligns with the skills needed for a cybersecurity career, and to what extent?

The research evaluates the effectiveness of current curricula in addressing the evolving demands of the cybersecurity landscape, providing insights to guide future improvements in education.

## Delimitations

The study focuses only on Swedish universities offering cybersecurity master's programs. Vocational schools, corporate training programs, and bachelor-level programs were excluded. Only compulsory courses were included because elective courses differ between students and cannot guarantee consistent role preparation. The analysis is also limited by the availability of publicly accessible information.

## Background

Literature on cybersecurity education encompasses curriculum design, implementation, and assessment, reflecting the field's dynamic and evolving nature. Several studies explore strategies for integrating cybersecurity concepts into existing academic programs, such as those by Belle et al. (2013) and Bogolea and Wijekumar (2004), while others, including Endicott-Popovsky and Popovsky (2014), emphasize hands-on, experiential learning approaches. Hentea et al. (2006) investigate the effectiveness of pedagogical techniques in fostering cybersecurity knowledge, and Whitman and Mattord (2004) examine the alignment of various teaching methods with the roles required in the cybersecurity workforce.

Efforts to enhance student learning often focus on adopting multidisciplinary approaches. Cheung et al. (2011) advocate integrating diverse fields to strengthen cybersecurity education, while Beuran et al. (2016) analyze prominent Japanese training programs to identify best practices and methodologies. The development of frameworks such as Cybersecurity Training and Operation Network Environment (CyTrONE) further supports practical training by automating content creation and environment setup for cybersecurity exercises (Beuran et al., 2018). Tailoring curricula to core knowledge, skills, and abilities (KSAs) has also been suggested to improve student preparedness for professional roles (Jones et al., 2018).

Research additionally examines alignment with established frameworks to ensure educational relevance. Cabaj et al. (2018)

evaluated 21 master's programs in cybersecurity against ACM/IEEE curricular guidelines, assessing topic coverage and distribution across courses. Other studies have utilized frameworks such as NICE to define essential workforce competencies and guide learning outcomes (AlDaajeh et al., 2022). In Sweden, the Knowit Institute mapped courses to cybersecurity job roles across private and governmental institutions, highlighting potential gaps and ensuring alignment with industry requirements (Abdullahi and Olivia, 2024).

Overall, research demonstrates that universities are actively innovating in course design, pedagogy, and assessment to meet workforce needs. Despite these advancements, further research and collaboration are essential to continuously enhance cybersecurity education and prepare graduates for the demands of a rapidly evolving professional landscape. Most of the studies reviewed above were published between 2004 and 2023 and only a few explicitly address the Swedish higher-education context. Apart from the recent national mapping by Abdullahi and Olivia (2024), which does not use ECSF as an analytical lens, we found no systematic analysis of Swedish master's programs based on European skills frameworks. This temporal and geographical gap motivates the present study, which provides an updated picture for the 2024 admissions round and examines how Swedish programs relate to ECSF.

## Cybersecurity skill frameworks

In cybersecurity, frameworks provide foundational structures that guide education, training, and workforce development. They establish a shared understanding of professional role profiles, including relevant skills and competencies. Competencies combine knowledge, technical skills, and human dispositions, representing an individual's ability to perform tasks at varying proficiency levels (Parrish et al., 2018). Within educational contexts, frameworks are used to define learning outcomes, providing a common language that facilitates communication of tasks, expectations, and qualifications across academic and professional environments.

### National Initiative for Cybersecurity Education (NICE)

The NICE framework provides detailed structures for defining cybersecurity work roles, including the associated knowledge, skills, and abilities (KSAs) required to perform them. Knowledge refers to information applied directly to tasks, skills denote observable competence, and abilities indicate the capacity to apply knowledge and skills effectively to produce tangible outcomes (Newhouse et al., 2017). Tasks are defined as specific activities that, combined with other tasks, fulfill responsibilities within a specialized role. The framework is widely used in education to design curricula that align with professional requirements, with particular emphasis on knowledge areas essential for each role.

### CSEC2017 Joint Task Force

The CSEC2017 Joint Task Force (JTF) resulted from collaborative efforts by ACM, IEEE, AIS SIGSEC, and IFIP WG 11.8. It provides guidance for cybersecurity programs to integrate theoretical knowledge with practical skill development. The framework organizes content into Knowledge Areas (KAs) and Knowledge Units (KUs), representing thematic groupings of topics necessary for each area. This structure enables educators to ensure that curricula comprehensively cover both foundational and applied cybersecurity knowledge (CSEC2017 Joint Task Force, 2017).

## European commission report

The European commission report aims to harmonize cybersecurity terminology and definitions across the EU. While it does not specify required knowledge or skills, it provides a coherent taxonomy of cybersecurity domains and subdomains, supporting consistent communication and categorization of competencies across educational and professional contexts (Fovino et al., 2019).

## Cyber security body of knowledge (CyBOK)

CyBOK consolidates widely acknowledged cybersecurity knowledge from textbooks, research, and standards into a unified framework. It defines knowledge areas to provide a shared vocabulary, goals, and approaches to cybersecurity education. By mapping curriculum topics and learning outcomes to these knowledge areas, CyBOK enables comparisons across programs and serves as a foundational guide for designing comprehensive curricula (Rashid et al., 2021; Hallett et al., 2018).

