*Issue 4 (22), 2025* *Pedagogy and Education Management Review (PEMR)*
e-ISSN 2733-2039 print-ISSN 2733-2144

# Competency Gaps in Cybersecurity Teaching: Digital Skills, Pedagogy, and Governance

**Boris Zarkov**[1]
[1]*Ph.D. (National Security), Academy of National and Information Security, Plovdiv, Bulgaria*

***Citation:***
Zarkov, B. (2025). Competency Gaps in Cybersecurity Teaching: Digital Skills, Pedagogy, and Governance. *Pedagogy and Education Management Review*, (4(22), 60–71. https://doi.org/10.36690/2733-2039-2025-4-60-71

***Received: November 16, 2025***
***Approved: December 29, 2025***
***Published: December 31, 2025***



***Abstract.*** *Cybersecurity education increasingly occurs in digitally mediated environments that require educators to integrate technical expertise with effective pedagogy and accountable governance. Yet many programs still treat educator readiness as synonymous with subject matter knowledge, leaving critical capability gaps that affect learning quality, equity, and institutional risk. This article identifies and systematizes competency gaps in cybersecurity teaching across three interdependent domains: digital skills, pedagogy, and governance. A structured narrative review and framework mapping approach was applied. Key workforce and curriculum references were used as anchors, including the NIST NICE Framework, ENISA's European Cybersecurity Skills Framework, and the Cybersecurity Curricula 2017 guidelines, complemented by educator digital competence frameworks and cybersecurity risk governance guidance. The analysis indicates three recurring gap patterns. First, technical teaching often underemphasizes platform, cloud, and AI enabled security contexts and the transferable skills emphasized by workforce evidence. Second, pedagogical gaps appear in assessment design for authentic performance, inclusive learning design, and safe handling of sensitive or exploit oriented content. Third, governance gaps emerge in procurement literacy, data governance, incident readiness for learning platforms, and alignment of teaching practice with institutional cybersecurity risk management. Competence in cybersecurity teaching is best treated as a role-based capability that integrates digital practice, pedagogy, and governance rather than as isolated technical mastery. Future studies should validate measurable educator competency indicators, test the effects of targeted professional development on learner outcomes, and develop audit-ready governance routines for AI enabled cybersecurity instruction.*

***Keywords:*** *cybersecurity education; educator competence; digital competence; cyber pedagogy; assessment design; workforce frameworks; NICE Framework; ECSF; curriculum alignment; cyber governance; risk management; professional development.*
***JEL Classification: I21; I23; I28; O33; L86; K24; D83***
***Formulas: 0; fig. 0; tabl. 2; bibl.: 11***

e-ISSN 2733-2039 print-ISSN 2733-2144

**Introduction.** Cybersecurity education is shaped by rapid technological change, adversarial dynamics, and expanding institutional dependence on digital platforms. This context makes teaching quality inseparable from educators' capacity to operate effectively in digital learning ecosystems and to make defensible instructional decisions under uncertainty. Curriculum guidance, such as Cybersecurity Curricula 2017, frames cybersecurity as a discipline involving technology, people, information, and processes in the presence of adversaries, which implies that effective teaching requires more than technical content delivery (Joint Task Force on Cybersecurity Education, 2017).

At the same time, workforce frameworks formalize the tasks and skills expected in real cybersecurity work. The NIST NICE Framework provides a common lexicon of tasks, knowledge, and skills that can be used to align education, training, and workforce development (Petersen et al., 2020). ENISA's European Cybersecurity Skills Framework similarly operationalizes role profiles to support training design and skills recognition (ENISA, 2022). Despite this growing infrastructure, cybersecurity teaching often remains uneven because educator readiness is not consistently defined, assessed, or supported across institutions.

This article argues that competency gaps in cybersecurity teaching cluster into three domains that reinforce one another. Digital skills gaps involve the applied use of modern security tooling and digital learning platforms. Pedagogical gaps involve instructional design, assessment validity, inclusivity, and learner development under conditions of risk. Governance gaps involve procurement, data governance, incident readiness, and alignment with institutional cybersecurity risk management practices, including the type of governance embedded in the NIST Cybersecurity Framework 2.0 and related guidance (NIST, 2024).

