From Classroom to Cyber Front: AI Literacy for National Security Workforces

Від навчальної аудиторії до кіберфронту: грамотність у сфері штучного інтелекту для кадрового потенціалу сектору національної безпеки

Samuel Nnadoziem Ndukuba
Department of ICT, e-mail: sndukuba@rbi.ac.za, ORCID ID: https://orcid.org/0000-0002-4161-213X
The Independent Institute of Education (IIE), Cape Town, South Africa

Семюел Ннадозієм Ндукуба
Кафедра інформаційно-комунікаційних технологій, e-mail: sndukuba@rbi.ac.za, ORCID ID: https://orcid.org/0000-0002-4161-213X
Коледж Роузбенк Незалежного інституту освіти, м. Кейптаун, Південно-Африканська Республіка

Received: August 01, 2026 | Revised: August 25, 2026 | Accepted: August 31, 2026

UDC 378.147:004.8:351.86

DOI: https://doi.org/10.33445/sds.2026.16.4.33

Purpose. To systematically review the literature on the integration of artificial intelligence (AI) into higher education for national security workforce development, with particular attention to developing-country contexts.

Method. Following PRISMA 2020 reporting guidelines, relevant publications from 2019–2026 were selected through structured searches of bibliographic databases, publisher platforms, and institutional repositories. The heterogeneous evidence base, comprising peer-reviewed studies, conference papers, policy documents, and institutional reports, was analysed using narrative thematic synthesis. The findings were organised around the research questions and interpreted through securitization theory and human capital theory.

Findings. The reviewed evidence identifies foundational AI literacy as a prerequisite for developing applied digital competencies and security-specific capabilities. National strategies increasingly assign higher education an important role in AI workforce development. However, the evidence from developing-country contexts indicates persistent constraints, including limited AI-specialised programmes, low faculty adoption outside STEM fields, resource limitations, and institutional fragmentation.

Theoretical implications. The review integrates securitization theory and human capital theory to interpret the gap between the strategic prioritisation of AI-capable security workforces and the educational investment required to develop them. AI-literate workforce capacity is conceptualised as a form of security-relevant human capital rather than as a referent object of securitization.

Originality/value. The study proposes the AI-Ready Security Workforce (ARSW) conceptual readiness framework, comprising four interrelated dimensions: foundational AI literacy, applied digital competencies, domain-specific security integration, and strategic national capacity. The framework is presented as a diagnostic heuristic rather than an empirically validated maturity scale.

Limitations/future research. The evidence base is heterogeneous, cybersecurity education is used as a proxy for broader national security professions, and the developing-country evidence is limited. The ARSW framework has not been empirically validated. Future research should validate the framework across different national and institutional contexts and examine the transition of graduates from AI-integrated curricula into security-sector employment.

Paper type: Review article.

Key words: Artificial Intelligence; Higher Education; National Security; Human Capital Theory; Systematic Literature Review.

Мета дослідження. Систематизувати літературу щодо інтеграції штучного інтелекту (ШІ) у вищу освіту для підготовки кадрів у сфері національної безпеки, зосередившись на країнах, що розвиваються.

Метод дослідження. Відповідно до рекомендацій PRISMA 2020 здійснено структурований пошук публікацій за 2019–2026 роки в бібліографічних базах даних, видавничих платформах та інституційних репозиторіях. Рецензовані дослідження, матеріали конференцій і програмно-політичні документи опрацьовано методом наративно-тематичного синтезу з використанням теорій сек'юритизації та людського капіталу.

Результати. Грамотність у сфері ШІ є передумовою розвитку цифрових компетентностей і спеціалізованих безпекових спроможностей. Заклади вищої освіти відіграють важливу роль у підготовці відповідних кадрів. Водночас країни, що розвиваються, стикаються з нестачею спеціалізованих програм, низьким рівнем застосування ШІ поза STEM-дисциплінами, ресурсними обмеженнями та інституційною фрагментацією.

Теоретична цінність дослідження. Поєднання теорій сек'юритизації та людського капіталу дає змогу пояснити розрив між стратегічною потребою в кадрах, здатних застосовувати ШІ, та освітніми інвестиціями, необхідними для їх підготовки. Такий кадровий потенціал визначено як форму людського капіталу, значущого для національної безпеки.

Оригінальність / цінність дослідження. Запропоновано концептуальну рамку AI-Ready Security Workforce (ARSW), що охоплює базову грамотність у сфері ШІ, прикладні цифрові компетентності, безпекову інтеграцію та стратегічну спроможність держави. Рамка є діагностичним орієнтиром, а не валідованою моделлю зрілості.

Обмеження / подальші дослідження. Доказова база є неоднорідною, а дані щодо країн, що розвиваються, — обмеженими. Кібербезпекову освіту використано як наближену сферу для ширшого контексту національної безпеки. Подальші дослідження мають передбачати емпіричну валідацію ARSW та оцінювання працевлаштування випускників у секторі безпеки.

Тип статті: оглядова стаття.

Ключові слова: штучний інтелект; вища освіта; національна безпека; теорія людського капіталу; систематичний огляд літератури.

Introduction

Artificial Intelligence (AI) is changing the national security workforce in areas like cybersecurity, intelligence analysis, critical infrastructure protection, and defense-adjacent public administration. Governments are starting to view higher education as the primary gateway to this workforce (Mahmood, 2026; Dawson et al., 2026). A comparative analysis of national strategies for artificial intelligence in many countries shows that 95% of them attribute a significant role to higher education institutions in the development of AI talent and workforce (Demaidi, 2025; Dempere et al., 2023; Pedro et al., 2019; UNESCO IESALC, 2024). A growing recognition of the need for AI as a specific competency requirement within security workforce frameworks. Instead, the United States National Institute of Standards and Technology (NIST) has created an AI Security Competency Area within its NICE Workforce Framework for Cybersecurity. This group detailed the foundational knowledge that is necessary for understanding the relationship between AI and cybersecurity (Witko et al., 2023; NIST, 2025; Nizich, 2023).