## European cybersecurity skills framework (ECSF)

The ECSF defines twelve role profiles for cybersecurity professionals commonly employed in European organizations. Each profile includes key skills, knowledge, and competencies, offering a standardized language for curriculum development and program alignment. The framework supports higher education, vocational training, and other educational initiatives by guiding course learning outcomes, enabling joint programs, and promoting student mobility. ECSF emphasizes knowledge requirements for each role, assisting universities in designing programs that prepare graduates for specific professional responsibilities while aligning education with labor market needs (Di Franco and Grammatopoulcs, 2022). In the Swedish context, European skills frameworks are relevant because universities operate within the European Higher Education Area and are expected to support mobility and comparability of qualifications. Coordinators in our study described using ECSF and related European documents as informal reference points when discussing program revisions, even when they are not formally mandated. ECSF is therefore treated not as a rigid template, but as a flexible guide that can be interpreted and adapted to local institutional regulations, degree structures and pedagogical traditions.

## Methodology

This study employed a mixed-methods approach to explore the content of cybersecurity programs at Swedish universities, combining document analysis and semi-structured interviews. Document analysis is a systematic procedure for reviewing and evaluating both printed and electronic materials (Bowen, 2009). In this research, document analysis facilitated convergence and corroboration by integrating multiple data sources, primarily focusing on course content available on university websites. Using a framework-based approach, courses were mapped to the roles defined in the European Cybersecurity Skills Framework (ECSF), allowing a detailed assessment of how programs align with industry-relevant competencies and knowledge areas. This approach also enabled demographic analysis, providing insights into the distribution and characteristics of cybersecurity programs across

Swedish universities. In practical terms, this meant using ECSF roles and knowledge items as a checklist when reviewing course syllabi and assessment tasks, identifying which roles each program primarily supports and where important competencies are weakly represented. These document and interview data were interpreted through a four-level analytical structure, comprising policy frameworks, program design, curriculum content and institutional conditions, which we refer to as the ECCA Framework.

## Course–role mapping procedure

For each program, only compulsory courses were included in the mapping, because elective courses, project courses and theses differ between students and cannot guarantee consistent role preparation. Course titles and detailed learning outcomes in the official syllabi were compared with the knowledge units in the European Cybersecurity Education and Professional Training Minimum Reference Curriculum. When a course title exactly matched a curriculum item (for example “Network and Applications Security”), it was assigned to the corresponding role or roles in the European Cybersecurity Skills Framework. For courses that were not explicitly listed, the first author read the course description and learning outcomes and coded the course to the role whose knowledge units best reflected the main focus of the course. For instance, a course emphasizing network architecture, secure configuration and administration was mapped to the Cybersecurity Architect and Cybersecurity Implementer roles.

## Sample selection for universities

The study focused exclusively on academic programs offered by Swedish universities, excluding vocational or private institutions. Emphasis was placed on Master’s degree programs (60–120 credits) explicitly addressing cybersecurity, information security, or network security. Programs were identified using the official Swedish university admissions portals ([Universityadmissions.se](https://www.universityadmissions.se), 2025; [Antagning.se](https://www.antagning.se), 2024) for the Autumn 2024 semester. To ensure relevance, search terms included “Cybersecurity,” “Information Security,” and “Network Security,” alongside their Swedish equivalents. Systematic exclusion of duplicate programs, non-relevant offerings, and programs with both Swedish and English versions resulted in a refined sample of twelve Master’s programs offered at 11 Swedish universities, comprising 91 compulsory courses.

## Semi-structured interviews

To complement document analysis, semi-structured interviews were conducted with program coordinators responsible for the selected cybersecurity programs. This qualitative method was chosen for its ability to capture nuanced perspectives and in-depth insights into curriculum design, course content, and graduate preparedness (Barriball and While, 1994). Interviews were conducted via Zoom, allowing flexibility for participants across different locations while maintaining the benefits of face-to-face interaction. Participants received a summary of the ECSF prior to interviews to provide context, but were not informed of the specific interview questions to ensure unbiased responses. Seven coordinators participated, representing a mix of cybersecurity and information security programs, providing rich, context-specific data. The interviewees included program directors and course coordinators with backgrounds in computer science, information systems and information security, and with several years of experience in curriculum development. To reduce the

risk of social desirability bias, interviews were conducted by a researcher who was not directly involved in the programs under study, and participants were assured that their institutions and programs would not be identifiable in the reporting. During analysis, contrasting views were noted and retained rather than forced into a single consensus narrative, and interpretations were discussed among the author team to check for alternative readings of the data.

The interviews were structured following a five-step guide, encompassing preparation, leveraging existing knowledge, developing and piloting the interview guide, and finalizing questions (Kallio et al., 2016). Questions focused on four main areas: program design and frameworks, role relevance and essential skills, assessment and evaluation, and success factors and challenges. This structure allowed participants to reflect on curriculum alignment with ECSF roles, industry needs, and the effectiveness of their programs in developing key professional competencies.

## Data analysis

Interview recordings were transcribed verbatim to facilitate in-depth qualitative analysis (Kvale, 2007). Data analysis employed descriptive and pattern coding techniques, identifying recurring themes and patterns across interviews. Attribute coding was also used to contextualize responses based on participant roles and institutional characteristics (Wholey et al., 2010). This iterative approach ensured that emerging insights were continuously refined and integrated, enhancing the reliability and validity of the findings.

All interview transcripts were imported into qualitative analysis software (NVivo) and coded by the first author. An initial codebook was developed deductively from the interview guide (program design and frameworks, role relevance and skills, assessment and evaluation, success factors and challenges) and was then refined inductively as new themes emerged in the data. To enhance consistency, previously coded transcripts were revisited whenever new codes were added or definitions were adjusted. Descriptive codes captured what coordinators reported, while pattern codes grouped related statements into higher-level themes on, for example, curriculum change processes or collaboration with industry.

