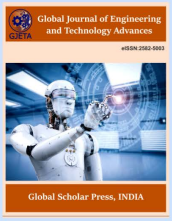
Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/



(REVIEW ARTICLE)

Check for updates

CYBERSECURITY READINESS FOR ARTIFICIAL INTELLIGENCE: A COMPARATIVE ANALYSIS OF NATIONAL AI POLICIES AND CYBERSECURITY EDUCATION

Ifeyinwa Nkemdilim Obiokafor [1,*] and Michael Ebere Ajonuma [2]

[1] Department of Computing Sciences, Cybersecurity Programme, Admiralty University of Nigeria.
[2] Department of Computer Science, Federal Cooperative College, Oji, Nigeria.
* Corresponding Author

ORCID Details
Ifeyinwa Nkemdilim Obiokafor: https://orcid.org/0000-0002-8013-461X
Michael Ebere Ajonuma: https://orcid.org/0009-0007-4624-187X

Global Journal of Engineering and Technology Advances, 2026, 29(01), 341–350

Publication history: Received on 05 September 2026; revised on 11 October 2026; accepted on 13 October 2026

Article DOI: https://doi.org/10.30574/gjeta.2026.29.1.0291

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

The coverage of cybersecurity readiness for AI is uneven and under-theorised across countries, as they compete and develop their own national capacity-building strategies for AI. The paper provides a comparative policy review of AI policies and cybersecurity education programs in six jurisdictions, United States, EU, United Kingdom, Singapore, India, and Nigeria (in West Africa and African Union context). The review utilizes thematic synthesis to compare governance models, targets for the cybersecurity workforce pipeline and translation mechanisms for curricula, across thirty peer-reviewed and grey literature sources, such as national strategy documents, agency frameworks like ENISA, the NIST NICE Framework, and the Nigeria National Information Technology Development Agency (NITDA), as well as systematic reviews of curricula in cybersecurity. In every national AI strategy, cybersecurity is a national priority, but it is seldom defined in terms of competencies, and when it is, it is rarely addressed in terms of instruction, evaluation or certification. The centralised systems, like Singapore, are characterised by a stronger coupling of strategy to curriculum, while the federated or co-regulatory systems, like the United States and the European Union, exhibit weaker coupling, and Nigeria exemplifies a third model, where there are a highly ambitious curricular timeframe set in a central manner, but significant capacity constraints to support the workforce and a less unified regional legal framework. There is limited capacity for assessing educational interventions in each of the jurisdictions studied. The paper recommends a crosswalk between national AI policies and cybersecurity education competency frameworks, as well as priority areas for future research and policy design, such as cross-border harmonisation, including at the regional level in Africa, in particular the African Union, equity-oriented implementation, and longitudinal outcome evaluations.

Keywords: National AI Policy; Cybersecurity Education; Comparative Governance; PRISMA comparative Review; Workforce Readiness; Curriculum Policy

1 INTRODUCTION

AI is transforming the offensive and defensive sides of cybersecurity. As attackers gain new capabilities through AI-powered tools to reduce technical hurdles, defenders now also have the ability to respond to threats at machine speed and perform detection and triage at a speed that industry observers say would have once taken years. In this context, over 60 countries and regions have released AI strategies since 2017, with an increasing number making cybersecurity capacity a prerequisite for safe use of AI technologies, and therefore cybersecurity education (Airlie et al. 2026; Radu, 2025). However, a persistent lack of workers, estimated to be about 600,000 in the United States alone, shows that strategic intent has not translated into an educated talent pool of practitioners ready to secure AI systems or secure other systems using AI.

The gap between the aims of AI policy and cybersecurity education capacity is the issue this paper tackles. Current scholarship focuses on either the national AI policy (technology and industrial policy) or on cybersecurity education (curriculum and workforce development), with few comparative studies that seek to connect the two issues and ask how national-level instruments of AI policy are shaping, financing, or ignoring cybersecurity education readiness (Cyber Security Agency of Singapore, 2024; Obiokafor, 2026; Tahereh, & Tayebeh, 2023) which is largely limited to high-income and OECD-inspired settings. This review focuses on these two gaps, comparing six jurisdictions that vary in their governance approaches and resource contexts: the federated, whole-of-society model of the United States; the supranational co-regulatory model of the European Union; the centrally strategised but devolved-implementation model of the United Kingdom; the tightly coordinated, centralised model of Singapore; the large-scale, equity-oriented federal model of India; and the 2024 National AI Strategy and NITDA-led cybersecurity architecture in Nigeria, where the digital economy is the largest in West Africa and capacity is constrained in a regionally embedded way.