However, the stakes and constraints of this transformation are different for developing countries. A comparative policy analysis of AI education and workforce strategies in many countries shows that developing countries are facing more resource constraints and institutional fragmentation challenges than developed economies like the USA, Canada, and the UK (Predo et al., 2019; Aderibigbe et al., 2023; Shi, 2025). This is evidenced by the case study from Palestine (where, despite the national AI strategy explicitly identifying education as a priority pillar, only 9% of the country's universities and colleges offer AI-specialised academic programmes (Hamamra et al., 2026; Khlouf, 2025; Demaidi, 2025). This review addresses the conceptualisation and evaluation of higher education systems, especially in developing countries, as sites of national security policy. Three research questions guide the review:

- RQ1: What does the literature report about AI literacy and digital competency development within higher education relevant to national security workforce pipelines?
- RQ2: What structural and resource-related challenges constrain security-relevant AI workforce readiness in developing nations?
- RQ3: How can existing evidence be synthesised into a practical model for assessing and advancing AI-ready security workforce development in developing-nation contexts?

The remainder of the paper proceeds as follows. Section 2 presents the literature review, including theoretical lens and thematic review of evidence. Section 3 details the materials and methods used for the systematic literature review. Section 4 presents the results, including the summary of reviewed literature, synthesis by research question, and the proposed model. Section 5 discusses the findings and their implications. Section 6 presents the conclusions and directions for further study.

Literature Review

This literature review is grounded in two complementary traditions from security studies and the economics of education: securitization theory, which implies how and why an issue such as AI-literate workforce capacity comes to be treated as a matter of national security rather than routine policy, and human capital theory, which implies how education produces the specific kind of workforce capacity that securitized issues then demand. Read together, these theories provide the lens through which the thematic evidence reviewed in this section is interpreted, and they are formalised into an applied model in Section 4.3.

Securitization Theory

Securitization theory, developed by Buzan, Wæver, and de Wilde (1998) within the Copenhagen School of security studies, holds that an issue becomes a security issue not through its objective properties alone but through a discursive process, a "securitizing move", in which a

legitimate actor presents the issue as posing an existential threat to a valued referent object, thereby justifying extraordinary measures beyond normal political procedure. Applied to the domain examined in this review, the securitization framework implies that AI's integration into national security workforce policy should be read as a specific and identifiable securitizing move: national strategies and institutional frameworks such as NICE (Khlouf, 2025; NIST, 2025) and national cyber workforce strategy documents do not merely describe AI as a useful skill but position AI-literate workforce capacity as itself a matter of national security, with the state, critical infrastructure, or citizenry as the referent object placed at risk by its absence.

The above-mentioned theoretical implication has a significant influence on graduates from the higher education system in relation to artificial intelligence. Security is critical, and the absence of AI security within higher education will create unrest and reduce growth; for example, 9 % of AI programs in developing countries do not represent an enhancement of the security infrastructure (Buzan et al., 1998; Hamamra et al., 2026; Demaidi, 2025). This should be considered in education as well as an unsecuritised threat, which has been brought up in the policies but not addressed through the exceptionality approach predicted by the theory.

Human Capital Theory

Where securitization theory implies why AI-literate capacity is treated as a security matter, human capital theory implies how education is expected to produce it. Becker's (1964) foundational formulation treats education and training as investments that increase an individual's stock of skills and knowledge, thereby increasing their future productivity and earnings, with the aggregate effect, at national scale, of increasing a country's productive capacity. Applied here, human capital theory implies that AI-security curricula function as a specific, targeted investment in a specialised form of human capital, one whose value derives not from general productivity but from its direct applicability to security-relevant tasks such as those catalogued in the AI-cybersecurity curriculum literature (Das, 2026; Nazareth, 2025).

The theoretical implication drawn here is that the persistent gaps documented across Sections 2.4 to 2.8- low faculty AI adoption outside STEM (Parviz, 2024), scarce AI-specialised programming (Etemad, 2026), and uneven national prioritisation (Shi, 2025)- represent under-investment in this specific form of human capital relative to the level of securitization theory implies national policy now demands. Read together, the two theories imply a testable proposition: national security policy is securitizing AI-literate workforce capacity faster than higher education systems, particularly in developing nations, can produce the human capital that securitization presupposes already exists or is readily attainable.

Towards an Integrated Theoretical Lens

Combining these two traditions yields the theoretical proposition this review carries into the thematic evidence and subsequently tests against the systematic findings: national AI-security strategies (Predo et al., 2019; Buzan et al., 1998) presuppose a level of AI-literate human capital (Becker, 1964) that current higher education systems, especially in developing nations, have not yet produced, and the gap between the two constitutes an unresolved securitization with direct human-capital-investment implications. Sections 2.4 to 2.8 review the literature relevant to each half of this proposition, Section 4 returns to it explicitly when presenting the findings, and it is formalised as the AI-Ready Security Workforce (ARSW) Maturity Model.

The thematic review is organised into six subheaded themes, moving from foundational AI literacy, through digital competencies and national strategy, to the specific structural constraints developing nations face.

AI Literacy and the Changing Security Landscape

Foundational AI literacy, understanding what AI systems are, how they function, and where their limitations lie, emerges across literature as a prerequisite rather than an advanced competency. From empirical data collected from literacy assessments for students with respect to

their knowledge of AI and cybersecurity, there appears to be a significant shortfall in literacy about such knowledge of students studying courses adjacent to technology security (Chapagain, 2025). There is also a challenge associated with faculty, where curricula integration within developing countries shows that few faculty members have incorporated AI beyond STEM courses (Olatunde-Aiyedun, 2024; Xhako et al., 2025; Nassarawa et al., 2025). Read against human capital theory (Section 2.2), these findings indicate that the foundational investment layer, on which all subsequent, more specialised human-capital formation depends, remains incomplete.

Digital Competencies in Security-Relevant Higher Education

Beyond basic literacy, the literature identifies specific technical competencies required for security-relevant AI applications. A systematic review of AI-cybersecurity curriculum integration identifies three distinct AI technique categories now relevant to security professionals: perception AI, generative AI, and agentic AI, each carrying distinct capability and risk profiles requiring different instructional treatment and finds that current curricula still concentrate disproportionately on perception AI relative to the generative and agentic techniques now shaping real-world threat landscapes (Xhako et al., 2025; Nassarawa et al., 2025). Applied curriculum-design work corroborates this at the module level, developing lecture content that addresses the absence of structured AI resources within existing cybersecurity curricula.