## Validity and reliability

The combination of document analysis and semi-structured interviews strengthened the study’s validity by triangulating multiple data sources (Denzin and Lincoln, 2005). Framework-based mapping provided a structured and consistent evaluation of curricula, while interviews allowed for exploration of participant perceptions and experiences. Reflexivity, neutral descriptors, and pattern matching were applied to minimize bias and ensure credible interpretations (Johnson, 1997).

## Results

This section presents the results data derived from the study, beginning with the findings from the mapping of university courses against the ECSF framework. Following this, insights obtained from semi-structured interviews with program coordinators are detailed. By presenting the results sequentially, this chapter aims to provide a comprehensive overview of the research findings obtained through both methodologies. The integration of these results contributes to a

deeper understanding of the current state of cybersecurity education in Sweden, highlighting the alignment of curricula with professional requirements and identifying potential gaps in preparing graduates for roles in the cybersecurity workforce. In total, the dataset included 12 master's programs at 11 universities and 91 compulsory courses.

## Mapping course contents to roles

As introduced previously, the European Cybersecurity Skills Framework (ECSF) defines twelve roles in the cybersecurity domain, each requiring a distinct set of knowledge and competencies. These roles are designed to cover the diverse range of responsibilities and challenges encountered by cybersecurity professionals in contemporary organizations. The twelve roles are:

- Chief Information Security Officer (CISO): Oversees the organization's overall cybersecurity strategy, ensuring alignment with business goals and regulatory requirements (ENISA, 2024).
- Cyber Incident Responder: Responds swiftly to cyber incidents, implementing mitigation strategies to reduce potential damage (ENISA, 2024).
- Cyber Legal, Policy and Compliance Officer: Ensures compliance with relevant laws and regulations governing cybersecurity practices (ENISA, 2024).
- Cyber Threat Intelligence Specialist: Analyzes threat intelligence to anticipate and mitigate emerging cyber risks (ENISA, 2024).
- Cybersecurity Architect: Designs and implements secure systems and networks, integrating security principles at all stages of development (ENISA, 2024).
- Cybersecurity Auditor: Conducts evaluations to ensure the effectiveness of security measures and identifies areas for improvement (ENISA, 2024).
- Cybersecurity Educator: Develops and delivers training programs to improve cybersecurity awareness and skills among individuals and organizations (ENISA, 2024).
- Cybersecurity Implementer: Designs, implements, and manages cybersecurity solutions across systems, networks, and software applications (ENISA, 2024).
- Cybersecurity Researcher: Engages in research to discover vulnerabilities and threats while developing innovative cybersecurity solutions (ENISA, 2024).
- Cybersecurity Risk Manager: Evaluates and mitigates risks associated with cybersecurity threats, ensuring preparedness for potential impacts (ENISA, 2024).
- Digital Forensics Investigator: Investigates and analyzes digital evidence related to cybercrimes and security incidents (ENISA, 2024).
- Penetration Tester: Conducts authorized simulated attacks to identify vulnerabilities and strengthen organizational security (ENISA, 2024).

These roles reflect the increasing complexity and interconnectedness of modern digital systems. The ECSF framework serves as a benchmark for defining the competencies needed to fill these roles and provides a reference point for evaluating cybersecurity education programs.

CyberSec4Europe has conducted a comprehensive review of cybersecurity educational and training initiatives across Europe (European Cyber Security Organization, 2023). This initiative curates a wide range of programs and contributes to the development of the

European Cybersecurity Education and Professional Training Minimum Reference Curriculum. By leveraging this framework, the study aimed to assess the alignment of Swedish university programs with the knowledge requirements associated with each ECSF role.

## Mapping courses to roles

To align university courses with ECSF-defined knowledge areas, the study employed a mapping approach based on the European Cybersecurity Education and Professional Training Minimum Reference Curriculum (European Cyber Security Organization, 2023). Table 1 summarizes how each course corresponds to the ECSF roles. It is important to note that the Minimum Reference Curriculum emphasizes foundational knowledge and skills required for each role. These courses provide essential preparation but do not guarantee mastery or readiness for independent professional practice. For instance, a course in "Cybersecurity Principles" may contribute to the competencies needed for a CISO but is not sufficient on its own to fully prepare a graduate for this role.

Table 1 illustrates these alignments with several concrete examples. Courses such as "Network and Applications Security" and "Vulnerability Assessment and Threat Management" address technical content on secure network configuration, attack techniques and incident handling, and are therefore mapped mainly to the Penetration Tester, Cyber Threat Intelligence Specialist, Digital Forensics Investigator and Cyber Incident Responder roles. In contrast, courses like "Information and Cybersecurity Management" and "Cybersecurity and Digital Era Leadership" focus on governance, risk management, regulatory compliance and strategic decision-making, which align more closely with roles such as Chief Information Security Officer, Cyber Legal, Policy and Compliance Officer and Cybersecurity Risk Manager. This combination shows how different types of curriculum content support distinct clusters of ECSF roles.

Graduates are assumed to be ready for junior-level roles, such as trainee positions, where practical experience complements theoretical knowledge (European Cyber Security Organization, 2023). Elective courses, project-based learning, and thesis work were excluded from the mapping due to their variability across students, focusing the assessment solely on core program components.