The review is organised around three research questions. First, what is the status of cybersecurity education as a part of AI readiness in the national policies? Secondly, how is AI policy and cybersecurity education coordinated among the selected jurisdictions through governance models and institutional arrangements? Third, what are the thematic discussions and gaps in the existing literature regarding the national approaches?

2 LITERATURE REVIEW

The literature is organized thematically rather than chronologically or by jurisdiction, which is consistent with best practices for comparative policy evaluations using a variety of document forms.

2.1 Global Cybersecurity Governance Architectures

The ENISA framework on national cybersecurity strategy governance provides a structural blueprint, including high-level principles, sectoral goals and responsibilities, that numerous Member States adopt in developing their own cybersecurity strategies, while making explicit the aspect of capacity development, training, and awareness-raising as one of four structural elements, (Crawford, & Ji, 2023), along with strategic governance, operational coordination, and stakeholder engagement. The NICE Framework developed by the National Institute of Standards and Technology (NIST) serves as a de facto standard in the United States, according to which cybersecurity education programs and positions are mapped, and there have been legislative proposals regarding the extension of such a framework to AI positions by NIST (Petersen et al., 2020). Savas and Karatas (2022) reviewed the cybersecurity governance literature describes the discipline as being fragmented into legal, technical, and managerial approaches, with few papers bridging the gap between governance theory and education policy, fragmentation that is inherent to this review too and which this paper aims to alleviate somewhat through the narrow focus on the intersection of AI and cybersecurity education.

2.2 National AI Strategies and Their Cybersecurity Education Provisions

The level of explicitness with respect to cybersecurity education differs across national AI strategies, as revealed by comparative descriptive analysis. The National Cyber Workforce and Education Strategy, from the Office of the National Cyber Director, takes a four-pillar, whole-of-society strategy; it builds on the notion of a cyber education program in which every American is provided with basic skills, while simultaneously transforming cyber education, developing the national cyber workforce, and strengthening the federal cyber workforce; it clearly favours localised cyber ecosystems over a single prescribed curriculum (Kifaru, 2025). Even well-resourced governance systems consider AI and cyber to be adjacent and not treated as one by default, and this is reflected in industry submissions to the ONCD, including from CrowdStrike, (2023), which have called for greater convergence between the upcoming national AI governance framework and the cyber workforce governance framework.

The European Union's strategy adds the binding AI Act to an already existing cybersecurity skills architecture: the European Cybersecurity Skills Framework by ENISA (2022), offers a common competency taxonomy, and the Cybersecurity Skills Academy 2023 pledges itself to creating specific training modules for AI in cybersecurity while

updating the ECSF with competencies related to AI. One follow-up EU Action Plan on Cybersecurity and Artificial Intelligence provides capacity-building tools such as a “Grand Challenge” to encourage the deployment of AI-based cybersecurity solutions and facilitated access to the AI Factory computing resources, which are more industry-leaning with obvious workforce-development implications. ENISA's position paper on cybersecurity in the frontier AI era makes the same point: The time from vulnerability to exploitation is narrowing and calls for an urgent change in the skills of the defenders; again, this is not an educational-outcomes research paper, but rather is based on consultation with stakeholders.

As to education, the National AI strategy of the United Kingdom (2021), sees the provision of AI skills in schools as a policy priority, which is implemented in England through the policy paper on generative AI in education published by the Department for Education (2023) education policy is devolved, and Wales and Scotland are autonomous in the way curricula are implemented, which is why this guidance applies only to schools in England, with Wales and Scotland having the autonomy to decide on the curricula to be offered. Additionally, the UK has emerged as a leader in coordinating cybersecurity workforces across borders, serving as a convenor for the International Coalition on Cybersecurity Workforces, established in 2024.

Singapore is an example of a tightly coupled model. In December 2023, it released its National AI Strategy 2.0, which explicitly lists education as one of its transformation areas and explicitly targets a number,15,000 AI practitioners by 2027, which directly connects to the SkillsFuture reskilling programme and the Ministry of Education's EdTech Masterplan 2030. For the security side, the Cyber Security Agency of Singapore’s (CSA) 2024 Operational Technology Cybersecurity Masterplan and the new generative-AI governance framework bring a continuum of this coordination to the critical-infrastructure sector workforce capacity, with Singapore also collaborating with the University of Oxford’s Global Cyber Security Capacity Centre (2026) to pilot an AI Cybersecurity Readiness Metric aimed at benchmarking national capacity in critical-infrastructure and digital-economy dimensions.

Even while the India’s National Education Policy (2020) and the National Digital Education Architecture make AI the driver behind curricular modernisation and establish an ambitious Gross enrollment target for higher education, comparative analysis shows that while the competency detail for AI-literacy or vernacular-access is quite comprehensive, that of cybersecurity is very limited. This reflects the scale and resource-heterogeneity problems of implementing a single framework for a federal state with a distinct regional disparity.