National AI Strategy and Workforce Readiness

National-level evidence shows the securitizing move implied by Section 2.1 is already well underway in policy terms. A U.S. interagency technical report from as early as 2020 explicitly called for AI to be integrated across primary, secondary, and university education and considered as part of formal accreditation processes, treating workforce readiness as a whole-of-education-system responsibility (Kundu & Bej, 2025; NITRD, 2020). This was operationalised in early applied work: an NSF-funded project developed an immersive, multidisciplinary learning environment specifically to build a cybersecurity workforce capable of understanding the usefulness and limitations of AI in security contexts (Maennel & Maennel, 2024; Chourasia, 2025). In 2023, this evolved into a national strategy with the development of the U.S. National Cyber Workforce and Education Strategy, which explicitly takes into consideration AI and machine learning regarding how they affect the cyber workforce skills requirements and the requirement for increased coordination between education and workforce. On an international scale, a comparative policy analysis reveals near-complete recognition of how universities should play a role in training for AI expertise (Ragunathan, 2024; UNESCO IESALC, 2024; Joshi, 2025), although few nations have managed to translate their recognition into concrete strategies, which are primarily the developed nations (Shi, 2025). Institutionally, a suggested multi-dimensional strategy for preparing the cybersecurity workforce involves training, faculty development, and curriculum revision as related readiness strategies and has been adopted by NICE in terms of the AI Security Competency Area (NIST, 2025).

Security Education and Geopolitical Constraints

Security-relevant AI education shows the clearest evidence of geopolitical entanglement of any theme reviewed here, a dimension securitization theory (Section 2.1) helps explain: if AI-literate capacity is itself securitized, control over the international flow of AI-security knowledge becomes a security concern. Conceptual work on cross-border higher education cooperation finds that AI governance approaches now diverge explicitly along national-security lines, with major powers embedding national security considerations directly into research-cooperation and data-governance frameworks, a dynamic with direct implications for developing nations' access to international AI-security research partnerships and training pipelines (Xhako et al., 2025; Nassarawa et al., 2025; Ragunathan, 2024). At the most explicit end of this theme, a 2026 curriculum design case study describes a university-level "SecureAI" concentration built specifically to expand graduate employability across defense, government, and critical-infrastructure sectors, aligning coursework directly with public-sector workforce qualification frameworks (Ragunathan, 2024;

Predo et al., 2019), the clearest example in the reviewed literature of higher education explicitly naming national security workforce development as a curricular design objective.

Developing Nations: Structural Barriers to AI-Security Education

Reading Sections 2.4 to 2.7 through a developing-nations lens surfaces a consistent structural pattern. It has been understood from the case study analysis that the education pillar is a vital one in the AI strategy for Palestine; however, there are no specialized courses for AI in relation to the said strategy (Das, 2026; Ragunathan, 2024; Nazareth, 2025). However, it has been noted through the comparative analysis of the approaches used in the policies of 50 countries that this is a common practice and not an exception that has occurred due to limitations in resources affecting developing countries rather than developed ones (Shi, 2025). In relation to the institutional readiness for AI, it has been observed through the research conducted on developing countries that there is poor adoption of AI technology in the curricula except for STEM subjects because of a lack of training (Ragunathan, 2024). Applied conceptual frameworks proposing multi-dimensional readiness, combining training, faculty development, and curriculum restructuring, offer a partial response, but no source identified in this review tests such a framework specifically within a developing-nation institutional context.

Summary and Research Gap

Read together, Sections 2.4 to 2.8 establish two things clearly and one thing not at all. They establish clearly that national policy, in developed-economy contexts especially, increasingly treats AI-literate security workforce capacity as a securitized priority, formalised through frameworks such as NICE and the national cyber workforce strategy (Section 2.6). They establish equally clearly that developing nations face compounding literacy, competency, and institutional barriers to producing that capacity (Sections 2.4, 2.8). What the literature does not establish, in any source identified in this review, is a validated diagnostic model connecting foundational AI literacy, through applied competency and institutional integration, to the strategic national capacity that securitization theory implies policy is demanding. This is the gap the summary of reviewed literature and results (Section 4) and systematic review (Section 3) are designed to make explicit, and which the discussion in Section 5 addresses.

Materials and Methods

Having reviewed the literature in Section 2, this section details the materials and methods used for the formal systematic literature review (SLR). The review follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) protocol.

Research questions and eligibility criteria

Eligible sources were required to (a) address artificial intelligence, machine learning, or related digital technologies; (b) be situated within higher education curricula, workforce policy, or national strategy relevant to cybersecurity, intelligence, critical-infrastructure, or broader national-security-adjacent professions; (c) be published between 2019 and 2026 in peer-reviewed journals, conference proceedings, institutional policy reports, or reputable preprint repositories; and (d) be published in English. Because dedicated national-security-specific higher education literature is scarce, cybersecurity-education literature was treated as a core proxy domain, consistent with cybersecurity's centrality to national security workforce definitions in frameworks (NIST, 2025). Sources that addressed AI only in general education without a clear connection to workforce development, security, or relevant competencies were excluded from the formal corpus.

Search strategy

Searches were structured across Scopus, Web of Science, IEEE Xplore, and ACM Digital Library, with further targeted searches of publisher platforms and authoritative institutional repositories such as UNESCO IESALC, NIST, NITRD, and the U.S. National Cyber Workforce and Education Strategy. The search concepts combined five groups of terms: (1) AI technologies

("artificial intelligence" OR AI OR "machine learning" OR "generative AI" OR "agentic AI"); (2) higher education ("higher education" OR university OR curriculum OR education); (3) security domains (cybersecurity OR "national security" OR intelligence OR "critical infrastructure"); (4) workforce outcomes ("workforce development" OR competencies OR "digital skills" OR employability); and (5) context ("developing country" OR "developing nation" OR "Global South"). Searches covered the 2019–2026 publication window. The publisher and institutional searches were used to identify relevant policy and technical documents that might not be indexed consistently in bibliographic databases. The core Boolean structure was: ("artificial intelligence" OR AI OR "machine learning" OR "generative AI" OR "agentic AI") AND ("higher education" OR university OR curriculum OR education) AND (cybersecurity OR "national security" OR intelligence OR "critical infrastructure") AND ("workforce development" OR competencies OR "digital skills" OR employability) AND ("developing country" OR "developing nation*" OR "Global South"). Search terms were adapted to the syntax of each database.