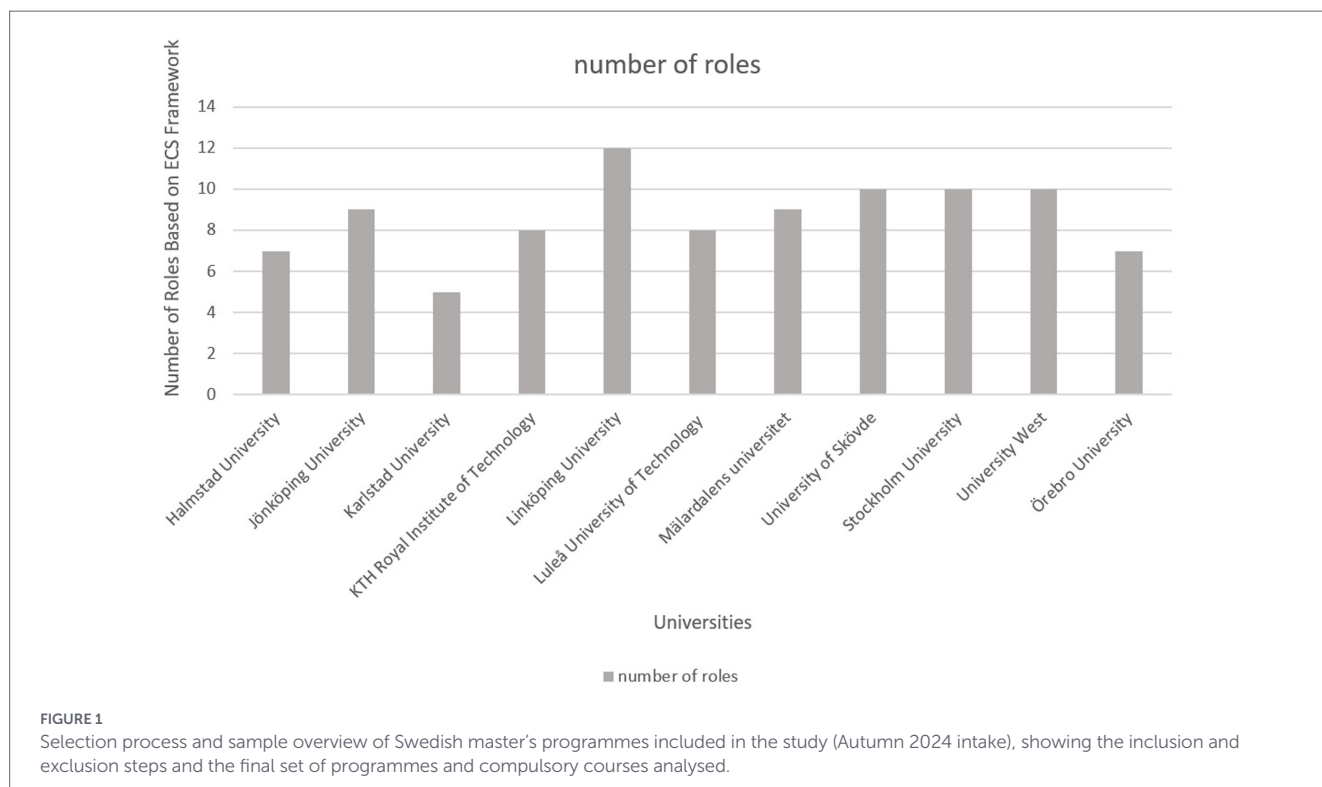
The mapping demonstrates that while foundational courses are covered across multiple universities, specialized topics such as AI security, cloud security, and machine learning security appear less frequently. This disparity highlights potential gaps in preparing students for emerging cybersecurity challenges, and suggests that curricula could be strengthened by expanding dedicated content on AI security, machine learning security and cloud security beyond the small number of courses currently identified. This course to role mapping forms the curriculum level of the ECCA Framework and provides the empirical basis for distinguishing different types of Swedish cybersecurity related master's programs in the taxonomy presented later in the article.

## University-specific analysis

Figure 1 illustrates the frequency of courses offered by universities, while Figure 2 summarizes the number of roles each university addresses. The data indicate that certain emerging topics, including AI, machine learning, and cloud cybersecurity, are underrepresented, suggesting areas for curriculum development.

TABLE 1 Mapping of courses to ECSF roles.