Nigeria is an example of a sixth configuration. In August 2024, the Nigerian Federal Ministry of Communications, Innovation, and Digital Economy launched the Nigerian National Artificial Intelligence Strategy, together with the Nigerian AI Strategy and Policy Framework in regard to ethics, bias, data privacy, and cybersecurity, partly supported financially by international organizations such as the Google grant on AI talent development program in 2024. In cybersecurity sphere, the NITDA proposed a four pillar approach: Governance (using the Cybercrime Act and Presidential decree on making the critical digital infrastructure into national assets), Capacity Building (3 Million Tech Talent, National Digital Literacy Framework aiming at achieving 95 percent digital literacy by 2030), Incident Management (National Cybersecurity Coordination Centre within the Office of the National Security Adviser and sectorial CERTs), and Collaboration (with the African Union, Smart Africa, and worldwide CERTs network). Beginning in 2026, digital literacy, as well as cyber security education, will be mandated in all educational levels, from kindergarten through tertiary education, and on paper, is more broadly and explicitly stated throughout the entire education pipeline than in several higher-income comparators (Gorsky, 2026). AI-related workforce information from $(ISC)^2$, quoted in a 2026 study on AI and African Cybersecurity, shows that despite Nigeria being the largest economy in Africa and Africa’s most populous country, the country has approximately 8,352 cybersecurity professionals, compared to 482,985 in the United States. The national efforts also operate in a weak regional legal framework, as the African Union's Malabo Convention on Cyber Security and Personal Data Protection, which was adopted in 2014, has not yet been ratified by all the 54 AU member states and a regional AI strategy is being developed, which will aim to improve the continent's legal framework on AI. This is different from what one finds in Singapore, which is also very ambitious, has less of a workforce-capacity deficit, and is tightly coupled on the regional harmonisation layer, and from the supranational-plus-Member-State combination in the European Union.

2.3 Cybersecurity Curriculum and Competency Frameworks

A specific literature has been written on the topic of cybersecurity skills being converted into an education curriculum outside the scope of national AI policy frameworks. In one study, Hajny et al. (2021) have suggested a framework of tools and best practices for cybersecurity curriculums which can enable institutions to use competency frameworks like ECSF and NICE and convert them into actual course designs (Ahmed, et. al. 2024). In another study, Alnajim et. al. (2023) reviewed the training methods which range from traditional to virtual reality or augmented reality and found out that immersive approaches increase engagement but still lack evaluation on the basis of effectiveness.

2.4 The Dual Role of AI Within Cybersecurity Education

The third thread involves an investigation of AI not as a backdrop to governance but as a topic and tool for pedagogy and operations (Obiokafor & Mbonu, 2026). Tian (2025) comparative literature review of the incorporation of AI in higher-education cyber security courses analyzes competency frameworks, lab settings, and interdisciplinary integration approaches and concludes that the adoption of AI-based curriculum by institutions happens faster than the creation of tools for assessing competence created by such curricula. Nott (2025) reviewed systematically the organisational readiness to adapt to the use of generative AI in cyber security, which includes twenty-five papers written between 2022 and 2025, argues that those organisations with more developed security infrastructures, especially those from the spheres of finance and critical infrastructure, show greater readiness for adapting to the AI due to effective governance, establishment of AI teams and investments in human capital, which means the need for different approaches to the preparation of graduates for AI-based cyber jobs in differently equipped education systems. The 2026 executive and policy briefing of the ATARC Cybersecurity Education and Workforce Development Working Group considers AI and cybersecurity as converging into one single operational approach, which current educational systems cannot address due to their outdated structure.

2.5 Evidence Quality and Assessment Gaps in Cybersecurity Education Research

Finally, another strand critically analyzes the evidence supporting cybersecurity education. A PRISMA-based comparative review of 412 cybersecurity education intervention studies published in the Journal of Cybersecurity Education, Research and Practice revealed that 45.4 percent did not identify any learning outcomes to be assessed, that 5.8 percent of intervention studies assessed used an assessment instrument, and that 22.5 percent of any intervention studies that were assessed made some of their artefacts publicly available for reuse, and that there was no statistically significant growth of assessment rigour from 2015 to 2025. A PRISMA review of online cybersecurity course design from 2010 to 2024, which is a systematic review of existing practices, revealed that the online cybersecurity course design literature was focused on project-based and practical tasks with limited use of validated assessment tools, while both critical reviews of cybersecurity education in the United States by Crabb et. al. (2024), and cybersecurity leaders by Anderson et. al. (2024), concluded that there is a lack of outcome-specific evidence compared to the amount of pedagogical review. Taken together, this strand indicates that although there are instances in which national policies on AI and cybersecurity have generated curricular activity, the current assessment systems for AI are not robust enough to ensure that the activity translates into the competencies outlined in the policy documents.

