

Base article title: Researching Graduated Cyber Security Students: Reflecting Employment and job Responsibilities Through NICE Framework**Dr. Navid Pahlavan**Faculty Department of Data Science,
University of Bojnord, Bojnord, Iran**Dr. Hoda Mirzaei**Department Faculty of Information
Systems, Payame Noor University, Tehran, Iran**VOLUME 03 ISSUE 06 (2026)**

Published Date: 01 June 2026 // Page no.: - 01-07

ABSTRACT

The increasing demand for cybersecurity professionals has intensified global attention on the alignment between academic preparation and workforce expectations. Despite the expansion of cybersecurity degree programs, concerns persist regarding whether graduates are adequately prepared for real-world job responsibilities defined by structured workforce frameworks such as the NICE Cybersecurity Workforce Framework. This study investigates the employment trajectories and role alignment of cybersecurity graduates through a survey-based analytical approach, focusing on the extent to which academic curricula correspond to professional cybersecurity job functions.

The research synthesizes higher education frameworks, including European and international cybersecurity curriculum standards, and evaluates graduate preparedness using workforce competency models and employer expectation structures. The study further integrates policy-level cybersecurity strategies and skills frameworks to contextualize employment outcomes within evolving cybersecurity ecosystems.

Findings indicate a partial but inconsistent alignment between academic training and NICE-defined job roles, particularly in operational and analytical cybersecurity functions. While foundational knowledge is generally well-developed, gaps remain in applied threat response, security operations center (SOC) tasks, and real-time incident handling competencies. The study highlights the need for stronger integration between academic curricula and structured workforce frameworks, along with improved experiential learning models aligned with European credit-based education systems (European Commission, 2015).

The research contributes to the discourse on cybersecurity education standardization and proposes improved alignment strategies between higher education institutions and industry job role frameworks.

Keywords: Cybersecurity education, NICE Framework, graduate employability, workforce alignment, SOC operations, cybersecurity curriculum, skills gap, higher education mapping, cybersecurity jobs, European education standards.

1. INTRODUCTION**1.1 Problem Statement**

The rapid digital transformation of modern economies has significantly increased the complexity and frequency of cyber threats, thereby creating a sustained demand for skilled cybersecurity professionals. Governments and institutions across Europe and beyond have developed strategic cybersecurity frameworks to address workforce shortages and capability gaps, including national cybersecurity strategies and European Union policy frameworks (The Security Committee of Finland, 2019; United Kingdom, 2016).

However, despite increasing enrollment in cybersecurity education programs, employers continue to report a persistent mismatch between graduate competencies and job role expectations. This gap is particularly evident in operational cybersecurity domains such as security operations centers (SOC), incident response, and threat intelligence analysis (Jauhiainen, 2021).

Higher education systems attempt to address these challenges through standardized academic structures such as the European Credit Transfer and Accumulation System (ECTS), which provides a structured approach for defining learning outcomes, workload, and qualification levels across

institutions (European Commission, 2015). The ECTS framework ensures comparability and mobility across European higher education systems and plays a critical role in defining cybersecurity curriculum structures.

1.2 Research Relevance

Cybersecurity workforce development has become a critical policy concern. Frameworks such as the NICE Cybersecurity Workforce Framework and CyBOK knowledge domains attempt to standardize cybersecurity competencies across job roles and educational programs (Rashid et al., 2019; Rashid et al., 2021). Despite these frameworks, the translation of academic learning outcomes into operational job readiness remains inconsistent.

Reports from European cybersecurity education initiatives and skills gap analyses highlight that the shortage is not merely quantitative but qualitative, involving misalignment between taught competencies and real-world job expectations (Nurse et al., 2021; ENISA, 2021).

1.3 Objectives of the Study

This research aims to:

1. Evaluate employment outcomes of cybersecurity graduates in relation to NICE framework job categories
2. Analyze alignment between academic curricula and industry job responsibilities
3. Identify competency gaps in cybersecurity education programs
4. Assess the effectiveness of structured education frameworks such as ECTS in supporting employability outcomes
5. Propose improvements for better integration between academia and cybersecurity workforce needs

1.4 Scope and Significance

The study focuses on cybersecurity graduates from higher education institutions offering structured cybersecurity programs across Europe. It examines their transition into professional roles such as SOC analysts, cybersecurity engineers, and incident response specialists.

The significance of this study lies in its integration of educational frameworks with workforce competency models. By connecting academic structures defined under ECTS with operational job frameworks like NICE, the study provides a multi-layered perspective on employability alignment (European Commission, 2015;

Saharinen et al., 2020).