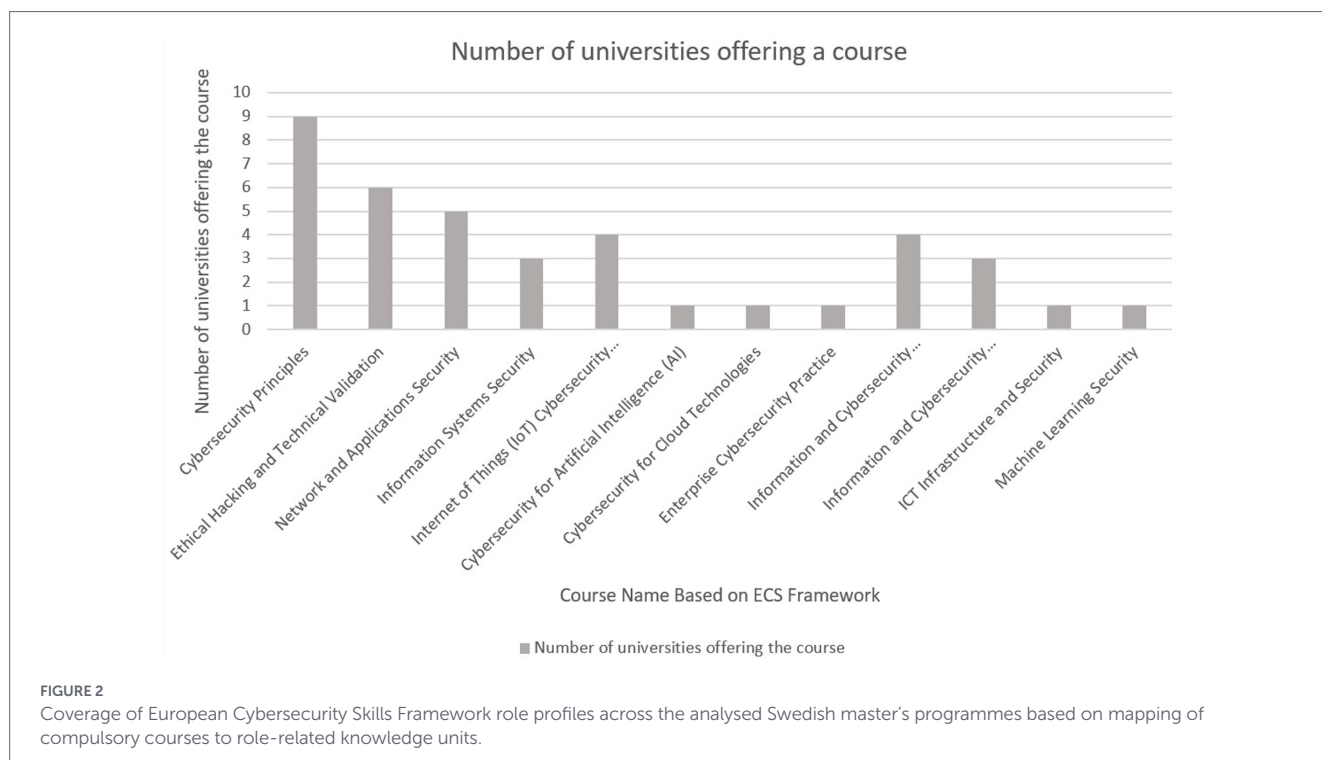
Subject name	Mapping with ENISA ECSF roles
ICT Infrastructure and Security	Cybersecurity Architect, Cybersecurity Implementer
Cybersecurity Principles	Chief Information Security Officer (CISO), Cybersecurity Auditor, Cybersecurity Implementer
Information and Cybersecurity Management	Cyber Legal, Policy and Compliance Officer, CISO, Cybersecurity Risk Manager
Cybersecurity Project Management	CISO, Cybersecurity Researcher, Cybersecurity Implementer
Information Systems Security	CISO, Cybersecurity Architect, Cybersecurity Implementer
Enterprise Cybersecurity Practice	CISO, Cybersecurity Risk Manager, Cybersecurity Implementer, Cyber Incident Responder
Network and Applications Security	Cyber Threat Intelligence Specialist, Cybersecurity Implementer, Penetration Tester
Vulnerability Assessment and Threat Management	Penetration Tester, Cyber Threat Intelligence Specialist, Digital Forensics Investigator, Cyber Incident Responder
Cybersecurity for AI	Cyber Threat Intelligence Specialist, Cybersecurity Researcher
Machine Learning Security	Cyber Threat Intelligence Specialist, Cybersecurity Architect, Cybersecurity Researcher
Cybersecurity for Cloud Technologies	Cyber Legal, Policy and Compliance Officer, Cyber Threat Intelligence Specialist, Cybersecurity Implementer, Cybersecurity Risk Manager
Cybersecurity for the Digital Transformation	CISO, Cybersecurity Educator, Cybersecurity Researcher
Cybersecurity and Digital Era Leadership	CISO, Cybersecurity Educator
Ethical Hacking and Technical Validation	Penetration Tester, Cyber Threat Intelligence Specialist, Digital Forensics Investigator
Cybersecurity and Cyber Ranges in Practice	Cybersecurity Educator, Penetration Tester
Cybersecurity Forensics/Threat Intelligence	Cyber Threat Intelligence Specialist, Digital Forensics Investigator
IoT Cybersecurity Practitioner	Cyber Legal, Policy and Compliance Officer, Cybersecurity Educator, Cybersecurity Researcher



## Interview results

Interviews with program coordinators provide qualitative insights into the design, implementation, and evaluation of cybersecurity programs in Sweden. Respondents were divided into two categories:

coordinators from cybersecurity-focused programs and those from information security programs. Findings are organized into four thematic areas: Program Design and Framework, Role Relevance and Essential Skills, Assessment and Evaluation, and Success Factors and Challenges.



## Program design and framework

Responses revealed variations in the adoption of frameworks such as ECSF, CSEC2017, and CyBok. Some coordinators integrate frameworks extensively, while others adapt existing courses or develop new ones to address identified gaps. Coordinators highlighted that ECSF serves as guidance for professional roles rather than academic program design. Many emphasized that universities should focus on foundational knowledge and research competencies, leaving role-specific vocational training for post-graduation or industry programs. Within the ECCA Framework these interview insights correspond to the program design and institutional conditions levels, showing how local choices and constraints shape ECSF alignment in practice.

## Role relevance and essential skills

Coordinators noted the importance of aligning programs with industry demands. Technical programs emphasize skills for Penetration Testers and Digital Forensics Investigators, while managerial or human-centric programs focus on CISOs and Risk Managers. Internship opportunities remain limited, and industry requests for trainees with broad skill sets underscore the value of versatile graduates.

## Assessment and evaluation

Universities employ metrics such as graduate employment rates, student feedback, and industry input to evaluate program effectiveness. Initiatives like Cybercampus Sweden aim to consolidate resources, promote cross-university collaboration, and enhance research and education in cybersecurity. While frequent minor updates occur, comprehensive curriculum redesigns are less common due to resource constraints and the complexity of implementation.

## Success factors and challenges

Key factors for program success include responsiveness to industry developments, balanced theoretical and practical training, and inclusive learning practices. Challenges include recruiting qualified faculty, rapidly evolving technologies, and the resource-intensive nature of implementing new courses. Coordinators stressed the importance of developing both technical and soft skills, including communication and management competencies, to prepare graduates for diverse professional roles.