3 METHODOLOGY

This review adopts a PRISMA-informed method with modifications that are appropriate for the comparative governance subject, combining peer-reviewed academic literature and policy/agency grey literature, which is a mixed corpus of sources that is typical of comparative research in cybersecurity and education policy fields where primary literature (national strategy, agency framework documents) is just as essential to the knowledge base as academic journal articles. The review follows the four PRISMA 2020 stages: identification, screening, eligibility, and inclusion, alongside extending standard database search to policy repositories, consistent with recognised PRISMA-based protocols for AI-and-education reviews.

3.1 Search Strategy

The search included academic databases (Scopus, IEEE Xplore, ERIC) along with policy and government repositories (ENISA, Office of the National Cyber Director, NIST, OECD.AI Policy Observatory, ministry websites for the United States, the European Union, the United Kingdom, Singapore, India, and for the sixth country, Nigeria Federal Ministry of Communications, Innovation and Digital Economy, the African Union, and continental/West Africa-based repositories including the Malabo Convention and Continental AI Strategy). Searches were conducted using a set of terms related to AI policies (“national AI strategy”, “AI policy”, “AI governance”) in conjunction with a separate set of terms related to cybersecurity education (“cybersecurity education”, “cyber workforce”, “cybersecurity curriculum”, “cybersecurity readiness”) with the use of AND Boolean logic separately for each jurisdiction as well as an additional specific West Africa/Nigeria search set (“Nigeria” OR “West Africa” OR “ECOWAS” OR “Malabo Convention”) AND (“AI strategy” OR “cybersecurity education”).

3.2 Inclusion and Exclusion Criteria

The inclusion criteria for this study include the following: the document had to be written in English, address any national or supranational cybersecurity or artificial intelligence governance initiative or a comparative/critical review of cybersecurity education, and must have been published or last updated in the period between 2020 and 2026. The exclusion criteria included marketing documents from vendors that had no underlying primary literature; opinion papers with no evidence base; and cybersecurity research papers that contained no aspect of education or workforce policies.

3.3 Selection Strategy and PRISMA Flow

The selection and screening procedure is shown in Table 1 below. The final set contained thirty-five (35) sources: Eighteen (18) peer-reviewed or preprint systematic/critical reviews and seventeen (17) primary policy/agency/regional governance measures, covering all six comparator jurisdictions, including the Nigeria/West Africa example.

Table 1: PRISMA-informed identification and screening flow.

PRISMA Stage	n	Notes
Records identified through database and repository searching (Scopus, IEEE Xplore, ERIC, government/agency repositories: ENISA, ONCD, NIST, OECD.AI, national ministries, NITDA, African Union)	94	2020–2026 window; keyword strings combining AI-policy and cybersecurity-education terms, including a dedicated Nigeria/West Africa/Malabo Convention string
Duplicates removed	19	Cross-listed policy, media, and academic records
Records screened (title/abstract)	75	—
Records excluded at screening	29	Vendor marketing without primary sourcing; non-education cybersecurity technical papers; opinion pieces without evidentiary basis
Full-text reports assessed for eligibility	46	—
Reports excluded, with reasons	11	No national/supranational/regional governance instrument (n=5); language/access barriers (n=2); duplicate coverage of same instrument (n=4)
Studies and documents included in synthesis	35	18 peer-reviewed/preprint reviews; 17 primary policy, agency, or regional-governance instruments

3.4 Case selection

The included sources have been analyzed using an inductive coding process to identify the five thematic areas discussed in Section 2 above in accordance with the thematic synthesis approach, whereby descriptive codes such as “target of the workforce”, “competency framework”, “assessment tool” were grouped to form analytical themes after several iterations of comparative analyses among jurisdictions. Case selection for comparative analysis employed a “most different systems” approach whereby the jurisdictions selected were based on their variations on the degree of centralization of governance, membership of regional blocs, and levels of resources or capacity, with Nigeria included to include variation on resource constraints and regional rather than supranational harmonization of law.

3.5 Limitations

This review does not purport to cover the databases exhaustively as would be done in a clinical PRISMA review; policy documents develop quicker than research papers, and grey literature searches will always have less reproducibility than database searches. The comparative six jurisdiction approach, although intended to create variation, still will not encompass all the different ways through which countries can deal with the issue, and the selection will continue to be biased in favor of English language and OECD related sources. The Nigerian case study, however, serves to balance out this bias but is largely based on the information from agency communications, ministerial press releases, and newspaper reports, owing to the paucity of the literature on the subject in West Africa at the time of conducting the review.