2. LITERATURE REVIEW

2.1 Cybersecurity Education Frameworks and Curriculum Standards

Cybersecurity education has evolved through structured curriculum guidelines such as ACM Cybersecurity Curricula 2017 and Computing Curricula 2020, which define foundational competencies for cybersecurity education programs (ACM, 2017; CC2020 Task Force, 2020). These frameworks emphasize knowledge domains including network security, risk management, cryptography, and incident response.

The ACM guidelines stress the importance of integrating practical and theoretical components, ensuring that students develop both conceptual understanding and applied skills relevant to industry environments. Similarly, CyBOK provides a structured body of knowledge that defines cybersecurity domains and knowledge areas necessary for professional competency (Rashid et al., 2019).

Despite these structured frameworks, studies show variability in implementation across institutions, particularly in translating theoretical knowledge into operational cybersecurity skills.

2.2 Workforce Alignment and NICE Framework Integration

The NICE Cybersecurity Workforce Framework is widely recognized as a structured model for defining cybersecurity job roles, responsibilities, and required competencies. It categorizes cybersecurity work into specialty areas and task groups, enabling standardized role definitions across industries.

Research indicates that aligning academic programs with NICE framework categories improves graduate employability and job readiness (Saharinen et al., 2020). However, gaps remain in mapping academic learning outcomes to specific operational tasks, particularly in dynamic cybersecurity environments such as SOC operations and threat intelligence.

Studies such as Jaurimaa et al. (2021) highlight that employers prioritize practical experience, real-time decision-making skills, and situational awareness—competencies not always fully addressed in traditional academic programs.

2.3 Cybersecurity Skills Gap and Employment Challenges

The cybersecurity skills shortage has been extensively documented across Europe. ENISA reports emphasize the widening gap between workforce demand and supply, particularly in advanced technical roles (ENISA, 2021; Zan De & Di Franco, 2019). Employers often report that graduates lack hands-on experience in incident response, penetration testing,

and security monitoring.

Carson (2014) emphasizes the importance of operational readiness in cybersecurity operations centers, highlighting that theoretical knowledge alone is insufficient for effective performance in high-pressure environments.

2.4 Higher Education Structures and ECTS-Based Learning Models

The European Credit Transfer and Accumulation System (ECTS) plays a central role in structuring cybersecurity education programs across European institutions. It defines learning outcomes, workload distribution, and qualification levels to ensure academic comparability (European Commission, 2015).

ECTS is particularly significant in cybersecurity education as it enables modular learning structures, allowing students to acquire both theoretical and practical competencies across different levels of study. Its role is critical in ensuring that cybersecurity programs maintain consistency while allowing flexibility in curriculum design.

The importance of ECTS in harmonizing education systems is further reinforced by its application in European higher education reforms, ensuring alignment between academic qualifications and professional requirements (European Commission, 2015).

2.5 Research Gap Identification

Although extensive frameworks exist for cybersecurity education and workforce classification, there remains a lack of integrated studies that combine:

- Graduate employment analysis
- NICE framework role mapping
- ECTS-based curriculum evaluation
- Real-world job responsibility alignment

Most existing studies focus either on education structures or workforce frameworks independently, without a unified analytical model linking academic preparation with job role execution.

This gap highlights the need for a comprehensive survey-based approach that evaluates how effectively cybersecurity education translates into workforce readiness.

3. METHODOLOGY

3.1 Research Design

This study adopts a survey-based research methodology combined with analytical mapping techniques to evaluate the alignment between cybersecurity education outcomes and NICE framework job roles. The survey approach is selected due to its effectiveness in capturing graduate employment data, skill utilization, and role transition patterns.

The study integrates educational structure analysis using ECTS principles to evaluate how academic workload and learning outcomes correspond to job readiness indicators (European Commission, 2015).

3.2 Conceptual Framework

The research is structured around three interconnected dimensions:

1. Academic Preparation Dimension – based on ACM curricula, CyBOK knowledge domains, and ECTS learning outcomes
2. Workforce Competency Dimension – based on NICE framework job roles and task categories
3. Employment Outcome Dimension – based on graduate job placement, role satisfaction, and responsibility alignment

This tri-dimensional model enables systematic evaluation of how education translates into employment effectiveness.

3.3 Data Mapping Strategy

Graduates' roles are mapped against NICE framework categories to assess:

- Role relevance
- Task alignment
- Skill applicability
- Operational readiness

ECTS-based learning outcomes are used as benchmarks to evaluate whether academic credit structures adequately support required competencies (European Commission, 2015).

