DOCTORAL CONSORTIUM

WHO WILL KEEP US SAFE? RETHINKING CYBERSECURITY COMPETENCIES FOR AI-TRANSFORMED WORK IN SMES AND SMALL STATES

ANDREJA MARKUN

University of Maribor, Faculty of Organizational Sciences, Kranj, Slovenia
andreja.markun@student.um.si

Cybersecurity is ultimately a human challenge. The ability of organisations to defend themselves depends on the competencies of their people -- yet the competency frameworks designed to support workforce development have not kept pace with how artificial intelligence is transforming what cybersecurity work actually demands. This doctoral research investigates this transformation, focusing on two underserved contexts: small and medium-sized enterprises (SMEs), where one person may be responsible for all security functions simultaneously, and small states, where constrained labour markets and full EU regulatory obligations create a structural mismatch that generic frameworks cannot address. Building on prior empirical research among 235 Slovenian organisations that documented widespread competency gaps and multi-dimensional barriers to their resolution, the research will develop and empirically validate a new competency model designed for AI-augmented cybersecurity environments in SMEs and small states. This paper presents the research plan and explicitly invites feedback on its design and open methodological questions.

DOI
https://doi.org/10.18690/um.fov.4.2026.78

ISBN
978-961-299-152-4

Keywords:
cybersecurity competencies,
artificial intelligence,
SMEs,
small states,
workforce development

University of Maribor Press

1 Introduction

Behind many cybersecurity breaches lies a human gap: between what a person knows and what the situation demands, between the competencies an organisation has developed and those it actually needs. The integration of AI into security operations is widening this gap by reshaping what cybersecurity professionals do, how they work, and which knowledge and skills are critical, while competency frameworks have evolved only slowly.

A security professional in a small Slovenian company may patch systems, manage access, respond to incidents, train colleagues, and navigate regulatory obligations under NIS2 and the new ZInfV-1 law. AI-powered tools automate routine tasks, generate alerts, and suggest responses, yet no existing framework tells this practitioner how to govern such tools, when to trust AI output, or how to explain AI-driven decisions to non-technical managers. The frameworks that shape their development were built for a different organisational reality.

Across Europe, AI adoption in cybersecurity is creating a new category of competency gap: not only a shortage of staff, but a mismatch between existing knowledge and evolving role demands. In Slovenia, 70.6% of organisations report shortages of qualified cybersecurity staff and face barriers extending beyond headcount, including insufficient resources, high turnover, weak development culture, and regulatory demands that grow faster than internal capacity (Markun & Brezavscek, 2025). This points to a structural problem that cannot be solved by hiring alone.

The challenge is particularly acute for SMEs and small states. SMEs – over 99% of EU businesses – often rely on a single security generalist, with no formal team or significant training budget, yet face similar threats and regulatory requirements as large organisations. In small states like Slovenia, these organisational constraints intersect with a labour market that cannot supply enough specialised cybersecurity professionals for a fully differentiated workforce (Blazic, 2021).

This doctoral research starts from these realities. It investigates how AI is transforming cybersecurity work and examines whether existing competency frameworks can support this transformation, particularly for SMEs and small states

that they were never designed to serve. Building on prior empirical work in Slovenia, the research aims to produce a validated competency model that reflects resource-constrained, AI-augmented environments and invites critical engagement from Doctoral Consortium advisors and peers.

2 Problem Definition

2.1 What Existing Frameworks Assume - and What They Miss

The cybersecurity competency landscape is shaped by four key frameworks. NICE maps the workforce into 33 specialty areas with detailed knowledge, skill, and ability statements. ENISA's European Cybersecurity Skills Framework (ECSF) defines 12 professional profiles for the European context (ENISA, 2022). CyBOK organises foundational knowledge across 19 domains, mainly for education (Rashid, 2021). ISC2 certification schemes define professional standards through credentials such as CISSP (ISC2, 2025).

All four frameworks assume large organisations with dedicated security teams, clear role boundaries, specialist career paths, and institutional resources for continuous professional development. This assumption is embedded in role profiles, competency statements, and learning pathways. Analyses of EU-based frameworks highlight limited flexibility for resource-constrained contexts and inadequate coverage of competencies needed in high-stakes environments with limited capacity (Almeida, 2025; Chowdhury & Gkioulos, 2021).