Study selection and quality appraisal

Records were screened in two stages: title/abstract screening followed by full-text eligibility assessment. The PRISMA flow diagram reports 198 records identified, 156 records remaining after duplicate removal, 156 records screened, 112 records excluded as off-topic or not sufficiently related to security or education, and 44 full-text sources assessed for eligibility. Thirty full-text sources were excluded because they did not meet the review focus, literacy/competency requirements, or language criterion. 26 sources therefore met all eligibility requirements and formed the final qualitative synthesis. Quality appraisal was undertaken using source-type-appropriate criteria. For empirical, review, and conceptual studies, the appraisal considered clarity of purpose, methodological transparency, appropriateness of the design and evidence, analytical coherence, and consistency between findings and conclusions. For policy and institutional documents, the appraisal considered authority, provenance, transparency, currency, relevance, and potential bias. Appraisal informed the weighing and interpretation of the evidence rather than serving as an automatic exclusion criterion, given the heterogeneity of the corpus. Sources with limited methodological detail were used judiciously, especially for contextual/policy claims. The study-selection process and corresponding record counts are summarised in Table 1.

Table 1: Search Protocol and Study Selection Method

Stage	Selection Method / Procedure	Records (n)
Identification	Records identified through database searches	198
Duplicate removal	Duplicate records removed before screening	42
Screening	Records remaining after duplicating removal and screened by title, abstract, and keywords	156
Screening exclusion	Records excluded because they were off-topic or not sufficiently related to security or education	112
Eligibility	Full-text sources retrieved and assessed against the eligibility criteria	44
Full-text exclusion	Sources excluded because they did not meet the review focus, literacy/competency requirements, or language criteria	30
Inclusion	Sources meeting all eligibility criteria and included in the qualitative synthesis	26

Source: compiled by the author based on the study-selection results.

The eligibility and screening criteria applied in the review are presented in Table 2.

Table2: Study Selection Protocol

Criterion	Selection Protocol
Publication period	Studies published within the predefined review period
Language	English-language publications
Research focus	Studies addressing the relationship between **AI/security and education**, consistent with the review objectives
Population/context	Studies addressing relevant learners, educators, institutions, or security-related educational contexts
Literacy/competency	Studies explicitly address AI literacy, digital literacy, cybersecurity literacy, AI competency, or related competency development
Study relevance	Studies sufficiently aligned with the research questions and conceptual focus
Document type	Peer-reviewed scholarly sources meeting the predefined inclusion criteria
Exclusion	Studies that were off topic, insufficiently related to security or education, failed to address literacy/competency requirements, or did not meet the language criteria
Screening procedure	Title, abstract and keyword screening followed by full-text assessment
Final synthesis	**26 eligible sources** included in the qualitative synthesis
Reporting framework	PRISMA 2020 systematic review reporting framework

Source: compiled by the author based on the eligibility criteria and the PRISMA 2020 reporting framework.

The study-selection process is presented in Figure 1.

Data synthesis

Because the included sources were heterogeneous in design and evidence type, meta-analysis was not appropriate. Narrative thematic synthesis was therefore used. Findings were coded into themes aligned with RQ1–RQ3 and then mapped against the theoretical constructs in Section 2. The synthesis distinguished empirical findings, policy statements, conceptual arguments, and the authors' own theoretical inferences so that these forms of evidence were not treated as equivalent.

Results

Summary of Reviewed Literature

Table 3 summarises, in tabular form, the fourteen sources discussed narratively in Section 2, drawn from a systematic search described in Section 3. The evidence base is necessarily mixed in provenance, reflecting the nascency of this specific research intersection: it combines systematic reviews and empirical studies with authoritative institutional policy sources (UNESCO IESALC, NIST/NICE, NITRD, U.S. national cyber workforce strategy), consistent with the review's aim of establishing a foundational synthesis in an underdeveloped area of the literature.