**Literature review.** Cybersecurity education is increasingly framed as preparation for work in adversarial environments where technology, people, information, and processes interact under persistent risk. Curriculum guidance emphasizes that cybersecurity is not a narrow technical specialization but a discipline that integrates human, organizational, and societal dimensions, which implies that teaching must develop judgement, responsible practice, and contextual decision making (Joint Task Force on Cybersecurity Education, 2017). Workforce-oriented frameworks reinforce this shift by describing cybersecurity through role profiles, tasks, and knowledge and skill statements that can be used to align education with professional practice (Petersen et al., 2020; ENISA, 2022). In this literature, an educator's subject matter knowledge is necessary but insufficient, because effective teaching requires applied competence in the environments where cybersecurity is practiced, including cloud platforms, identity systems, incident workflows, and security tooling ecosystems. Contemporary work on cyber workforce development also indicates that skills gaps persist and

e-ISSN 2733-2039 print-ISSN 2733-2144

that the demand for adaptable competencies is growing, which increases pressure on educators to keep curricula and lab environments current (ISC2, 2024). The resulting research problem is that educator readiness is often assumed rather than operationalized, and this leads to competency gaps that emerge in digital skills, pedagogy, and governance. These gaps matter because they influence assessment validity, learner safety, and institutional risk exposure, particularly when courses rely on real platforms and third-party services.

Research that anchors education to workforce expectations argues that curricula should be designed around authentic tasks and role responsibilities rather than around static topic lists. The NICE Framework provides a structured vocabulary for cybersecurity work roles and tasks and is widely used as an alignment reference for education and training (Petersen et al., 2020). ENISA's European Cybersecurity Skills Framework similarly emphasizes role profiles and competence descriptions that can support coherent program design and skill recognition (ENISA, 2022). In practice, the literature suggests that digital skills gaps appear when teaching environments lag behind industry shifts, such as cloud-native architectures, identity-first security, automation, and platform security operations. Workforce evidence indicates that many organizations prioritize practical capability and transferable skills, including incident handling, risk communication, and secure configuration, which implies that educators must teach beyond conceptual knowledge toward situated performance (ISC2, 2024). The educational implication is that labs and assessments should represent contemporary operational contexts rather than purely theoretical or legacy network scenarios. Yet studies and policy reports frequently note constraints such as limited infrastructure, insufficient instructor time for toolchain updating, and reliance on vendor-specific materials, which can narrow competence development and reduce portability of skills. As a result, the literature supports ongoing curriculum refresh processes and explicit mapping from learning outcomes to role tasks as mechanisms to reduce digital skills gaps.

Pedagogical research in cybersecurity education emphasizes that assessment should measure authentic capability, including procedural competence, judgement under uncertainty, and responsible decision making. Curriculum guidelines explicitly highlight educational practice, suggesting that cybersecurity programs should incorporate experiential learning, controlled lab work, and scenario-based problem solving to reflect the adversarial nature of the domain (Joint Task Force on Cybersecurity Education, 2017). A persistent pedagogical gap appears when programs rely on low-cost recall testing that fails to capture practical competence, especially for skills such as secure configuration, log analysis, threat modeling, and incident response reasoning. This gap is amplified by the challenges of designing assessments that are both authentic and safe, because

e-ISSN 2733-2039 print-ISSN 2733-2144

cybersecurity instruction can involve dual-use techniques and may create risks if offensive content is presented without ethical framing and containment. The literature also indicates that inclusion is under-addressed in many technical programs, despite evidence that cybersecurity education is affected by heterogeneous prior experience, gendered participation patterns, and accessibility barriers. General educator competence frameworks emphasize empowering learners, using assessment formatively, and designing inclusive learning experiences, which are directly relevant to cybersecurity teaching even though they are not domain-specific (Redecker, 2017; UNESCO, 2018). Moreover, inclusive design approaches such as Universal Design for Learning suggest that accessibility should be embedded into course design through multiple means of engagement, representation, and expression, which can reduce barriers for learners with disabilities and for learners entering cybersecurity from non-traditional pathways (CAST, 2018). Taken together, the literature supports the view that cybersecurity educator competence must include assessment literacy, inclusive pedagogy, and ethical teaching design, not only technical expertise.