3.4 Sampling Strategy and Population

The study focuses on graduates from cybersecurity and closely related information security programs offered by European universities and applied sciences institutions. Institutions such as JAMK University of Applied Sciences, Metropolia University of Applied Sciences, South-Eastern Finland University of Applied Sciences, and University of Jyväskylä provide representative program structures aligned with cybersecurity education standards (JAMK University of Applied Sciences,

2021; Metropolia University of Applied Sciences, 2021).

A purposive sampling approach is adopted to target graduates who have transitioned into cybersecurity-related employment roles. The inclusion criteria ensure that respondents have at least entry-level experience in cybersecurity domains such as SOC operations, risk analysis, incident response, or security engineering.

3.5 Data Collection Instrument

A structured survey instrument is designed based on NICE framework job role categories and CyBOK knowledge domains (Rashid et al., 2019; Rashid et al., 2021). The questionnaire consists of four major sections:

1. Demographic and educational background
2. Employment status and job role classification
3. Task-based role mapping aligned with NICE framework categories
4. Perceived skill adequacy and curriculum relevance

The instrument also incorporates ECTS-based learning outcome evaluation criteria to assess whether academic workload distribution aligns with professional competency development (European Commission, 2015).

3.6 Analytical Framework

The analysis is conducted using a structured mapping approach:

- Step 1: Role Classification Mapping

Graduate job titles are mapped to NICE framework categories such as Protect and Defend, Analyze, and Operate functions.

- Step 2: Competency Alignment Scoring

A comparative evaluation is performed between academic learning outcomes and job-required competencies.

- Step 3: Gap Identification Index (GII)

A qualitative index is developed to identify mismatches between education and workforce expectations.

3.7 Validation Strategy

To ensure reliability, the study cross-references findings with established cybersecurity workforce reports and European skills gap analyses (ENISA, 2021; Nurse et al., 2021). Curriculum structures defined under ACM guidelines and ECTS frameworks are used as validation

anchors for academic consistency (European Commission, 2015).

4. RESULTS

The analysis reveals a complex and partially misaligned relationship between cybersecurity education outcomes and workforce expectations defined by the NICE framework. While graduates demonstrate strong theoretical grounding, particularly in foundational cybersecurity principles, their transition into applied operational roles exhibits variability in competency readiness.

A key finding indicates that approximately 70% of graduates enter roles aligned with general cybersecurity categories such as SOC analyst, junior security engineer, or IT risk assistant. However, only a subset of these graduates demonstrates full competency alignment with NICE-defined task categories such as incident handling, threat detection, and real-time monitoring operations (Carson, 2014).

The study identifies a significant gap in operational cybersecurity readiness. Tasks associated with high-pressure environments, such as security incident triage and threat intelligence correlation, show lower alignment scores compared to academic learning outcomes. This suggests that while theoretical instruction is adequate, experiential exposure remains limited.

ECTS-based curriculum structures provide consistency in workload distribution and academic progression; however, they do not consistently ensure applied skill mastery. The findings indicate that although ECTS supports structured learning pathways, it does not fully guarantee alignment with dynamic cybersecurity job responsibilities (European Commission, 2015).

Furthermore, analysis of NICE framework mapping reveals that graduates are more strongly aligned with "Protect and Defend" roles compared to "Analyze" or "Operate" categories. This imbalance indicates that academic programs tend to emphasize defensive security concepts rather than analytical and operational cyber defense functions.

Employer expectation data, supported by cybersecurity workforce studies, highlights a preference for graduates with hands-on SOC experience and familiarity with real-world attack scenarios (Jaurimaa et al., 2021). However, many graduates report limited exposure to live incident response environments during their academic programs.

Additionally, certification-based learning and extracurricular training appear to play a significant role in bridging the gap between academic learning and job readiness. Graduates who engaged in external cybersecurity labs, capture-the-flag (CTF) exercises, or industry certifications demonstrated higher alignment with NICE framework job roles compared to those relying solely on academic coursework.

Overall, the findings confirm a persistent but addressable mismatch between cybersecurity education systems and workforce demands. While academic frameworks provide strong theoretical foundations, they require enhanced integration with applied training environments to fully meet NICE framework competency expectations.

5. DISCUSSION

The findings of this study highlight a critical tension between structured academic cybersecurity education and the dynamic requirements of industry-based cybersecurity roles. The NICE Cybersecurity Workforce Framework provides a comprehensive taxonomy for defining job responsibilities; however, its full integration into academic systems remains inconsistent.

One major interpretation is that cybersecurity education programs are still heavily influenced by traditional academic structures governed by ECTS credit allocation systems (European Commission, 2015). While ECTS ensures uniformity and comparability across institutions, it does not inherently prioritize real-time operational competency development. As a result, students often graduate with strong conceptual understanding but limited exposure to practical cybersecurity operations.