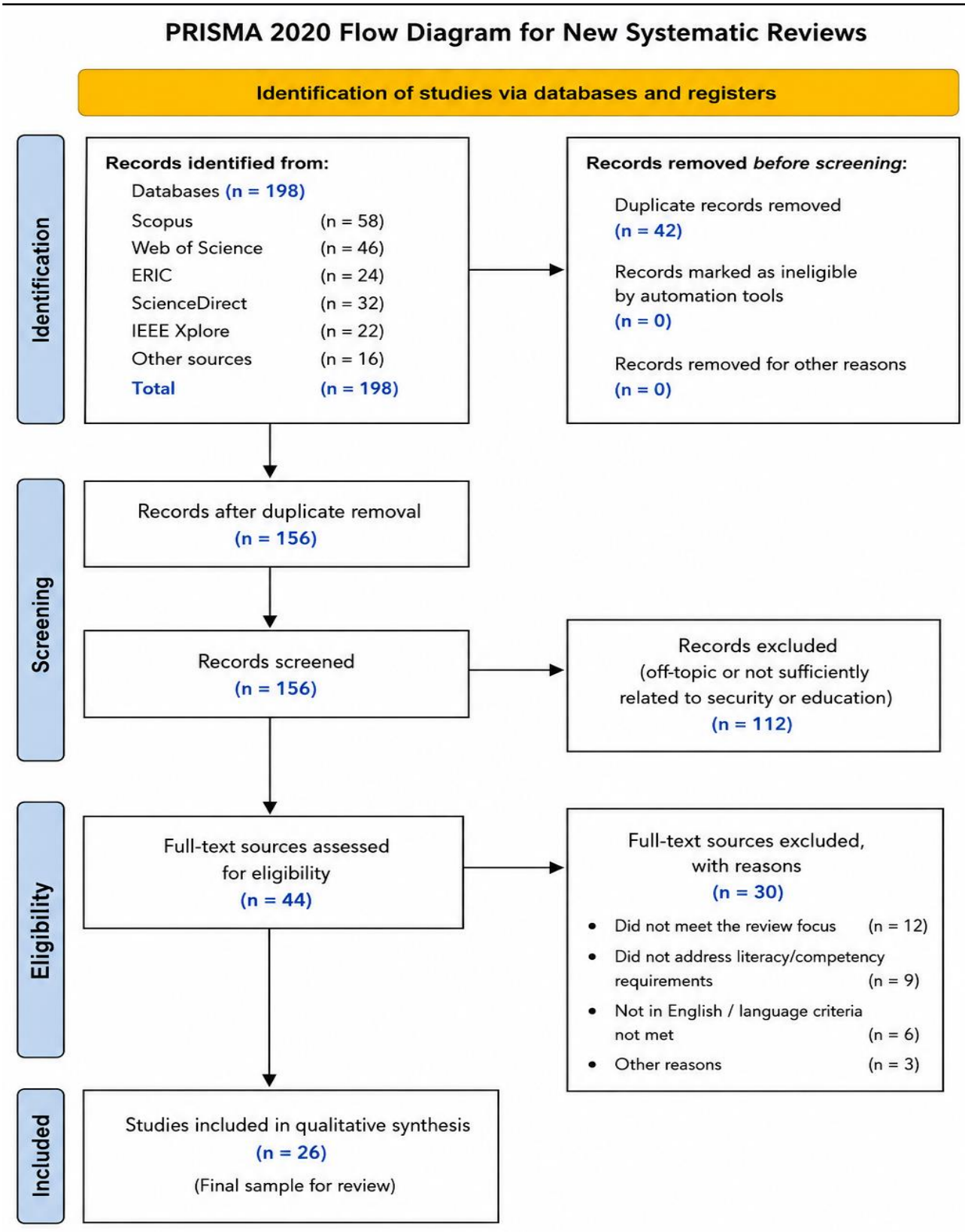

Figure 1: PRISMA flow diagram of the study selection process
Source: adapted by the author from Page et al. (2021).

Table 3: Characteristics of the 28 sources included in this systematic review

Study	Thematic Focus	Method	Key Contribution
UNESCO IESALC (2024)	Higher education's role in national AI strategies	Comparative policy review, multi-country	Finds 95% of countries assign HE the lead role in AI talent and workforce development
NIST/NICE (2025)	AI's impact on the cybersecurity workforce	Institutional framework analysis	Introduces a formal AI Security Competency Area within the national cybersecurity workforce framework
NITRD (2020)	National AI-cybersecurity research and education priorities	U.S. interagency technical report	Recommends AI integration across primary, secondary, and university education as a national priority
Designing SecureAI Curriculum for National Security Needs (2026)	AI-security curriculum for national security workforce	Curriculum design case study	Explicitly builds curriculum around defense, government, and critical-infrastructure workforce needs.
Chapagain (2025)	AI and cybersecurity literacy assessment	Empirical literacy assessment (preprint)	Assesses student AI/cybersecurity literacy levels and learning needs
Mahmood (2026)	Enterprise AI governance and risk intelligence	Conceptual framework and policy analysis	Developed AI governance and risk intelligence models to strengthen national AI leadership and enterprise resilience.
Dawson et al. (2026)	AI and cybersecurity curriculum design	Curriculum design and case study	Proposed a SecureAI curriculum aligned with national security and workforce development needs.
Pedro et al. (2019)	AI in education for sustainable development	Policy review	Identified opportunities and challenges of AI adoption in education and highlighted equitable implementation.
Shi (2025)	National AI competence development strategies	Comparative policy analysis	Compared global AI education strategies and best practices for workforce competence.
Dempere et al. (2023)	National AI policies and higher education	Conceptual analysis	Examined the influence of AI strategies on curriculum reform and governance.
Demaidi (2025)	National AI strategy in developing countries	Policy analysis	Addressed governance, infrastructure, and capacity constraints.
Witko et al. (2025)	AI-assisted cybersecurity competencies	Expert validation	Validated the FCCI using human–GenAI teaming.

Study	Thematic Focus	Method	Key Contribution
Nizich (2023)	Cybersecurity workforce development	Conceptual review	Outlined strategies for preparing future cybersecurity professionals.
Aderibigbe et al. (2023)	AI in developing countries	Literature review	Identified barriers and opportunities for AI adoption.
Hamamra et al. (2026)	AI integration in higher education	Qualitative interviews	Explored educators' experiences with AI integration.
Khlouf (2025)	AI and digital media curriculum	Mixed methods	Recommended AI-focused media curriculum reforms.
Das (2026)	AI across sectors	Conceptual overview	Reviewed cross-sector AI transformation.
Nazareth (2025)	AI adoption and national security	Doctoral research	Linked AI adoption to national security competitiveness.
Etemad (2026)	AI governance frameworks	Framework development	Adapted NIST AI RMF to Canadian regulation.
Parviz (2024)	AI adoption among instructors	Comparative empirical study	Compared STEM and non-STEM AI adoption.
Olatunde-Aiyedun (2024)	AI in science education	Curriculum analysis	Proposed AI integration into Nigerian science curricula.
Xhako et al. (2025)	AI in STEM programmes	Comprehensive review	Identified gaps in STEM AI curriculum integration.
Nassarawa et al. (2025)	Emerging technologies in STEM	Empirical study	Showed AI integration enhances skills acquisition.
Kundu & Bej (2025)	Comparative AI policies	Comparative policy analysis	Compared school AI policies across countries.
Maennel & Maennel (2024)	Human-AI cybersecurity training	Conference study	Explored learning analytics opportunities.
Chourasia (2025)	AI-enhanced cybersecurity training	Conceptual study	Showed that AI analytics improve cybersecurity training.
Ragunathan (2024)	AI skills in cybersecurity	Doctoral research	Investigated drivers of AI skill integration.
Joshi (2025)	AI-enabled military education	Conceptual framework	Proposed reskilling framework for agentic AI era.