A growing body of governance scholarship argues that digital education environments should be treated as socio-technical infrastructures with cybersecurity, privacy, and accountability requirements. NIST's Cybersecurity Framework 2.0 places explicit emphasis on governance as an organizing function, reinforcing that cybersecurity is managed through institutional accountability, policy, and risk processes rather than through technical controls alone (National Institute of Standards and Technology, 2024). When cybersecurity courses use cloud tenants, learning management systems, external labs, and AI-enabled tools, governance competence becomes directly relevant to teaching practice. The literature suggests that governance gaps emerge when instructors and institutions adopt tools without clear understanding of data flows, vendor responsibilities, or incident response procedures for course platforms. These gaps include weak procurement literacy, limited documentation of risk decisions, and unclear escalation routes for misuse, credential leakage, or breaches in learning environments. Workforce and education strategy documents further emphasize that cyber education is a systemic endeavor and that institutions must build capacity through coordinated policy, training, and support structures (Office of the National Cyber Director, 2023). This implies that educator competence in cybersecurity teaching cannot be fully addressed through individual training alone, because institutional routines determine whether teaching environments are secure-by-default and whether accountability mechanisms exist. In synthesis, the governance literature frames cybersecurity teaching as part of institutional risk management, requiring alignment between academic practice and organizational cybersecurity governance.

e-ISSN 2733-2039 print-ISSN 2733-2144

Across the reviewed sources, a consistent conclusion is that competency gaps in cybersecurity teaching are multidimensional and mutually reinforcing. Digital skills gaps can lead to outdated lab scenarios and poor alignment with role tasks, which then undermines the authenticity of assessment and the credibility of program outcomes (Petersen et al., 2020; ENISA, 2022). Pedagogical gaps can yield invalid or unsafe assessments and can intensify exclusion when accessibility and scaffolding are not embedded into course design (CAST, 2018; Joint Task Force on Cybersecurity Education, 2017). Governance gaps can expose institutions to privacy and security risks and can constrain educators' ability to teach safely when platform decisions are made without transparency or accountability (National Institute of Standards and Technology, 2024). The literature therefore supports integrated competence models that combine domain-specific cyber practice with educator competence in assessment, inclusion, and ethics, and with governance competence in tool stewardship and incident readiness (Redecker, 2017; UNESCO, 2018; Office of the National Cyber Director, 2023). An additional implication is the need for better measurement. Framework mapping provides alignment structure, but evidence of educator competence should be demonstrated through teaching artifacts, assessment rubrics, lab security design, and documented governance decisions, rather than through training completion alone. Future research is increasingly oriented toward validating indicators that capture judgement, safety, and accountability in digitally mediated cybersecurity instruction.

**Aims.** The aim of this article is to identify and systematize educator competency gaps in cybersecurity teaching across the interdependent domains of digital skills, pedagogy, and governance, and to frame these gaps as a role-based capability agenda that can inform measurable professional development and audit-ready institutional routines.

**Methodology.** A structured narrative review and framework mapping approach was used to identify and synthesize educator competency gaps. The process had three steps. First, anchor frameworks were selected to represent workforce expectations, curriculum structure, and institutional risk governance. These included the NIST NICE Framework (Petersen et al., 2020), ENISA ECSF (ENISA, 2022), and Cybersecurity Curricula 2017 (Joint Task Force on Cybersecurity Education, 2017), supplemented by the NIST Cybersecurity Framework 2.0 and its overview guide for governance logic (NIST, 2024).

Second, educator digital competence frameworks were used to interpret what "teaching-ready" means in digitally mediated instruction. DigCompEdu and UNESCO's ICT Competency Framework for Teachers were used as general educator competence references for professional engagement, digital resources, assessment, and learner empowerment (Redecker, 2017; UNESCO, 2018).

e-ISSN 2733-2039 print-ISSN 2733-2144

Third, a thematic synthesis was conducted. Statements and constructs were coded into three domains: (a) digital skills and digital teaching operations, (b) pedagogy and assessment, and (c) governance and risk management. The outcome is a gap taxonomy and implementation-oriented recommendations.