Three gaps are central to this research. First, current frameworks provide little guidance for multi-role environments where one person is responsible for all security functions – a common reality in SMEs (Rawindaran et al., 2025). Second, they overlook labour-market constraints and regulatory implementation challenges in small states (Blazic, 2021). Third, they insufficiently address how AI is restructuring cybersecurity work.

2.2 AI and the Changing Nature of Cybersecurity Work

AI is changing the character of security work – which tasks exist, what human judgement is needed, and what counts as competence. A review of 232 empirical studies shows AI-driven change across threat detection, incident response, vulnerability management, and security monitoring (Kaur et al., 2023). Machine-learning techniques are spreading across security operations, creating demand for professionals who can evaluate, govern, and critically assess AI systems, not just operate tools (Sarker et al., 2021).

This transformation has three dimensions. Some competencies are being replaced: log correlation, signature-based detection, and repetitive monitoring are increasingly automated, shifting focus from manual analysis to interpreting and governing AI output. Other competencies are being transformed: threat hunting now involves directing AI tools, understanding their assumptions and blind spots, and intervening when automated reasoning fails. New competencies are emerging with no precedent in current frameworks, including AI governance, explaining AI-driven decisions to non-technical stakeholders, detecting bias in models, and judging when human override is necessary (Zhang et al., 2022; Abidin et al., 2025).

For an SME security professional, this is particularly demanding. Without a team of specialists, a single practitioner must manage the transition from performing security tasks to overseeing AI systems that do so, while still handling other responsibilities as the only security person. No existing framework has been designed with this situation in mind.

2.3 The Human Reality of Cybersecurity in SMEs and Small States

The SME competency challenge is structurally different from the enterprise challenge. Studies of Welsh SMEs show that existing frameworks offer little actionable guidance for professionals covering multiple roles in organisations without formal security processes, dedicated budgets, or specialist support (Rawindaran et al., 2025). The problem is a misfit between tools and workplace realities, not a lack of motivation.

Research on cybersecurity competencies in SMEs remains limited. Most evidence on workforce development comes from large-organisation contexts, and frameworks often assume conditions SMEs cannot meet (Chaudhary et al., 2023). There is, however, clear demand for cost-effective, scalable, and context-appropriate frameworks that work within SME constraints (Jayathilaka & Wijayanayake, 2025).
In small states, organisational constraints intersect with structural labour-market limitations. Slovenia has a small pool of specialists, professionals often work across multiple institutional settings, and the state must implement NIS2, GDPR, ZInfV-1 and DORA with far less governance capacity than larger member states (Blazic, 2021; ENISA, 2025). Existing frameworks do not start from this context.

2.4 The Research Gap and Central Question

AI-driven change, SME constraints, and small-state conditions together create a misalignment between what cybersecurity work demands and what competency frameworks specify. Studies on frameworks seldom address AI or SME contexts (Almeida, 2025; Chowdhury & Gkioulos, 2021). Research on AI in cybersecurity rarely translates technical findings into competency implications (Kaur et al., 2023). SME-focused studies often omit AI-related competencies (Rawindaran et al., 2025). The small-state dimension remains under-researched (Ruoslahti et al., 2021; Nkongolo et al., 2023). This doctoral research addresses their intersection.
.
The central research question is:

How does artificial intelligence reshape cybersecurity competency requirements, and to what extent do existing competency frameworks reflect these changes in the context of SMEs and small states?

Six sub-questions guide the investigation:

- RQ1: How are AI-related competencies currently represented in major cybersecurity competency frameworks?
- RQ2: How do AI-related competency demands appear in real-world labour market requirements?
- RQ3: What are the key misalignments between framework-defined competencies and actual practice in SMEs?

- RQ4: How do competency requirements differ for multi-role cybersecurity professionals in SME contexts?
- RQ5: How do organisational size, resource constraints, and national context shape competency requirements?
- RQ6: How can a revised, empirically validated competency model be developed for AI-augmented SME environments in small states?

3 Research Contribution

The doctoral research will make three distinct and interconnected contributions to knowledge.

First, it offers a theoretical contribution by proposing a conceptual framework that treats cybersecurity competencies as dynamic functions of AI adoption and organisational context rather than static role attributes. Existing frameworks assume relatively stable profiles that can be mapped and periodically updated; in an AI-driven environment, that assumption no longer holds. The model introduces a categorisation of AI-driven competency change – replaced, transformed, newly required – integrated with a multi-level architecture that explicitly incorporates SME constraints and small-state context.