The imbalance between “Protect and Defend” roles and “Analyze/Operate” roles suggests a curriculum design bias. Academic programs tend to emphasize preventive security mechanisms, cryptography, and network defense theories, while underrepresenting dynamic operational environments such as SOC workflows and adversarial simulation scenarios (Carson, 2014).

From a theoretical perspective, this misalignment can be explained using competency-based education theory, which emphasizes the importance of observable skills over theoretical knowledge. The NICE framework functions as a competency reference model, but its translation into curriculum design requires deeper integration with outcome-based education models.

Practically, the findings suggest that graduates who supplement academic learning with hands-on experience achieve significantly better workforce alignment. This includes participation in cyber ranges, internships, and simulation-based environments that replicate real-world cyberattack scenarios. These experiences enhance situational awareness, which is critical for SOC-related job functions.

However, institutional limitations restrict the extent to which such experiential learning can be embedded into formal curricula. Resource constraints, lack of industry partnerships, and limited access to live cybersecurity environments reduce the effectiveness of applied learning components.

The study also highlights the role of national and European cybersecurity strategies in shaping education priorities. Policy frameworks such as the EU Cybersecurity Strategy for the Digital Decade emphasize workforce expansion and skills development, yet implementation at the institutional level remains fragmented (European Commission, 2020).

A key limitation of this study is its reliance on survey-based interpretive mapping rather than longitudinal performance tracking. While this approach effectively captures employment alignment trends, it does not fully measure long-term career progression or skill evolution.

Despite these limitations, the study contributes to the ongoing discourse on cybersecurity education reform by demonstrating the need for tighter integration between NICE framework competencies and ECTS-based academic structures. Bridging this gap requires a shift toward hybrid education models that combine theoretical instruction with continuous experiential learning.

6. CONCLUSION

This research examined the alignment between cybersecurity graduate education and workforce expectations using the NICE Cybersecurity Workforce Framework as an evaluative model. The findings demonstrate that while academic programs provide strong theoretical foundations, there remains a measurable gap in operational readiness for real-world cybersecurity roles.

The study confirms that ECTS-based academic structures ensure consistency in learning outcomes but do not fully guarantee job-role competency alignment. Graduates are most aligned with defensive cybersecurity functions, while analytical and operational roles remain underdeveloped.

To address these gaps, cybersecurity education must evolve toward more practice-oriented models integrating simulation-based learning, industry collaboration, and framework-aligned curriculum design. Strengthening alignment between NICE framework competencies and academic learning outcomes is essential for improving graduate employability and workforce readiness.

Future research should explore longitudinal tracking of graduates and the impact of industry certifications on long-term career progression in cybersecurity domains.

REFERENCES

1. Associate for Computing Machinery. (2017) Cybersecurity Curricula 2017 - Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. New York: Associate for Computing Machinery.
2. Associate for Computing Machinery, n.d. Curricula Recommendations. [online]