**Results.** Cybersecurity teaching is often evaluated through content coverage, certification alignment, and learner satisfaction. These indicators are necessary but insufficient, because they do not directly capture whether instructional practice develops authentic capability, preserves safety, and remains accountable to institutional risk constraints. A deeper reading of the literature suggests that competency gaps cluster into three domains that interact causally. First, digital skills gaps reduce the authenticity of learning tasks and weaken alignment with workforce role expectations (Petersen et al., 2020; ENISA, 2022). Second, pedagogical gaps limit assessment validity and can unintentionally normalize unsafe practices or exclude learners with heterogeneous backgrounds (Joint Task Force on Cybersecurity Education, 2017; CAST, 2018). Third, governance gaps arise when teaching platforms and lab environments are treated as neutral infrastructure rather than as security-relevant systems requiring oversight, documentation, and incident readiness (National Institute of Standards and Technology, 2024). The combined effect is not only reduced learning quality, but also elevated institutional exposure to privacy, security, and reputational risks, especially when courses use cloud tenants, third-party labs, and AI-enabled tools (Office of the National Cyber Director, 2023).

*Digital skills gaps.* Digital skills gaps in cybersecurity teaching are best understood as misalignment between what learners do in educational settings and what practitioners must do in real operational contexts. Workforce frameworks describe cybersecurity capability through tasks and role profiles, which implies that instruction should be mapped to observable performance rather than to static topic lists (Petersen et al., 2020; ENISA, 2022). A common gap pattern is legacy bias, where courses overemphasize traditional perimeter and network-centric scenarios while underrepresenting identity and access management, cloud security posture, DevSecOps workflows, platform security monitoring, and automation practices. This gap appears in lab designs that rely on isolated virtual machines without realistic identity, logging pipelines, access controls, or operational constraints, which then trains learners for an environment that rarely exists outside the classroom. Another recurrent gap concerns toolchain realism. Educators may teach concepts accurately but without sustained competence in current tool ecosystems, including security telemetry, scripting for automation, and safe handling of credentials and secrets. This gap matters because cybersecurity competence is procedural and contextual, and students must learn not only what controls are, but how controls fail, how signals are interpreted, and how decisions are justified. A third digital gap involves operational security in

e-ISSN 2733-2039 print-ISSN 2733-2144

learning environments. Instructors may unintentionally model insecure practices, for example sharing credentials, using weak segmentation, or allowing unsafe storage of artifacts, which can teach harmful norms and increase risk (National Institute of Standards and Technology, 2024). These skill gaps often have structural causes, such as limited infrastructure support, lack of protected time for tool updates, and fragmented coordination between academic units and institutional security teams.

*Pedagogical gaps.* Pedagogical gaps emerge when cybersecurity teaching is treated as technical transmission rather than as competence formation under risk. CSEC2017 emphasizes cybersecurity as a discipline defined by adversaries and uncertainty, which implies that education must develop judgement, not only knowledge (Joint Task Force on Cybersecurity Education, 2017). The first pedagogical gap is assessment validity. Many programs rely heavily on quizzes and short-answer tests that measure recall but fail to capture performance in threat modeling, incident triage, secure configuration, log interpretation, and risk communication. When assessment does not measure authentic performance, educators receive weak feedback about learner competence, and students receive weak signals about what matters. A second gap concerns safe pedagogy for dual-use content. Offensive techniques can be legitimate for learning, but instruction must define boundaries, ethical framing, and containment controls, otherwise the course may normalize harmful behaviors or create unsafe experimentation outside controlled contexts. A third pedagogical gap is inclusion and accessibility. Technical fields often assume a uniform baseline of prior experience, yet cybersecurity cohorts are typically heterogeneous, including learners entering from non-traditional pathways. Without scaffolding, alternative learning pathways, and accessible materials, instruction can amplify exclusion, which is inconsistent with inclusive design principles such as multiple means of engagement, representation, and expression (CAST, 2018). A fourth pedagogical gap is feedback design. Cybersecurity competence improves through iteration, but learners often receive sparse diagnostic feedback on why an approach failed, which limits metacognitive development and professional judgement formation. Educator competence frameworks highlight assessment literacy and learner empowerment as core educator capabilities, which suggests that cyber educators need explicit pedagogical competence, not only technical expertise (Redecker, 2017; UNESCO, 2018).