Second, it contributes empirically by building on the Slovenian survey (Markun & Brezavscek, 2025) to produce the first systematic evidence base on AI-related cybersecurity competency gaps in SMEs within a small EU member state. The doctoral research extends the earlier work by isolating AI-specific and SME-specific dimensions and comparing them with the general competency gap picture.

Third, it offers a practical contribution in the form of an operationally usable competency model tailored to organisations that cannot afford role specialisation and must manage AI-augmented security under resource constraints. Rather than simplifying NICE or ECSF, it aims to provide a tool for the organisational reality of the approximately 25 million SMEs across the EU and the people who work in them (ENISA, 2025), supporting SME managers, HR practitioners, training providers, and policymakers in small member states.

4 Methodology

The research adopts a mixed-methods approach structured across five sequential phases (Table 1). Qualitative and quantitative methods are combined to provide both deep theoretical grounding for model design and empirical validation in real organisational contexts..

Table 1: Research design overview

Phase	Purpose	Methods / Tools	Output
1	Systematic Literature Review	PRISMA; Scopus, WoS, ScienceDirect, IEEE Xplore (2020-2026)	Synthesis of knowledge; research gap map
2	Comparative Framework Analysis: coverage and gaps in NICE, ECSF, CyBOK, ISC2	Structured content analysis; gap matrix coding scheme	Gap matrix: missing dimensions per framework
3	Conceptual Model Development: integrate AI transformation, SME constraints, small-state context	Theory synthesis; AI competency categorisation	Draft conceptual model ready for validation
4	Empirical Validation: test model in Slovenian SMEs; method combination to be finalised (see Table 2)	Mixed methods — options under consideration	Empirically refined and validated model
5	Model Finalisation and Publication	Expert review panel; iterative revision	Final validated competency framework

Source: Own

4.1 Phases 1 and 2: Foundations

Phase 1 will conduct a PRISMA-guided review across four domains: existing competency frameworks and their limitations; AI-driven transformation of cybersecurity tasks; workforce challenges in SMEs; and small-state dynamics in cybersecurity workforce development. Searches in Scopus, Web of Science, ScienceDirect, and IEEE Xplore (2020–2026) will build on initial scoping, which already shows rich AI-focused work but few SME-specific studies.

Phase 2 will compare NICE, ENISA ECSF, CyBOK, and ISC2 using a coding scheme that captures (1) competency coverage and role-specialisation assumptions, (2) organisational context assumptions, including multi-role and resource-constrained environments, and (3) AI-related content such as AI governance, explainable AI, and human–machine teaming. The resulting gap matrix will directly inform the conceptual model.

4.2 Phase 3: Building the Conceptual Model

The conceptual model will integrate the Phase-2 gap matrix with insights from the literature review. It will operate at macro, educational, and organisational levels: accounting for the regulatory environment (NIS2, ZInfV-1, GDPR, DORA) and small-state labour-market dynamics; mapping gaps between existing training and SME needs; and reflecting the reality of multi-role professionals with limited time, budgets, and specialist support.

At its analytical core, the model will distinguish competencies replaced by AI automation, competencies transformed by AI augmentation, and new competencies created by AI adoption, including AI governance, explainable AI, AI ethics, and human–machine collaboration. This structure provides a basis for deciding which existing competencies to deprioritise, reframe, or newly specify. Phase 3 thus produces a testable model.

4.3 Phase 4: Empirical Validation

Phase 4 will test and refine the model in Slovenian SMEs. Several methodological options are under consideration.

A Delphi study with 15–20 cybersecurity experts, HR practitioners, and educators could build normative consensus around the model but is constrained by the size of Slovenia's expert pool. Semi-structured interviews with practitioners in SMEs would provide rich qualitative insight into how AI is experienced and what competency needs it creates. A quantitative survey extending the validated instrument from the earlier Slovenian study would allow statistical assessment across a broader organisational sample. A combined approach offers the most robust validation but

requires careful sequencing and substantial resources. The final design will be informed by a pilot phase and practical considerations around participant availability.