4 FINDINGS

Table 2 below is an overview of the policy framework for the six regions based on four criteria: the AI policy instrument(s) employed, the cybersecurity education component inherent or implied therein, the key governance body and the overall governance structure.

Table 2: Comparative overview of national AI policy and cybersecurity education governance.

Jurisdiction	Core AI Policy Instrument(s)	Cybersecurity Education Provision	Lead Governance Body	Governance Model
United States	National AI Initiative; National Cyber Workforce and Education Strategy (NCWES, 2023)	Four-pillar strategy: public cyber skills, K-12/higher-ed transformation, national workforce, federal workforce; NICE Framework competency baseline	Office of the National Cyber Director (ONCD); NIST	Federated, whole-of-society; non-prescriptive
European Union	EU AI Act (2024); Cybersecurity Skills Academy (2023); European Cybersecurity Skills Framework (ECSF, 2022) ENISA (2023a)	ECSF role-based competency profiles updated for AI; dedicated AI-in-cybersecurity training modules under the Skills Academy	European Commission; ENISA	Supranational co-regulatory; Member-State implementation
United Kingdom	National AI Strategy (2021); DfE policy paper on Generative AI in Education (2023)	AI literacy guidance for schools; devolved authority means Wales/Scotland set separate curricula	Department for Science, Innovation and Technology (DSIT); Department for Education (DfE)	Centralised strategy, devolved implementation
Singapore	National AI Strategy 2.0 (2023); Smart Nation 2.0; OT Cybersecurity Masterplan (2024)	SkillsFuture reskilling pipelines; EdTech Masterplan 2030; target of 15,000 AI practitioners by 2027	AI Singapore (AISG); Cyber Security Agency (CSA); Ministry of Education (MOE)	Centralised, tightly coordinated whole-of-government
India	National Education Policy (NEP, 2020); National Digital Education Architecture (NDEAR)	AI positioned as cross-curricular catalyst; vernacular-access and inclusion emphasis; limited cybersecurity-specific competency detail	Ministry of Education; Ministry of Electronics and Information Technology (MeitY)	Decentralised federal; equity-oriented, capacity-constrained
Nigeria (West Africa)	National AI Strategy (2024); Nigerian AI Strategy and Policy Framework (NITDA) (2025); regionally anchored by the AU Malabo Convention (2014/2023) and the AU Continental AI Strategy.	Four-pillar cybersecurity strategy (governance, capacity building, incident management, collaboration); 3 Million Tech Talent (3MTT) programme; National Digital Literacy Framework (95% target by 2030); digital literacy and cybersecurity curriculum mandated kindergarten-to-tertiary from 2026	National Information Technology Development Agency (NITDA); Office of the National Security Adviser (ONSA)/National Cybersecurity Coordination Centre; Federal Ministry of Communications, Innovation and Digital Economy	Centralised national strategy nested in a fragmented regional (ECOWAS/AU) architecture; donor- and partner-dependent capacity building

4.1 Cybersecurity Is Named as a Priority but Rarely Operationalised

Each of the jurisdictions in the corpus prioritises cybersecurity, cyber skills, or cyber resilience in the context of their respective AI policy frameworks. The difference is that while the level of operationalisation is quite granular in some cases, in others, it is far from being so. For example, Singapore's strategy has specified the workforce number (fifteen thousand AI practitioners by 2027), which is linked to the country's national AI strategy. In other cases, like for the

United States and European Union, there are separate, adjacent workforce strategies (NCWES, 2023), and the Cybersecurity Skills Academy.

4.2 Governance Centralisation and Strategy-to-Curriculum Coupling

Within this corpus, governance centralisation is directly linked to tight strategy-to-curriculum coupling. The model of Singapore, whereby AI Singapore, the Cyber Security Agency, and the Ministry of Education work under a unified Smart Nation agenda, is the only model in which there is the clearest line of continuity between national policy and classroom/workplace initiatives. This is not the case in the United Kingdom and India where, unlike Singapore, there is an explicit process of devolution/federal fragmentation (DfE guidance for England only in the UK; differences in state-based implementation of initiatives in India). The middle ground belongs to the European Union where, even as the Skills Academy and ECSF ensure competency consistency through a unified language, implementation rests with 27 Member States.