*Governance gaps.* Governance gaps occur when cybersecurity teaching environments are not governed with the same seriousness as other institutional information systems. NIST CSF 2.0 emphasizes governance as a core function, reinforcing that cybersecurity is sustained through accountability, policies, and risk processes (National Institute of Standards and Technology, 2024). In teaching contexts, governance includes procurement and vendor stewardship, data governance and privacy

e-ISSN 2733-2039 print-ISSN 2733-2144

compliance, incident readiness for learning platforms, and documentation of risk decisions. A common governance gap is procurement illiteracy, where instructors adopt external platforms and lab services without adequate review of data flows, retention practices, access control models, and vendor responsibilities. This is increasingly significant because course platforms may process sensitive student data, credentials, telemetry, and submitted artifacts. Another governance gap is weak incident readiness. Programs often lack clear procedures for credential leakage, misuse of lab resources, unauthorized access, or suspected breaches in teaching environments. Without playbooks and escalation channels, incidents are handled informally, leading to inconsistent response quality and weak learning from failures. A third governance gap concerns accountability and auditability. Many programs cannot reconstruct why a tool was adopted, what risks were considered, and how impacts were monitored. This reduces institutional trust and undermines continuous improvement. National strategies on cyber workforce development emphasize systemic capacity building, which implies that education governance is not separate from cybersecurity governance but part of it (Office of the National Cyber Director, 2023). The practical conclusion is that educator competence must be supported by institutional governance routines, otherwise individual training will not close the gap.

Table 1 translates the taxonomy into operational terms by connecting each gap to observable indicators, likely harms, and realistic institutional controls that enable sustainable improvement.

**Table 1. Competency gaps in cybersecurity teaching: deeper descriptors, indicators, risks, and institutional controls**

| Sub-gap | Observable indicators in teaching practice | Likely harms if unaddressed | Institutional controls and supports |
|---|---|---|---|
| Digital skills | | | |
| Role-task misalignment | Outcomes not mapped to NICE or ECSF roles; labs focus on generic topics rather than tasks | Weak employability transfer; shallow competence | Role-mapped curricula; periodic alignment reviews (ENISA, 2022; Petersen et al., 2020) |
| Legacy lab realism | Isolated VM labs with minimal identity, logging, or operational constraints | Unrealistic mental models; poor readiness for modern environments | Managed cloud tenants; identity and logging baselines; reference architectures |
| Toolchain currency gap | Limited exposure to telemetry pipelines, automation, or platform security workflows | Skill obsolescence; low confidence in practice | Tool refresh cycles; shared lab engineering support; instructor upskilling time |
| Insecure teaching operations | Credential reuse; weak segmentation; poor secrets handling in course materials | Teaches unsafe norms; increases incident probability | Secure-by-default templates; access control standards; minimum lab security baselines (National Institute of Standards and Technology, 2024) |
| Pedagogy | | | |
| Low validity assessment | Recall-heavy tests; few performance rubrics; minimal scenario-based evaluation | Misleading grades; poor competence signal | Authentic assessments; performance rubrics; peer review of assessment design (Joint Task Force on Cybersecurity Education, 2017) |

| Sub-gap | Observable indicators in teaching practice | Likely harms if unaddressed | Institutional controls and supports |
|---|---|---|---|
| Unsafe dual-use teaching | Offensive content without ethics framing and containment; unclear boundaries | Normalization of harm; unsafe external experimentation | Ethics modules; codes of conduct; controlled environments; escalation procedures |
| Inclusion and accessibility gap | High prerequisite assumptions; inaccessible materials; limited scaffolding | Exclusion of non-traditional learners; inequitable outcomes | UDL-aligned design; accessibility checks; multiple pathways (CAST, 2018) |
| Weak feedback for judgement | Sparse diagnostic feedback; limited reflection; limited iteration | Slow development of professional judgement | Structured feedback protocols; reflective write-ups; iteration cycles (Redecker, 2017) |
| Governance | | | |
| Procurement and vendor stewardship gap | Tools adopted without privacy or security review; undocumented data flows | Privacy violations; vendor lock-in; compliance risk | Procurement checklists; review gates; contractual controls; documentation requirements |
| Incident readiness gap | No playbooks for credential leaks or platform misuse; unclear reporting channels | Delayed response; inconsistent handling; reputational risk | Incident playbooks; reporting channels; coordination with security team (National Institute of Standards and Technology, 2024) |
| Low auditability and accountability | No record of risk rationale; no monitoring of differential impacts | Weak trust; limited learning from failures | Audit trails; periodic governance reviews; cross-functional committee oversight |
| Misalignment with institutional risk | Course environments managed outside institutional security processes | Fragmented controls; unmanaged exposure | CSF-aligned governance integration; shared responsibility models (Office of the National Cyber Director, 2023) |

*Source: systematized by the author*

The table 1 indicates that many competency gaps are system-level issues rather than individual deficits. Sustainable improvement requires coupling educator development with institutional controls that make secure, inclusive, and auditable teaching the default condition.