The results indicate that Swedish universities provide foundational knowledge for all ECSF roles, but specialized courses are unevenly distributed. Interview findings highlight the tension between academic priorities and industry needs, with practical constraints affecting program design and update frequency. Emerging areas such as AI, machine learning, and cloud security are less represented, suggesting potential directions for curriculum enhancement. Overall, the integration of course mapping with interview insights provides a comprehensive view of Sweden's cybersecurity education landscape, highlighting strengths, gaps, and opportunities for continuous improvement.

In summary, the main empirical findings are: (1) all twelve ECSF roles are covered across the Swedish programs, but the depth and specialization of coverage vary substantially between institutions; (2) technical roles such as Penetration Tester, Digital Forensics Investigator and Cybersecurity Architect are strongly represented in some programs, while managerial and policy-oriented roles are more visible in others; (3) emerging domains such as artificial intelligence security, machine learning security and cloud security are only marginally addressed in compulsory courses; and (4) structural constraints on staffing, time and internal processes limit the pace at which programs can respond to new competence needs.

## Taxonomy of Swedish cybersecurity-related master's programs

Based on the ECCA Framework and the combined course mapping and interview findings, the analysed programs can be grouped into four categories. Technical specialist programs focus on areas such as penetration testing, digital forensics and secure systems engineering and primarily prepare students for highly technical ECSF roles. Management-oriented information security programs emphasize governance, risk management, compliance and organizational security, aligning more closely with roles such as CISO, Cybersecurity Risk Manager and Cyber Legal, Policy and Compliance Officer. Hybrid socio-technical cybersecurity programs deliberately combine technical content with human, organizational and policy perspectives and aim to provide broad preparation across multiple ECSF roles. Finally, general IS / CS programs with limited cybersecurity anchoring include only a small number of compulsory security courses and therefore offer partial preparation for specific ECSF roles rather than a full cybersecurity profile.

## Discussion and conclusion

The discussion focuses on key findings from this study and highlights areas for further research within the Swedish cybersecurity education landscape. Analysis of over half of Sweden's universities offering cybersecurity programs indicates that no single framework is universally adopted across institutions. Various organizations, including ENISA, have developed frameworks to guide curriculum development, aiming to harmonize cybersecurity education and address skill shortages across Europe. However, Swedish universities have largely not adopted these frameworks, reflecting the autonomy inherent in higher education institutions and the need for academic flexibility.

As cybersecurity education becomes increasingly prevalent at the undergraduate level, there is a growing need for master's programs to focus on specialized content. Students often acquire foundational cybersecurity knowledge during their undergraduate studies, creating an expectation for master's programs to provide deeper technical and managerial expertise. Despite this, there is no standardized approach in Sweden for assessing program effectiveness, though prior research highlights the importance of practical instruction, laboratory exercises, and periodic self-assessment to ensure compliance with accreditation standards and learning outcomes. The dynamic nature of cybersecurity—shaped by evolving digital technologies, emerging threats, and industry requirements—further complicates curriculum design and evaluation.

The interview findings also show that structured internship opportunities in Swedish cybersecurity master's programs are limited, with only one university in the sample offering a systematic internship model. Most programs rely on individual arrangements or thesis projects for workplace exposure, which creates unequal access to practice-based learning. To strengthen the link between curricula and labor market needs, universities could make internships an integrated and credit-bearing component of the program, develop common guidelines with industry partners for supervision and assessment, and use ECSF roles as a reference when formulating learning outcomes for

internship placements. Such measures would increase both the number and the quality of internships and better support students in applying their knowledge in real organizational settings.

Interviewees pointed to several reasons for this limited coverage of emerging areas such as artificial intelligence security, machine learning security and cloud security. Some coordinators described a lack of staff with specialized expertise in these domains, which makes it difficult to develop and sustain advanced courses. Others emphasized that program changes are slow and administratively demanding, so updating curricula to include new topics can take several years. In addition, many programs prioritize foundational security concepts and core infrastructure topics, which leaves little room for rapidly evolving specializations. Together, these factors help explain why emerging domains are often integrated as small topics within existing courses rather than offered as dedicated modules, despite being recognized as important for future graduates.

Two key strategies have been suggested to enhance cybersecurity education. First, closer collaboration between universities and professional organizations, such as ENISA, NIST, IEEE, and ACM, could help align curricula with industry needs and better prepare graduates for the workforce. Second, the incorporation of educational psychology principles, including instructional theories like cognitive load theory, can improve teaching effectiveness and optimize learning outcomes.

## Scientific contribution

The contribution of this article is threefold on cybersecurity education and competence development. First, it proposes the ECCA Framework (ECSF-based Cybersecurity Curriculum Alignment Framework), which integrates four levels of analysis: (1) external skills frameworks and policy expectations, (2) university-level program design logics, (3) curriculum-level ECSF role coverage based on mapping 91 compulsory courses, and (4) institutional conditions for curriculum change identified through interviews with seven program coordinators. The framework shows that national alignment to ECSF cannot be understood only by counting which roles are covered; it also depends on how programs are designed and governed, and on their capacity to adapt. Second, based on this framework, the article introduces a taxonomy of Swedish cybersecurity-related master's programs that distinguishes between technical specialist programs, management-oriented information security programs, hybrid socio-technical cybersecurity programs, and general IS / CS programs with limited cybersecurity anchoring. This taxonomy is empirically grounded in an ECSF-based mapping of 91 compulsory courses and seven in-depth interviews with program coordinators, and can be reused to classify curricula in other national contexts or in longitudinal studies. Third, the article contributes empirical evidence on the fragmented and *ad hoc* use of skills frameworks such as ECSF in Swedish higher education. It identifies systemic barriers to program adaptiveness, including staff shortages, slow and complex institutional change processes, and limited collaboration with industry, which collectively constrain universities' ability to respond to emerging needs such as AI security, machine learning security, and cloud security. Together, these contributions deepen our understanding of how a European skills framework is translated into actual curricula in a specific national context and offer a structured basis for future comparative and longitudinal studies of cybersecurity education.