4.3 A Persistent Assessment and Evidence Gap Cuts Across All Jurisdictions

Irrespective of the governance structure, the literature on education-research pertaining to the topic of cybersecurity interventions reviewed in Section 2.5 indicates poor and largely stagnant assessment practice within the cybersecurity educational intervention literature, where less than one out of ten studies included in the largest corpus of reviewed research utilizes an existing assessment tool. The issue in question does not seem to be jurisdictionally specific in the literature at hand, which implies that this problem exists on a field level.

4.4 AI-in-Education and AI-for-Cybersecurity Are Institutionally Siloed

Regardless of country of jurisdiction, the institutions that are charged with crafting and implementing AI in education policies (such as the respective Ministry of Education, or DfE equivalent) differ institutionally from the institutions responsible for implementing cybersecurity capabilities through AI (the cyber agencies like ONCD, ENISA, or CSA Singapore). The 2026 briefing by the ATARC working group constitutes a rare example where AI in education, cybersecurity via AI, and university campus digital infrastructure are addressed as one convergent policy problem. Yet the literature at large has not caught up with this integrated approach. Nigeria constitutes a rare counterexample on paper: the NITDA agency responsible for AI strategy and cybersecurity policy is also responsible for the kindergarten-to-university curriculum mandate, thus having a narrower institutional gap between AI and education and cybersecurity than the multiagency United States and EU.

4.5 A Capacity-Constrained, Regionally Embedded Pattern Distinguishes the Nigerian Case

Nigeria's comparative position reflects a trend that is not observed across the five jurisdictions: a high level of policy ambition, a policy that is particularly expressed in the curricular sequencing, accompanied by a very low level of supranational harmonisation and a significant deficit in workforce-capacity. While the number of cybersecurity professionals in Nigeria is still advancing to the United States (482,985), as compared to the other five jurisdictions, the per-capita number of cybersecurity professionals is inconsistent than any of the other five per-capita numbers reviewed, even though the jurisdictional curricular timeline (kindergarten-to-tertiary cybersecurity education from 2026) is more comprehensively scoped than the provisions in the source documents observed for the United States, United Kingdom, or India. Nigeria's AU-level legal framework, the Malabo Convention, still has not entered into force after nine years because of its requirement of reaching the ratification threshold, which has not been observed by most of the African Union member states, unlike the more developed supranational instruments of the European Union (the AI Act, the ECSF) or Singapore's bilateral coordination arrangements. The reverse is true in cases of capacity constrained jurisdictions, however, where the binding constraint on cybersecurity education readiness is implementation and workforce capacity, as opposed to strategic and curricular design (as was observed in higher-income comparators in Sections 4.1 and 4.2).

5 DISCUSSION

The findings suggest that the key governance issue between the national AI policy and cybersecurity education is the curricular translation gap: there is a persistent sign in the national and supranational level strategy documents that cybersecurity education is relevant to AI readiness, but mechanisms to implement this signal in validated classroom practice, competency crosswalks, funded curriculum development and outcome assessment are underspecified or delegated to a separate governance track. This gap aligns with and can be explained by the documented weaknesses in the assessment of AI-augmented cybersecurity education in the research literature: When national policy is not explicit on what competencies cybersecurity education should teach or how to measure them, it is not surprising that fewer than half of the interventions cited in the literature report any type of outcome assessment.

Even the comparison indicates a governance trade-off, not a simple and better governance model. Tight coupling provides traceability and a measurable workforce target, but is delivered via a small, central co-ordinated workforce system which can struggle to scale up to larger or more federated polities without compromising the local responsiveness which the United States' National AI Initiative; National Cyber Workforce and Education Strategy (NCWES) (2023) concept highlights as one of its strengths. The common-framework-plus-Member-State-implementation model offered by the European Union is an alternative of intermediate level of coupling, balancing the need for harmonisation within a large and diverse set of jurisdictions with some of the advantages of a common framework, which may be a more replicable model than either the Singaporean or the purely federated poles of the comparison.

There are equity considerations of institutional siloing, which the literature has started to consider, though not fully, in the context of Section 4.4. In contexts where AI-in-education policy is separate from AI-for-cybersecurity policy, under-resourced institutions face the double jeopardy of not being funded or having their AI integration priorities reflected in curricula, which was explicitly noted in the ATARC briefing and implicitly in comparative assessments of India's capacity-constrained federal rollout. A comparative governance crosswalk between each jurisdiction's AI policy instruments and each jurisdiction's competency frameworks for cybersecurity (NICE, ECSF, or equivalent) and curricular authority of its education ministry would be useful to reveal these gaps in coverage in a manner that the currently siloed literatures do not.

Lastly, the lack of an assessment gap in governance models with high levels of strategic coupling also indicates that it is not enough to just centralise. In the reviewed literature, no field-level validated-instrument problem is solved by the tightly coordinated system as observed patterns in this comparative corpus. This means that strategy to curriculum linkage is not a silver bullet solution to closing the curricular translation gap, and it is also essential to invest in the creation of cybersecurity-education measurement tools, which are not a current high priority in cybersecurity strategy documents, yet are essential to closing the curricular translation gap.