Table 2 proposes concrete evidence artifacts that institutions can use to assess educator competence in a practice-based way, reducing reliance on training completion as a proxy for capability.

**Table 2. Evidence artifacts that can demonstrate educator competence across the gap taxonomy**

| Domain | Evidence artifact | What it demonstrates | How it can be reviewed |
|---|---|---|---|
| Digital skills | Role-task mapping document | Alignment of outcomes to NICE or ECSF roles | Annual curriculum review panel |
| | Secure lab design specification | Segmentation, access controls, credential handling | Security and academic joint review |
| Pedagogy | Assessment rubric for a scenario-based task | Validity, performance criteria, judgement markers | Peer review, moderation, calibration |
| | Inclusion plan for a module | Scaffolding, accessibility measures, multiple pathways | Accessibility audit and learner feedback |
| Governance | Tool adoption rationale | Data flow, privacy, vendor responsibilities, risk trade-offs | Procurement and privacy review gate |
| | Incident playbook for course platforms | Preparedness, escalation, reporting roles | Tabletop exercise once per term |

*Source: systematized by the author*

e-ISSN 2733-2039 print-ISSN 2733-2144

Evidence artifacts make competence measurable and improveable. They also help institutions learn across courses, enabling consistent standards and reducing the variability that often produces recurring gaps.

A deeper taxonomy clarifies that cybersecurity teaching competence is not an individual characteristic expressed only in classroom delivery. It is a capability that is enacted through lab architectures, assessment designs, inclusion practices, and governance decisions. Workforce frameworks justify task-based alignment, curriculum guidance justifies authentic and safe pedagogy, and cybersecurity governance guidance justifies the integration of teaching platforms into risk management routines (ENISA, 2022; Joint Task Force on Cybersecurity Education, 2017; National Institute of Standards and Technology, 2024; Petersen et al., 2020). The main practical implication is that competency gaps close most reliably when institutions invest in shared lab infrastructure, assessment design capacity, and governance routines that reduce the burden on individual instructors while raising the baseline quality of teaching environments.

**Discussion.** The NICE Framework emphasizes task-based descriptions of cybersecurity work and explicitly supports education and training alignment with workforce needs (Petersen et al., 2020). However, teaching programs often lag behind practice shifts such as cloud-native architectures, platform security, identity-first security models, and AI enabled workflows. This mismatch is reinforced by workforce evidence indicating that skill gaps remain widespread and that organizations increasingly prioritize adaptable, transferable skills alongside technical expertise (ISC2, 2024). The practical implication is that cybersecurity educators need competence in continuous curriculum updating, toolchain maintenance, and role mapping so that instruction remains anchored in realistic task contexts.

CSEC2017 positions cybersecurity as a discipline requiring assured operations in the presence of adversaries, which implies that assessment must capture judgement, trade-offs, and procedural competence, not only conceptual understanding (Joint Task Force on Cybersecurity Education, 2017). Yet many instructional designs default to low-cost testing formats that under-measure authentic capability. A further pedagogical gap concerns inclusion. General educator frameworks emphasize learner empowerment and assessment competence as essential educator capacities, which suggests that accessibility and scaffolding should be embedded into cybersecurity instruction rather than treated as optional adjustments (Redecker, 2017; UNESCO, 2018). In cybersecurity, this is especially important because heterogeneous prior experience is common and because learning environments can unintentionally amplify exclusion when prerequisites are assumed rather than supported.

The NIST Cybersecurity Framework 2.0 formalizes cybersecurity governance through a dedicated function and encourages integration with broader risk management practices (NIST, 2024). For cybersecurity

e-ISSN 2733-2039 print-ISSN 2733-2144

education, governance competence includes understanding tool related data flows, managing credentials and lab segmentation, documenting risk decisions, and preparing for incidents in course platforms. These practices are often missing because teaching is treated as separate from institutional security operations. Yet education environments are operational technology in practice, particularly when courses use real cloud tenants, external platforms, and AI tools.