Source: compiled by the author based on the sources included in the systematic review.

Table 4 makes explicit, in summary form, the gap already established narratively in Section 2.9. Prior literature has examined national AI strategy, AI-cybersecurity curricula, and developing-nation education constraints as separate concerns; none has combined a security-studies theoretical lens with a diagnostic maturity model for developing-nation contexts specifically.

Table 4: Evidence coding matrix used to clarify the research gap. Coding distinguishes whether a source explicitly examines national AI strategy, AI-security curricula, or a developing-nation diagnostic model.

Prior Source	Examines National AI Strategy?	Examines AI-Security Curricula?	Proposes a Developing-Nation Diagnostic Model?
UNESCO IESALC (2024)	Yes	No	No
Dempere et al. (2023)	Yes	No	No
Shi (2025)	Yes	No	No
Aderibigbe et al. (2023)	No	Yes	No
Nizich (2023)	No	Yes	No
Dawson et al. (2026)	No	Yes	No
This review	Yes	Yes	Yes — conceptual ARSW framework

Source: developed by the author based on UNESCO IESALC (2024), Dempere et al. (2023), Shi (2025), Aderibigbe et al. (2023), Nizich (2023), and Dawson et al. (2026).

Note. Coding criteria: "Yes" indicates that the source explicitly addresses the relevant domain as a substantive focus; "No" indicates that the domain is not a substantive focus. The ARSW framework is classified as a conceptual, non-validated contribution and is not presented as an empirically tested diagnostic model.

Synthesis of Results by Research Question

In response to RQ1, the evidence indicates that AI literacy is best understood as a foundational layer that remains incompletely established among both students and faculty, even before more advanced digital competencies, of the kind catalogued in Section 2.5, can be meaningfully taught. In response to RQ2, structural and resource constraints, institutional fragmentation, low faculty AI adoption outside STEM, scarce AI-specialised programming, and uneven national strategic prioritisation recur consistently across the developing-nation evidence reviewed in Section 2.8, and compound across the literacy, competency, and readiness layers rather than remaining isolated to any single one.

RQ3: Development of a practical readiness model. The theoretical synthesis indicates a potential mismatch between the strategic importance assigned to AI capability in national and security-workforce policies and the institutional capacity required to develop that capability. Securitization theory helps interpret how AI workforce capacity may be framed as strategically important, while human capital theory explains the investment required to develop the knowledge and skills associated with that capacity. The Palestinian case provides an illustrative example of this implementation gap, but it should not be generalised to all developing countries. The resulting insight is therefore a conceptual proposition: workforce readiness can be strengthened by connecting AI literacy, applied competencies, institutional integration, and strategic capacity within a single diagnostic framework. The persistent gaps, most starkly in the Palestinian case where only 9 % of institutions offer AI-specialised programming despite explicit national strategic intent (Ragunathan, 2024; Das, 2026; Nazareth, 2025; Shi, 2025), indicate a securitization not yet met by adequate human-capital investment. This is the review's central analytical insight: national security workforce readiness in developing nations is not simply a curriculum-design problem to be solved locally, but is the observable gap between a securitising policy move and the human-capital investment that move presupposes, a gap this review argues has not previously been named in these explicit theoretical terms.

The AI-Ready Security Workforce (ARSW) Maturity Model

In direct response to RQ3, the review develops the AI-Ready Security Workforce (ARSW) conceptual readiness framework. It synthesises four interrelated dimensions identified in the literature: foundational AI literacy, applied digital competencies, domain-specific security integration, and strategic national capacity. The framework is intended as a diagnostic heuristic for institutions and policymakers, not as an empirically validated maturity scale. The resulting four-level ARSW conceptual framework is presented in Figure 2.

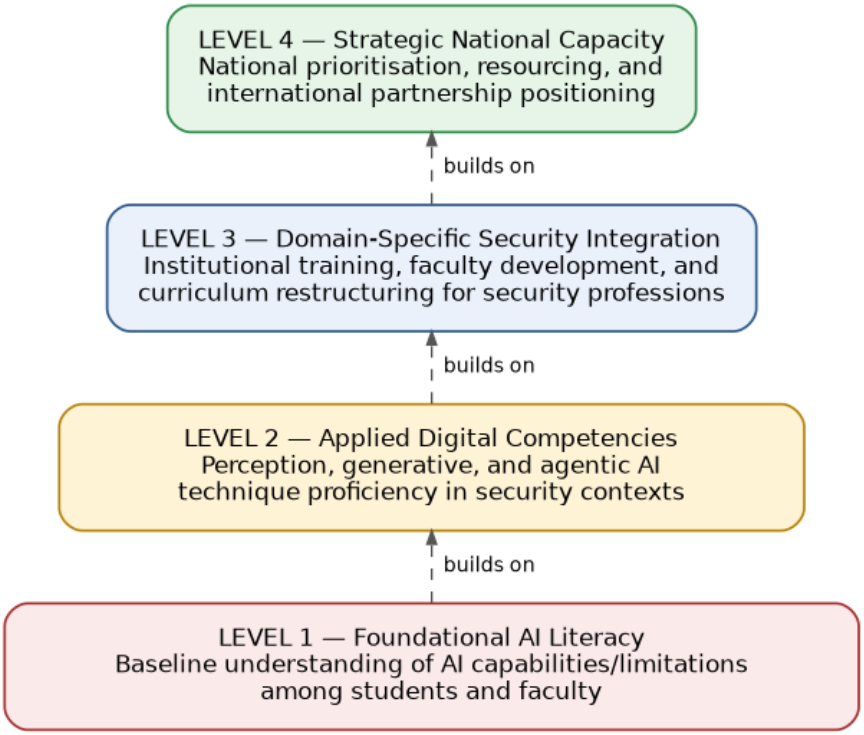

Figure 2: The AI-Ready Security Workforce (ARSW) Maturity Model, showing the four ascending readiness levels synthesised from Sections 2.4–2.7

Source: developed by the author based on the results of the systematic literature review.