In the Nigerian context, the curricular translation gap in the context of capacity constrained environment is reframed. While the findings in the United States, European Union, and India are primarily related to a coordination and design issue, findings in Nigeria are related to a resourcing and workforce issue that also is accompanied by a relatively well-specified curricular design. This is important for policy transfer because the point of difference is that the policy recommendations that focus on high income/high-capacity systems aim to tackle a different bottleneck than the one Nigeria and, by extension, much of West Africa is working on right now: shortages of teachers, infrastructure, and finance, as opposed to the lack of a curricular mandate. The limited state of the harmonisation of the competency lists under the Malabo Convention also means that Nigeria can count on a regional counterpart to the ECSF for the foreseeable future to help coordinate competency definitions between the states, since the responsibility falls entirely to the NITDA agency that has to carry the burden of both strategic design and implementation.

6 CONCLUSION

This review adopted a synthesis of policy instruments and academic literature informed by insights from the PRISMA framework to compare the preparedness of six jurisdictions (the U.S., the EU, the U.K., Singapore, India, and Nigeria) for AI policy and cybersecurity education. It concludes that "cybersecurity" is a priority identified in every research jurisdiction's national policy or plan for AI, but that the operational connection between that priority and known curriculum and assessment for cybersecurity is underdeveloped across all jurisdictions and weakest when AI-in-education and AI-for-cybersecurity governance are institutionally distinct. While the coupling of strategy to curriculum is tighter in centralised systems like Singapore, no jurisdictions in the corpus have been able to solve the problem of a lack of validated assessment instruments at the field level for cybersecurity education in their federated or co-regulatory system. Nigeria is added to the comparison to illustrate the fact that the nature of the “curricular translation gap” is not uniform; in higher-capacity, higher-income systems, it is mostly a problem of coordination and specification, while Nigeria, and it is reasonable to assume much of West Africa, has an unusually explicit curricular demand alongside a workforce and resourcing gap that is larger than anywhere else in the corpus, exacerbated by a still-immature region-wide legal architecture under the African Union’s Malabo Convention.

Three concrete priorities for policymakers in higher-capacity systems are suggested in the review: First, integrating explicit, measurable cybersecurity-education goals into national AI strategy documents rather than in the neighbouring, separately managed workforce strategy documents; second, investing in the development and use of rigorously tested assessment tools for cybersecurity-education interventions, similar in rigour to the competency frameworks already established for workforce positions; and third, formally connecting the institutions that govern AI-in-education with institutions that govern AI-for-cybersecurity, as seen in the ATARC working group and the UK-led International Coalition on Cybersecurity Workforces, that converge around AI. The priorities in Nigeria (and other capacity constrained jurisdictions) have an emphasis on the following priorities: Financing for the 2026 curricular rollout is

sustainable and diversified, not donor-dependent; investment in teacher supply and infrastructure is also part of the priorities, alongside curriculum design; and support for the development of a regional competency and legal framework similar to the EU's ECSF is also a priority, which will be available to complement national efforts. For researchers, the review calls for comparative studies over the long term that measure the impact of national policy change on graduate competency; and for further development of the comparative governance crosswalk recommended here, more attention should be paid to extending the list of comparative governance contexts by adding more lower-resource and non-English-language contexts, particularly those not represented in the present corpus. With the time between discovery of vulnerabilities and exploitation being reduced even further, the consequences of failing to fill this curricular translation gap will be felt most deeply by the education systems least prepared to do so on their own.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Acknowledgments

I sincerely thank Dr Michael Ebere Ajonuma for his wonderful contributions.

Disclosure of conflict of interest

There are no conflicts of interest.

REFERENCES

[1] Airlie H., Ayesha G., Emre K., Adriano S. K. (2026) Artificial intelligence policy worldwide: a comparative analysis. R. Soc. Open Sci. 1 13(2): 242234. https://doi.org/10.1098/rsos.242234

[2] ATARC Cybersecurity Education and Workforce Development Working Group. (2026). The convergence of AI-cybersecurity in education, workforce development, and campus infrastructure: Executive and policy briefing package. Advanced Technology Academic Research Center.

[3] African Union. (2014/2023). Convention on Cyber Security and Personal Data Protection (Malabo Convention). Entered into force June 2023.

[4] Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S., & Wasim, M. (2023). Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches. Symmetry, 15(12), 2175.