Table 2: Methodological options for Phase 4 empirical validation

Criterion	Delphi Method	Semi-structured Interviews	Quantitative Survey	Combined Approach
Builds normative expert consensus	Yes	Partial	No	Yes
Captures practitioner context and nuance	Partial	Yes	No	Yes
Enables statistical generalisation	No	No	Yes	Yes
Feasibility in small-state expert pool	Medium	High	Medium	Medium
Time and resource requirements	High	Medium	Low-Medium	High
Extends prior survey instrument	No	Partial	Yes	Yes
Suitability for normative model development	High	Medium	Low	High
Key limitation	Small expert pool; time-intensive	Not generalisable	Cannot build normative consensus	High complexity; careful sequencing needed

Source: Own

4.4 Phase 5: Finalisation

Findings from Phase 4 will be integrated with the conceptual model and subjected to structured expert review before publication. The publication strategy will target both academic and practitioner audiences, reflecting the model's intended application in SMEs and in national workforce-development policy.

5 Preliminary Results

5.1 What We Already Know: Evidence from Slovenian Organisations

A survey of 235 Slovenian organisations in May–June 2025 provides the empirical baseline (Markun & Brezavscek, 2025). The sample covered all size categories, ownership types, and sectors; about half were NIS2 or ZInfV-1 obligated entities.

Cybersecurity workforce availability was rated significantly below the neutral midpoint on a five-point scale ($M = 2.74$, $SD = 0.84$; $t(234) = -4.69$, $p < 0.001$, Cohen's $d = -0.31$). A total of 70.6% of organisations reported at least partial shortages of qualified staff, significantly above 50% (binomial test, $p < 0.001$). Shortages therefore appear as a general feature of the landscape.

Public-sector organisations reported higher perceived shortages ($M = 2.45$) than private ($M = 1.79$) or mixed-ownership organisations ($M = 1.73$), with a moderately large effect ($F(2, 232) = 23.82$, $p < 0.001$, $\eta^2 = 0.17$). Structural constraints in public-sector recruitment thus translate directly into higher experienced shortages, which a usable competency framework must acknowledge.

Organisations that treat cybersecurity as a strategic priority are more likely to recognise specific competency shortfalls ($\chi^2 = 59.42$, $df = 8$, $p < 0.001$, Cramer's $V = 0.36$), indicating that perceived gaps reflect both objective shortages and organisational awareness. A framework must therefore support organisations at different maturity levels.

Key barriers to competency development included shortages of qualified staff in the labour market (64.4%), insufficient resources for hiring or outsourcing (50.6%), and high staff turnover (47.8%). Factor analysis identified four underlying dimensions: organisational culture and leadership support, external resource and cost constraints, workforce-market instability, and weak internal motivation for professional development. These factors interact and reinforce one another.

Regulation has so far mainly driven training. NIS2 and ZInfV-1 obligated entities showed increased demand for additional training of existing staff ($\chi^2 = 5.25$, $p = 0.022$, Cramer's $V = 0.22$), but not for broader changes such as new role creation or increased leadership involvement. The doctoral research will explore this gap between regulatory pressure and organisational capacity.

The 2025 study did not address AI-related competencies, did not treat SMEs as a separate category, and did not examine the fit between organisations' needs and existing frameworks. These omissions define the agenda for the doctoral research.

5.2 Scoping the Literature

A preliminary scoping search in Scopus, Web of Science, and IEEE Xplore (2020–2026) found more than 570 results for queries combining cybersecurity competency gaps and AI, but fewer than 25 for queries combining cybersecurity competencies and SMEs. This asymmetry mirrors practice: research has followed new technologies such as AI more than the SME environments where much cybersecurity work takes place (Ruoslahti et al., 2021). Phase 1 will address this through a full PRISMA review.

5.3 Open Questions for Doctoral Consortium Discussion

The following questions are genuine open issues in the research design, presented to invite critical feedback:

- Validation methodology (Phase 4): Which combination of Delphi, interviews, and survey best balances rigour and feasibility in Slovenia?
- Scope of empirical validation: Should the study focus solely on Slovenia as a representative small EU member state, or include additional small states to strengthen generalisability?
- Operationalising AI driven competency change: How should the boundary between "transformed" and "newly required" competencies be defined in empirical instruments, and is the tripartite categorisation optimal?
- Positioning relative to ENISA ECSF: Should the model be framed as a contextual extension of ECSF for SMEs and small states, or as an independent, complementary model with its own policy logic?