Level 1: Foundational AI Literacy is the basic knowledge of the capabilities, limitations, risks, and appropriate use of AI by faculty and students. Level 2: Applied Digital Competencies. Level 2 focuses on the practical skills necessary to use perception, generative, and agentic AI techniques in security contexts. Level 3, Domain-Specific Security Integration, concerns institutional integration through curriculum restructuring, hands-on learning, faculty development, and alignment with relevant workforce competency frameworks such as NICE. Level 4, Strategic National Capacity, concerns national-level prioritisation, resourcing, governance, and international partnerships. These levels should be interpreted as interrelated readiness dimensions rather than as a validated linear scale.

The value of the framework lies in making the relationships among these dimensions explicit. Higher strategic ambition may be difficult to translate into workforce readiness when foundational literacy, applied competencies, and institutional integration remain weak. However, the framework does not establish that institutions must progress through the four levels in a fixed sequence, nor does it claim that Level 4 constitutes a complete securitizing move. These relationships require empirical testing across different institutional and national contexts.

Discussion

This section discusses the findings in relation to the research questions, theoretical framework, and literature reviewed in Section 2 and considers their implications for policy and practice.

Policy and Practice Implications

This synthesis has several practical implications. The ARSW Model should guide the sequencing of investment rather than prioritising visible strategic announcements (Level 4) over foundational literacy and competency building (Levels 1–2) and directly address the mismatch identified in the Palestinian case study. Low faculty adoption outside STEM is a recurring constraint identified in Sections 2.4 and 2.8 (Pedro et al., 2019; Etemad, 2026; Parviz, 2024), and thus targeted investment is justified in the development of faculty AI, not merely student-facing curricula. Institutions would also benefit from using formal competency frameworks like an adapted version of NICE's AI Security Competency Area, which would provide developing nation institutions with a concrete, internationally benchmarked target for Level 3 integration (Etemad, 2026; NIST, 2025).

Given the geopolitical and governance issues discussed in Section 2.7, developing countries may benefit from diversified international partnerships that strengthen local capacity while reducing excessive dependence on the priorities of any single AI-producing country (Shi, 2025; Etemad, 2026; Parviz, 2024). More broadly, policymakers and institutions should invest in faculty development, curriculum renewal, practical AI-security learning environments, and competency-based assessment. Because the reviewed corpus did not provide robust evidence linking AI-integrated higher education curricula to measured national-security workforce outcomes in developing-country contexts, future research should test these relationships empirically rather than assuming them.

Conclusions

Artificial intelligence is increasingly shaping national-security workforce requirements, particularly in cybersecurity, while higher education is widely positioned as an important pipeline for developing relevant skills. This systematic review finds evidence of a persistent implementation gap between the strategic importance assigned to AI capability and the capacity of higher education institutions to provide AI literacy, applied competencies, and security-relevant training. Viewed through securitization theory and human capital theory, the gap can be interpreted as a tension between policy prioritisation and the investment required to develop specialised human capital. Based on the reviewed corpus, the study develops the ARSW conceptual readiness framework to integrate these fragmented dimensions. The framework is a conceptual contribution and requires empirical validation before it can be used as a formal maturity or assessment instrument.

The review has several limitations. First, the formal corpus contains only fourteen sources, reflecting the limited number of studies located at the specific intersection of AI, higher education, and national-security workforce development. Second, because dedicated national-security higher-education literature is scarce, cybersecurity education was used as a core proxy domain; therefore, conclusions concerning intelligence analysis, defence administration, and other security professions should be treated as inferential. Third, the corpus combines peer-reviewed research with institutional and policy documents, creating heterogeneity in evidentiary strength. 26 sources, securitization theory and human capital theory predate generative and agentic AI and are therefore applied here by theoretical extension. Finally, the ARSW framework is conceptual and has not been empirically validated; it should not be interpreted as a tested maturity scale or assessment instrument.

Recommendations and Further Research

Based on the findings and limitations of this review, institutions and policymakers should prioritise faculty AI development, curriculum renewal, practical AI-security learning environments, and competency-based assessment. Future research should also prioritise empirical studies that

directly link AI-integrated higher education curricula to measurable national-security workforce outcomes in developing-country contexts, an intersection that remains underexplored relative to its practical importance.

A second priority is the development and validation of a formal ARSW assessment instrument, allowing institutions and national policymakers to score their current position across the four levels proposed in Section 4.3 and to identify specifically where Level 1–2 investment gaps exist relative to Level 4 strategic ambition, operationalising the diagnostic function the model is currently able to offer only conceptually.

Third, comparative research applying securitization theory (Section 2.1) across multiple developing-nation contexts beyond the single Palestinian case reviewed here (Section 2.8) would help establish whether the securitization-without-investment pattern identified in this review is a general feature of developing-nation AI-security policy or specific to particular political or resource contexts. Such research would ideally combine document analysis of national AI and cybersecurity strategies with institutional-level data on AI-specialised programme availability, replicating and extending the approach used in the Palestinian case study at a multi-country scale.

Finally, given the rapid evolution of generative and agentic AI capabilities documented in Section 2.5, future conceptual work should examine whether the ARSW Model's four levels remain stable over time or require periodic revision as the specific technical competencies constituting Level 2 change faster than institutional curricula, of the kind reviewed in Section 2.5 and 2.7, can typically be redesigned and accredited.

Funding

This study received no specific financial support.

Competing interests

The authors declare that they have no competing interests.

Use of Artificial Intelligence

Artificial intelligence was used for language editing, translation, and technical verification of the manuscript.

References

Aderibigbe, A. O., Ohenhen, P. E., Nwaobia, N. K., Gidiagba, J. O., & Ani, E. C. (2023). Artificial intelligence in developing countries: Bridging the gap between potential and implementation. Computer Science & IT Research Journal, 4(3), 185–199. https://doi.org/10.51594/csitrj.v4i3.629

Becker, G. S. (1964). Human capital: A theoretical and empirical analysis, with special reference to education. Columbia University Press for the National Bureau of Economic Research. https://www.nber.org/books-and-chapters/human-capital-theoretical-and-empirical-analysis-special-reference-education-first-edition

Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.