[5] Ahmed, A., Watterson, C., Alhashmi, S., & Gaber, T. (2024). How universities teach cybersecurity courses online: A systematic literature review. Frontiers in Computer Science, 6. https://doi.org/10.3389/fcomp.2024.1499490

[6] Anderson, A., Ahmad, A., & Chang, S. (2024). Case-based learning for cybersecurity leaders: A systematic review and research agenda. Information & Management, 104015.

[7] Crabb, J., Hundhausen, C., & Gebremedhin, A. (2024). A critical review of cybersecurity education in the United States. In Proceedings of the 55th ACM Technical Symposium on Computer Science Education, Vol. 1 (pp. 241–247).

[8] Crawford, A., & Ji, J. (2023). Comment to the Office of the National Cyber Director on a national strategy for a cyber workforce, training, and education. Center for Security and Emerging Technology, Georgetown University.

[9] CrowdStrike. (2023). National priorities for AI: Comments on the National AI Strategy request for information.

[10] Cyber Security Agency of Singapore. (2024). Operational technology (OT) cybersecurity masterplan.

[11] Department for Education (UK). (2023). Generative artificial intelligence in education [Policy paper].

[12] European Union Agency for Cybersecurity (ENISA). (2022). European cybersecurity skills framework (ECSF).

[13] European Union Agency for Cybersecurity (ENISA). (2023a). A governance framework for national cybersecurity strategies.

[14] European Union Agency for Cybersecurity (ENISA). (2023b). Multilayer framework for good cybersecurity practices for AI

[15] European Union Agency for Cybersecurity (ENISA). (2026). ENISA's view on cybersecurity in the frontier AI era [Position paper].

[16] Global Cyber Security Capacity Centre, University of Oxford. (2026). AI cybersecurity readiness workshop: Singapore

[17] Gorsky, M. A. (2026). Artificial Intelligence as Game Changer in Cybersecurity: What We Learned in 2025-2026, and how this is relevant for Africa (arXiv:2606.20102). arXiv. https://doi.org/10.48550/arXiv.2606.20102

[18] Government of India, Ministry of Education. (2020). National Education Policy 2020.

[19] Government of the United Kingdom. (2021). National AI strategy

[20] Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., & De Nicola, R. (2021). Framework, tools and good practices for cybersecurity curricula. IEEE Access, 9, 94723–94747.

[21] ISC2 (2026) Cybersecurity Workforce Study | ISC2 | https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study. Accessed April 7, 2026

[22] Kifaru, F. R. (2025). Artificial intelligence tools in education systems: A structured review of applications, challenges, and implications. Security Science Journal, *7*(1).

[23] National Information Technology Development Agency (NITDA), Nigeria. (2025). National Artificial Intelligence Strategy.

[24] National Information Technology Development Agency (NITDA), Nigeria. (2024). Nigerian AI Strategy and Policy Framework.

[25] National Institute of Standards and Technology (2020). NICE Cybersecurity Workforce Framework.

[26] Nott, C. (2025). Organizational Adaptation to Generative AI in Cybersecurity (arXiv:2506.12060). arXiv. https://doi.org/10.48550/arXiv.2506.12060

[27] Obiokafor, I. N. (2026). Empowering The Next Generation: AI In Cybersecurity Education for Resilient Digital Societies. ANSPOLY Journal of Innovative Development (AJID), 3(1), 13-26.

[28] Obiokafor, I. N., & Mbonu, O. (2025). The intersection of digital policy and cybersecurity: Implications for sustainable development. World J Adv Eng Technol Sci, 14, 077-85.

[29] Office of the National Cyber Director. (2023). National Cyber Workforce and Education Strategy (NCWES).

[30] Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., & Witte, G. (2020). Workforce Framework for Cybersecurity (NICE Framework). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181r1

[31] Radu, R. (2025) "The Global Landscape of National AI Strategies." Background paper prepared for World Development Report 2026: Artificial Intelligence for Development. World Bank.

[32] Savas, S., & Karatas, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. International Cybersecurity Law Review, 3(1), 7–34.

[33] Tahereh S., Tayebeh S. (2023) Topical review of artificial intelligence national policies: A mixed method analysis, Technology in Society, Volume 74, 102316, ISSN 0160-791X, https://doi.org/10.1016/j.techsoc.2023.102316.

[34] Tian, J. (2025). Integrating Artificial Intelligence into the Cybersecurity Curriculum in Higher Education: A Systematic Literature Review. Education Sciences. doi: 10.3390/educsci15111540

[35] Airlie H., Ayesha G., Emre K., Adriano S. K. (2026) Artificial intelligence policy worldwide: a comparative analysis. R. Soc. Open Sci. 1 *13*(2): 242234. https://doi.org/10.1098/rsos.242234