6 Future Development

Immediate priorities are the PRISMA systematic literature review and the comparative analysis of NICE, ECSF, CyBOK, and ISC2, which will underpin conceptual model development and later empirical work.

More broadly, the research is driven by the view that the competency challenge in cybersecurity is a human and organisational issue. SME practitioners across Europe operate in conditions that current frameworks rarely recognise: they adopt AI tools

without clear guidance, carry regulatory obligations without specialist support, and build competencies largely in isolation (Rawindaran et al., 2025; Jayathilaka & Wijayanayake, 2025). A validated competency model that starts from these conditions, rather than from large-organisation assumptions, could impact how organisations develop staff, how educators design training, and how policymakers support workforce development in small states.

The Doctoral Consortium is an early but important milestone: a chance to test and refine the research design before the most resource-intensive phases begin. The questions around methodology, scope, operationalisation, and positioning are genuine and will materially shape the project, so feedback on the open issues in Section 5.3 is explicitly sought.

References

Abidin, A., Ariffin, N., Nasruddin, Z., Habidin, N., & Yusoff, M. (2025). Evaluating and modelling artificial intelligence and emotional intelligence to improve cybersecurity employee ethical competence model. Journal of Advanced Research Design, 130(1), 13-25. https://doi.org/10.37934/ard.130.1.1325

Almeida, F. (2025). Comparative analysis of EU-based cybersecurity skills frameworks. Computers & Security. https://doi.org/10.1016/j.cose.2025.104329

Blazic, B. J. (2021). The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. Technology in Society, 66, 101769. https://doi.org/10.1016/j.techsoc.2021.101769

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). Developing cybersecurity education and awareness programmes. Computer Science Review, 50, 100592. https://doi.org/10.1016/j.cosrev.2023.100592

Chowdhury, N., & Gkioulos, V. (2021). Key competencies for critical infrastructure cyber-security. Information and Computer Security, 29(5), 697-723. https://doi.org/10.1108/ICS-07-2020-0121

ENISA. (2022). European Cybersecurity Skills Framework (ECSF) - Role profiles. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

ENISA. (2025). Cybersecurity roles and skills for NIS2 essential and important entities. https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities

ISC2. (2025). 2025 ISC2 Cybersecurity Workforce Study. https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study

Jayathilaka, H. M. T. N., & Wijayanayake, J. (2025). Systematic literature review on developing an AI framework for SME cybersecurity. Journal of Desk Research Review and Analysis, 2(1), 15-30. https://doi.org/10.4038/jdrra.v2i2.53

Kaur, R., Gabrijelcic, D., & Klobucar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Markun, A., & Brezavscek, A. (2025). Skills gaps and workforce challenges in information and cyber security: Insights from Slovenia. Uporabna informatika. https://doi.org/10.31449/upinf.260

Nkongolo, M., Mennega, N., & Van Zyl, I. (2023). Cybersecurity career requirements: A literature review. In Emerging Technologies in Computing. Springer. https://doi.org/10.1007/978-981-99-7962-2_7

Rashid, A. (Ed.). (2021). Cyber Security Body of Knowledge (CyBOK), version 1.1. University of Bristol. https://www.cybok.org/

Rawindaran, N., Jayal, A., & Prakash, E. (2025). Cybersecurity framework: Addressing resiliency in Welsh SMEs. Journal of Cybersecurity and Privacy, 5(2), 17. https://doi.org/10.3390/jcp5020017

Ruoslahti, H., Coburn, J., Trent, A., & Tikanmaki, I. (2021). Cyber skills gaps - A systematic review of the academic literature. Connections: The Quarterly Journal, 20(2), 43-58. https://doi.org/10.11610/connections.20.2.04

Sarker, I., Furhad, M., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modelling and research directions. SN Computer Science, 2. https://doi.org/10.1007/s42979-021-00557-0

Zhang, Z., Hamadi, H., Damiani, E., Yeun, C., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security. IEEE Access, 10, 93104-93139. https://doi.org/10.1109/ACCESS.2022.3204051

About the author

Andreja Markun holds a master's degree in Information Systems and works in the field of information security. Her research focuses on systemic approaches to developing cybersecurity competencies, the impact of regulation on human-resources measures, and the long-term resilience of organisations in the digital environment.