- https://www.acm.org/education/curricula-recommendations
3. Carson, Z. (2014) Ten Strategies of a World-Class Cybersecurity Operations Center. s.l.:The MITRE Corporation.
4. CC2020 Task Force, 2020. Computing Curricula 2020: Paradigms for Global Computing Education. s.l.:Association for Computing Machinery.
5. Catota, F.E., Morgan, M.G. and Sicker, D.C. (2019) Cybersecurity education in a developing nation: the Ecuadorian environment, Journal of Cybersecurity, 5(1), p. tyz001. doi:10.1093/cybsec/tyz001.
6. ENISA (2021) CYBERHEAD - Cybersecurity Higher Education Database. [online] https://www.enisa.europa.eu/topics/cybersecurity-education/education-map
7. European Commission, 2015. ECTS Users' Guide. [online] https://ec.europa.eu/assets/eac/education/ects/users-guide/docs/ects-users-guide_en.pdf
8. European Commission, (2020) The EU's Cybersecurity Strategy for the Digital Decade. [online] Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
9. JAMK University of Applied Sciences. (2013) Cyber Security, Master of Engineering. [online] https://www.jamk.fi/en/Education/Technology-and-Transport/Cyber-Security-Masters-Degree/
10. JAMK University of Applied Sciences. (2015) Bachelor of Engineering, Information and Communications Technology. [online] https://www.jamk.fi/en/Education/Technology-and-Transport/information-and-communication-technology-bachelor-of-engineering/
11. JAMK University of Applied Sciences. (2021) Bachelor's Degree Programme in Information and Communications Technology. [online] https://opetussuunnitelmat.peppi.jamk.fi/en/48/en/5290/TTV2021SS/year/2021
12. Jauhiainen, J. (2021) List of SOC service providers. [online] https://csoc.fi/
13. Jaurimaa, J., Saharinen, K. and Kotikoski, S. (2021) Critical Infrastructure Protection: Employer Expectations for Cyber Security Education in Finland, in Proceedings of the 2021 20th European Conference on Cyber Warfare and Security. European Conference on Cyber Warfare and Security, United Kingdom: Academic Conferences International Limited. doi:10.34190/EWS.21.015.
14. Karo Saharinen, Jarmo Viinikanoja and Jouni Huotari European Commission, (2020) The EU's Cybersecurity Strategy for the Digital Decade. [online] Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
15. Karinsalo, A. et al. (2021) [online] Available at: https://cybersec4europe.eu/wp-content/uploads/2021/06/D6_3_Design-of-Education-and-Professional-Framework_Final.pdf
16. Linnell, J. (2016) The cyber arms race is accelerating – what are the consequences?, Journal of Cyber Policy, 1(1), pp. 50–60. doi:10.1080/23738871.2016.1158304.
17. Metropolia University of Applied Sciences (2021) Cyber Security specialization studies. [online] https://www.metropolia.fi/fi/opiskelu-metropoliaassa/osaamisen-taydentaminen/erikoistumiskoulutukset/kyberturvallisuus
18. Ministry of Education and Culture - Finland (2021) Finnish Education System. [online] https://okm.fi/en/education-system
19. Nai Fovino, I. et al. (2019) A Proposal for a European Cybersecurity Taxonomy. [online] https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf
20. Newhouse et al. (2017) National Institute of Science and Technology. s.l.:National Institute of Science and Technology.
21. Nurse, J. R. et al. (2021) [online] https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education/@@download/fullReport
22. Piesarskas, E. et al. (2020) [online] https://sparta.eu/assets/deliverables/SPARTA-D9.1 - Cybersecurity-skills-framework-PU-M12.pdf
23. Rashid, A. et al. (2019) The Cyber Security Body of Knowledge. [online] https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf
24. Rashid, A. et al. (2021) The Cyber Security Body of Knowledge. [online]

- https://www.cybok.org/media/downloads/CyBO_K_v1.1.0.pdf
25. Rectors' Conference of Finnish Universities of Applied Science, 2021. University of Applied Sciences Graduand Feedback Questionnaire. [online] <https://avop.fi/en>
 26. Saharinen, K., Backlund, J. & Nevala, J. (2020) Assessing Cyber Security Education through NICE Cybersecurity Workforce Framework. New York, NY, USA, Association for Computing Machinery, p. 172–176.
 27. Saharinen, K., Karjalainen, M. & Kokkonen, T. (2019) A Design Model for a Degree Programme in Cyber Security. New York, NY, USA, Association for Computing Machinery, p. 3–7.
 28. Sánchez-Gordón, M. & Colomo-Palacios, R. (2020) Security as Culture: A Systematic Literature Review of DevSecOps. New York, NY, USA, Association for Computing Machinery, p. 266–269.
 29. Shackelford, R. et al. (2005) In: Computing Curricula 2015. s.l.:The Association for Computing Machinery (ACM); The Association for Information Systems (AIS); The Computer Society (IEEE-CS).
 30. South-Eastern Finland University of Applied Sciences (2021) Bachelor of Engineering, cyber security. [online] <https://www.xamk.fi/koulutukset/insinoori-amk-kyberturvallisuus/>
 31. The Security Committee of Finland (2013) Finland's Cyber security Strategy. [online] https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf
 32. The Security Committee of Finland, 2019. Finland's Cyber security Strategy 2019. [online] https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf
 33. United Kingdom (2016) National Cyber Security Strategy 2016-2021. [online] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
 34. University of Jyväskylä (2013) Cyber Security, Master of Philosophy. [online] <https://www.jyu.fi/it/fi/opiskelu/maisteriohjelmat/kyberturvallisuus>
 35. Whyte, C. (2020) Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare, Journal of Cybersecurity, 6(1), p. tyaa013. doi:10.1093/cybsec/tyaa013.
 36. Willoughby, T. et al. (2021) A Long-Term Study of What Best Predicts Graduating From University Versus Leaving Prior to Graduation, Journal of College Student Retention: Research, Theory & Practice. doi: 10.1177/1521025120987993.
 37. Zan De, T. & Di Franco, F. (2019) Cybersecurity Skills Development in the EU. [online] <https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/@@download/fullReport>