National policy also reinforces that education and workforce development are structural priorities and that barriers to access and diversity must be addressed. The U.S. National Cyber Workforce and Education Strategy explicitly frames cyber talent development as a systemic effort and highlights structural challenges related to workforce diversity and access to education and training (Office of the National Cyber Director, 2023). For institutions, the key point is that educator competence should be designed as institutional capability building, with governance routines that allow educators to teach safely and credibly.

Based on the results of the conducted research, offering:

1. *Adopt a role-mapped competence model for cybersecurity educators.* Use NICE and ECSF as anchors to map course outcomes to role tasks and to make competence expectations explicit (Petersen et al., 2020; ENISA, 2022).
2. *Upgrade assessment design toward authentic performance evidence.* Shift emphasis from recall testing toward scenario-based assessment, lab practicums, and structured rubrics aligned to tasks and decision quality (Joint Task Force on Cybersecurity Education, 2017).
3. *Institutionalize secure-by-default teaching environments.* Provide managed lab templates, access controls, segmentation, and logging so that instructor competence can focus on pedagogy rather than ad hoc infrastructure security (NIST, 2024).
4. *Embed inclusion and accessibility as core quality requirements.* Align cybersecurity teaching practice with educator competence frameworks that treat accessibility, learner empowerment, and assessment competence as foundational (Redecker, 2017; UNESCO, 2018).
5. *Create governance routines for procurement, privacy, and incident readiness in learning tools.* Use CSF logic to define approval gates, documentation requirements, monitoring, and incident playbooks for course platforms and AI tools (NIST, 2024).
6. *Treat educator development as continuous professional formation.* Use micro-credential pathways tied to demonstrable teaching artifacts, including lab designs, assessment rubrics, tool risk rationales, and documented improvements over time.

**Conclusion.** Competency gaps in cybersecurity teaching are best understood as an interaction between digital skills, pedagogy, and governance. Workforce and curriculum frameworks provide strong anchors

for aligning learning outcomes with real tasks, but educator readiness requires explicit capability development and institutional support. Governance is not external to teaching because cybersecurity instruction increasingly relies on platforms, third-party services, and AI tools that carry security, privacy, and accountability implications. A role-based competence model, supported by secure teaching infrastructure and auditable governance routines, offers a practical pathway to improve educational quality, inclusion, and institutional resilience.

**Funding.** The author declare that no financial support was received for the research, authorship, and/or publication of this article.

**Conflict of interest.** The author declare that the research 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 declare that no Generative AI was used in the creation of this manuscript.

**Publisher's note.** All claims expressed in this article are solely those of the author 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:**

1. CAST. (2018). *Universal design for learning guidelines version 2.2* [Graphic organizer]. CAST. https://udloncampus.cast.org/wicket/resource/org.cast.cwm.xml.FileXmlDocumentSource/usr/local/tomcat/content/downloads/udlg_graphicorganizer_v2-2_numbers-no.pdf
2. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. (2017). Joint Task Force on Cybersecurity Education. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf
3. ENISA. (2022). *European cybersecurity skills framework: Role profiles*. https://doi.org/10.2824/859537
4. European Union Agency for Cybersecurity. (2022). *European cybersecurity skills framework: Role profiles*. ENISA. https://doi.org/10.2824/859537
5. ISC2. (2024). *ISC2 cybersecurity workforce study 2024*. https://edu.arrow.com/media/wtjfmszx/2024-isc2-wfs.pdf
6. Joint Task Force on Cybersecurity Education. (2017). *Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity* (Version 1.0). Association for Computing Machinery, IEEE Computer Society, AIS SIGSEC, and IFIP WG 11.8. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf
7. National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
8. Office of the National Cyber Director. (2023). *National cyber workforce and education strategy: Unleashing America's cyber talent*. Executive Office of the President. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf
9. Petersen, R., Santos, D., Smith, M., Wetzel, K., & Witte, G. (2020). *Workforce framework for cybersecurity (NICE framework)* (NIST Special Publication 800-181 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181r1
10. Redecker, C. (2017). *European framework for the digital competence of educators: DigCompEdu* (JRC Science for Policy Report). Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC107466/pdf_digcomedu_a4_final.pdf
11. UNESCO. (2018). *UNESCO ICT competency framework for teachers (Version 3)*. https://unesdoc.unesco.org/ark:/48223/pf0000265721