## Research limitations and future research

This study includes the small sample size of seven interviewees and the evolving nature of university programs, which may affect the generalizability of the findings. Time constraints and participants' availability further limited the breadth of data collection. Future research could expand to survey all Swedish universities offering cybersecurity programs, employ longitudinal designs to track curriculum evolution, and investigate standardized methods for assessing program effectiveness. Future work should focus on comparative analyses of different educational frameworks, examining their strengths, limitations, and applicability within Sweden. Research into systematic evaluation methodologies for cybersecurity programs could support curriculum enhancement and ensure alignment with both industry demands and societal needs.

To sum up, the study demonstrates that while Swedish universities offer broad coverage of cybersecurity roles aligned with the European Cybersecurity Skills Framework (ECSF), gaps remain, particularly in specialized areas such as AI, cloud technologies, and machine learning security. Universities exhibit varied approaches to program design, reflecting both strengths in adaptability and challenges in ensuring consistency. Internship opportunities remain limited, potentially hindering students' practical exposure. Success factors include staying abreast of industry trends, integrating practical skills, and fostering inclusivity, while challenges include rapid technological change, recruitment of qualified staff, and resource constraints. Initiatives like Cybercampus Sweden highlight opportunities for collaboration and innovation, emphasizing the need for continued dialog between academia, industry, and policymakers to ensure that cybersecurity education remains effective, relevant, and responsive to evolving challenges.

## Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

## Ethics statement

Ethical principles were prioritized throughout the study, with particular attention to confidentiality, informed consent, and participant well-being (Brinkmann and Kvale, 2005; DiCicco-Bloom and Crabtree, 2006). Participants were informed of the study's objectives via email and provided consent for recording. Identifying information, including program and university names, was withheld to protect anonymity. These practices ensured the ethical integrity of the research and safeguarded participants while

generating valuable insights into cybersecurity education in Sweden.

## Author contributions

BB: Investigation, Conceptualization, Resources, Validation, Writing – review & editing, Visualization, Writing – original draft, Methodology, Software, Data curation, Formal analysis. AH: Conceptualization, Project administration, Supervision, Writing – original draft, Investigation, Funding acquisition, Writing – review & editing.

## Funding

The author(s) declared that financial support was not received for this work and/or its publication.

## Conflict of interest

The author(s) declared that this work was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

## Generative AI statement

The author(s) declared that Generative AI was not used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

## Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

## References

Abdullahi, A., and Olivia, M. (2024). Nationell kompetensförsörjning | IT-, informationsoch cybersäkerhet. Available at: <https://info.knowit.se/rapport-nationell-kompetensforsorjning> (Accessed January 25, 2024)

AlDaajeh, S., Saleous, H., Alrabaa, S., Barka, E., Breiting, F., and Choo, K. K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Comput. Secur.* 119:102754. doi: 10.1016/j.cose.2022.102754