Chapagain, D. (2025). AISCliteracy: Assessing artificial intelligence and cybersecurity literacy levels and learning needs of students [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2506.23321

Chourasia, R. (2025). AI-enhanced cybersecurity training: Learning analytics in action. International Journal of Advanced Research in Science, Communication and Technology, 5(2), 566–573. https://doi.org/10.48175/IJARSCT-23066

Das, S. S. (2026). Artificial intelligence across sectors.

Dawson, M., Ayed, A. B., Quaye, S., & Khan, A. H. (2026). Designing SecureAI curriculum for national security needs: The Illinois Tech program of study. Education Sciences, 16(2), 310. https://doi.org/10.3390/educsci16020310

Demaidi, M. N. (2025). Artificial intelligence national strategy in a developing country. AI & Society, 40(2), 423–435. https://doi.org/10.1007/s00146-023-01779-x

Dempere, J. M., Flores, P., & Allam, H. (2023). The challenges posed by national artificial intelligence strategies and policies on higher education institutions. In Proceedings of the HCT International General Education Conference (HCT-IGEC 2023) (pp. 185–200). Atlantis Press. https://doi.org/10.2991/978-94-6463-286-6_15

Etemad, M. (2026). SCITUS: A multi-jurisdictional framework for adapting NIST AI RMF to the Canadian regulatory context [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2607.15051

Hamamra, B., Khlaif, Z. N., & Mayaleh, A. (2026). Between promise and precarity: Palestinian university educators' experiences with AI integration in higher education. Interactive Learning Environments, 34(4), 2574–2589. https://doi.org/10.1080/10494820.2025.2547264

Joshi, S. (2025). Transforming US military education for the agentic AI era: A national framework for reskilling and workforce development [Preprint]. https://doi.org/10.20944/preprints202510.1034.v1

Khlouf, M. M. M. (2025). Reforming media curricula in Palestinian universities for AI and digital culture: Student and expert perspectives. Frontiers in Education, 10, 1678732. https://doi.org/10.3389/feduc.2025.1678732

Kundu, A., & Bej, T. (2025). AI policies in school education: A comparative study on China, Singapore, Finland, and the US. Journal of Science and Technology Policy Management. https://doi.org/10.1108/JSTPM-06-2024-0218

Maennel, K., & Maennel, O. M. (2024). Human-AI collaboration and cyber security training: Learning analytics opportunities and challenges. In 2024 17th International Conference on Security of Information and Networks (SIN) (pp. 1–8). IEEE. https://doi.org/10.1109/SIN63213.2024.10871610

Mahmood, H. (2026). Advancing United States leadership in artificial intelligence through enterprise AI governance and risk intelligence models. American Journal of Data Science and Analytics, 7(3), 1–44. https://doi.org/10.63125/2wedv223

Nassarawa, H. S., Bashir, I., Aminu, E. H., Muhammad, A., & Kangiwa, B. I. (2025). Integrating emerging technologies into science, technology, engineering, and mathematics (STEM) curriculum for enhanced skills acquisition in Kano State science and technical schools. Science Journal of Education, 13(6), 206–212. https://doi.org/10.11648/j.sjedu.20251306.14

National Institute of Standards and Technology [NIST]. (2025). The impact of artificial intelligence on the cybersecurity workforce. https://www.nist.gov/blogs/cybersecurity-insights/impact-artificial-intelligence-cybersecurity-workforce

National Science and Technology Council, Networking and Information Technology Research and Development Subcommittee [NITRD]. (2020). Artificial intelligence and cybersecurity: Opportunities and challenges. https://www.nitrd.gov/pubs/AI-CS-Tech-Summary-2020.pdf

Nazareth, C. (2025). Adoption of artificial intelligence by US firms: Implications for national security [Doctoral dissertation, Southern University and Agricultural and Mechanical College].

Nizich, M. (2023). Preparing the cybersecurity workforce of tomorrow. In The cybersecurity workforce of tomorrow (pp. 117–146). Emerald Group Publishing. https://doi.org/10.1108/978-1-80382-915-920231009

Olatunde-Aiyedun, T. G. (2024). Artificial intelligence (AI) in education: Integration of AI into science education curriculum in Nigerian universities. International Journal of Artificial Intelligence for Digital Marketing, 1(1), 1–14. https://doi.org/10.61796/ijaifd.v1i1.13

Page, M. J., McKenzie, J. E., Bossuyt, P. M., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Parviz, M. (2024). AI in education: Comparative perspectives from STEM and non-STEM instructors. Computers and Education Open, 6, 100190. https://doi.org/10.1016/j.caeo.2024.100190

Pedro, F., Subosa, M., Rivas, A., & Valverde, P. (2019). Artificial intelligence in education: Challenges and opportunities for sustainable development. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000366994

Ragunathan, R. (2024). To explore and understand the factors influencing the addition of artificial intelligence (AI) skills to the US cybersecurity workforce [Doctoral dissertation, Capitol Technology University].

Shi, L. (2025). Global perspectives on AI competence development: Analyzing national AI strategies in education and workforce policies. Human Resource Development Review, 24(4), 447–476. https://doi.org/10.1177/15344843251332360

The White House. (2023). National cyber workforce and education strategy. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf

UNESCO IESALC. (2024). The role of higher education in national artificial intelligence strategies: A comparative policy review. https://www.iesalc.unesco.org/en/articles/role-higher-education-national-artificial-intelligence-strategies-comparative-policy-review

Witko, D., Levy, Y., Neubauer, C., Simco, G., Dringus, L. P., & Carlton, M. (2025). Experts' validation of the fundamental cybersecurity competency index (FCCI) using a commercial cyber range through human-generative artificial intelligence (GenAI) teaming. Journal of Cybersecurity Education, Research and Practice, 2025(1), Article 22. https://doi.org/10.62915/2472-2707.1274

Xhako, D., Hyka, N., Gjevori, A., Muda, V., Duro, C., Demirneli, M., Spahiu, E., & Hoxhaj, S. (2025). The level of AI application in university STEM study programs: A comprehensive review. International Journal of Innovative Technology and Interdisciplinary Sciences, 8(4), 1244–1283. https://doi.org/10.15157/ijitis.2025.8.4.1244-1283