- Antagning.se Anmälan till högskola och universitet. Antagning.se, Stockholm (2024). Available at: <https://www.antagning.se/> (Accessed January 20, 2024)
- Auffret, J.-P., Snowden, J. L., Stavrou, A., Katz, J. S., Kelley, D., Rahman, R. S., et al. (2017). Cybersecurity leadership: competencies, governance, and technologies for industrial control systems. *Journal of Interconnection Networks* 17:1740001.
- Barriball, K. L., and While, A. (1994). Collecting data using a semi-structured interview: a discussion paper. *J. Adv. Nurs.* 19, 328–335.
- Belle, T., Imboden, T., and Martin, N. L. (2013). An undergraduate information security program: more than a curriculum. *J. Inf. Syst. Educ.* 24, 11–18.
- Beuran, R., Chinen, K. I., Tan, Y., and Shinoda, Y. (2016). *Towards effective cybersecurity education and training* Cham, Springer.
- Beuran, R., Tang, D., Pham, C., Chinen, K. I., Tan, Y., and Shinoda, Y. (2018). Integrated framework for hands-on cybersecurity training: CyTrONE. *Comput. Secur.* 78, 43–59. doi: 10.1016/j.cose.2018.06.001
- Bogolea, B., and Wijekumar, K. (2004). Information security curriculum creation: A case study. In proceedings of the 1st annual conference on information security curriculum development, Piscataway: IEEE, 59–65.
- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qual. Res. J.* 9, 27–40. doi: 10.3316/qj0902027
- Brinkmann, S., and Kvale, S. (2005). Confronting the ethics of qualitative research. *J. Constr. Psychol.* 18, 157–181. doi: 10.1080/10720530590914789
- Cabaj, K., Domingos, D., Kotulski, Z., and Respicio, A. (2018). Cybersecurity education: evolution of the discipline and analysis of master programs. *Comput. Secur.* 75, 24–35.
- Chakravarty, A., Grewal, R., and Sambamurthy, V. (2013). Information technology competencies, organizational agility, and firm performance: enabling and facilitating roles. *Inf. Syst. Res.* 24, 976–997. doi: 10.1287/isre.2013.0500
- Cheung, R. S., Cohen, J. P., Lo, H. Z., and Elia, F. (2011). Challenge-based learning in cybersecurity education. *Computer Engineering and Applied Computing: In Proceedings of the World Congress in Computer Science.*
- Conklin, W. A., Cline, R. E., and Roosa, T. (2014). *Re-engineering cybersecurity education in the US: An analysis of the critical factors.* In 2014 47th Hawaii international conference on system sciences. New York: IEEE, 2006–2014.
- CSEC2017 Joint Task Force (2017). *Cybersecurity curricula 2017: Curriculum guidelines for postsecondary degree programs in cybersecurity.* New York: ACM Available at: <https://www.acm.org/binaries/content/assets/education/curricularecommendations/csec2017.pdf>. (Accessed February 10, 2026)
- Daswani, N., and Elbayadi, M. (2021). “The yahoo breaches of 2013 and 2014” in Big breaches. Sebastopol: O’Reilly Media Cybersecurity lessons for everyone, 155–169.
- Denzin, N. K., and Lincoln, Y. S. (2005). *Handbook of qualitative research.* London, England: SAGE.
- DiCicco-Bloom, B., and Crabtree, B. F. (2006). The qualitative research interview. *Med. Educ.* 40, 314–321.
- Di Franco, F., and Grammatopoulou, A. (2022). European cybersecurity skills framework role profiles. Athens: ENISA. Available online at: <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles> (Accessed January 15, 2024)
- Endicott-Popovsky, B. E., and Popovsky, V. M. (2014). Application of pedagogical fundamentals for the holistic development of cybersecurity professionals. *ACM Inroads* 5, 57–68. doi: 10.1145/2568195.2568214
- ENISA (2024). European cybersecurity skills framework (ECSF): The common language for cybersecurity professional workforce development: European Union Agency for Cybersecurity.
- European Cyber Security Organization. (2023). European cybersecurity education and professional training: Minimum reference curriculum. Brussels: ECSO. Available at: <https://ecs-org.eu/?publications=european-cybersecurity-education-and-professional-training-minimum-reference-curriculum> (Accessed January 18, 2024)
- Fovino, I. N., Neisse, R., Hernández-Ramos, J. L., Polemi, N., Ruzzante, G., Figwer, M., et al. (2019). A proposal for a European cybersecurity taxonomy: Publications Office of the European Union.
- Hallett, J., Larson, R., and Rashid, A., (2018). Mirror, mirror, on the wall: What are we teaching them all? Characterising the focus of cybersecurity curricular frameworks. 2018 USENIX workshop on advances in security education ASE 18. Springer: Cham
- Hentea, M., Dhillon, H. S., and Dhillon, M. (2006). Towards changes in information security education. *J. Inf. Technol. Educ. Res.* 5, 221–233.
- Johnson, R. B. (1997). Examining the validity structure of qualitative research. *Education* 118, 282–292.
- Joiner, K. F., and Tutty, M. G. (2018). A tale of two allied defence departments: new assurance initiatives for managing increasing system complexity, interconnectedness and vulnerability. *Aust. J. Multi Discip. Eng.* 14:6407. doi: 10.1080/14488388.2018.1426407
- Jones, K. S., Namin, A. S., and Armstrong, M. E. (2018). The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school. *ACM Trans. Comput. Educ.* 18, 1–12. doi: 10.1145/3152893
- Kallio, H., Pietilä, A., Johnson, M., and Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *J. Adv. Nurs.* 72, 2954–2965. doi: 10.1111/jan.13031
- Kvale, S. (2007). *Doing interviews.*
- Marquardson, J., and Gomillion, D. (2018). Cyber security curriculum development: protecting students and institutions while providing hands-on experience. *Inf. Syst. Educ. J.* 16:12.
- McDuffie, E. L., and Piotrowski, V. P. (2014). The future of cybersecurity education. *Computer* 47, 67–69. doi: 10.1109/mc.2014.224
- McGettrick, A. (2013). Toward effective cybersecurity education. *IEEE Secur. Priv.* 11, 66–68. doi: 10.1109/msp.2013.155
- Newhouse, W., Keith, S., Scribner, B., and Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework. Gaithersburg: National Institute of Standards and Technology.
- Newlove-Eriksson, L., Giacomello, G., and Eriksson, J. (2018). The invisible hand? Critical information infrastructures, commercialisation and national security. *Int. Spectator* 53, 124–140. doi: 10.1080/03932729.2018.1458445
- Parenty, T. J., and Domet, J. J. (2020). *A leader’s guide to cybersecurity: Why boards need to Lead and how to do it: Harvard Business Review Press.*
- Parrish, A., Impagliazzo, J., Raj, R. K., Santos, H., Asghar, M. R., Jøsang, A., et al. (2018). “Global perspectives on cybersecurity education for 2030: a case for a meta-discipline” in Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education.
- Petersen, R., Santos, D., Smith, M., Wetzel, K., Witte, G., and Scarfone, K. (2020). Workforce framework for cybersecurity (NICE framework). NIST Special Publication, 800–181.
- A. Rashid, H. Chivers, E. Lupu, A. Martin and S. Schneider (Eds.). (2021). Knowledgebase. CyBOK. Available at: [https://www.cybok.org/knowledgebase1\\_1/](https://www.cybok.org/knowledgebase1_1/) (Accessed January 20, 2024)
- Triplett, W. J. (2022). Addressing cybersecurity challenges in education. *International Journal of STEM Education for Sustainability* 3, 47–67.
- Universityadmissions.se. Apply to Swedish universities. Universityadmissions.se. (2025). Available at: <https://www.universityadmissions.se/> (Accessed January 20, 2025)
- Whitman, M. E., and Mattord, H. J. (2004). “Designing and teaching information security curriculum” in Proceedings of the 1st annual conference on information security curriculum development, Boston: Thomson Course Technology. 1–7.
- Wholey, J. S., Hatry, H. P., and Newcomer, K. E. (2010). *Handbook of practical program evaluation.* San Francisco: John Wiley.
- Zorz, Z. (2018). *Researchers hack BMW cars, discover 14 vulnerabilities: HelpNetSecurity.*