UNIJERPS
Unizik Journal of Educational Research and Policy Studies VOL.22 (1);
July-December, 2026 https://unijerps.org
2023 Impact Factor: 6.834; 2022 *Impact Factor*: 5.156; *2021 Impact Factor: 5.641;*
2020 Impact Factor: 5.355. Indexing and Impact Factor URL: http://sjifactor.com/passport.php?id=21363

INDIGENOUS KNOWLEDGE AS CYBER-PEDAGOGY: EFFECT OF THE CULTURO-TECHNO-CONTEXTUAL APPROACH ON SECONDARY SCHOOL STUDENTS' ACHIEVEMENT IN CYBERSECURITY

Agbanimu, Deborah Oluwatosin
0000-0002-5880-1631
National Open University of Nigeria, Abuja

ABSTRACT

Digital transformation is now central to the delivery of the Sustainable Development Goals, yet the cyber insecurity that accompanies rapid connectivity threatens to erode the very development gains that digitalisation is meant to produce. Sub-Saharan Africa carries a disproportionate share of this risk, and the human factor rather than the absence of technology remains the dominant vulnerability. Cybersecurity education at the secondary level is therefore a sustainability intervention, but in Nigeria it is delivered largely through lecture in schools that lack functional ICT laboratories, leaving learners with an abstract and unmotivating account of a concept that governs their daily online lives. This study tested whether the Culturo-Techno-Contextual Approach (CTCA) a culturally responsive, technology-mediated and location-specific pedagogy developed for African science classrooms could improve achievement in cybersecurity without requiring new infrastructure. A mixed-methods, pretest–posttest non-equivalent group quasi-experiment was conducted with 51 senior secondary one (10th grade) computer studies students in two educational districts of Lagos State, Nigeria. The experimental group (n = 28) was taught through the five-step CTCA protocol, in which cybersecurity concepts were anchored in Yoruba indigenous knowledge and cultural practice and reinforced through mobile social media, while the control group (n = 23) received conventional lecture instruction. Achievement was measured with the Cybersecurity Achievement Test (KR-20 = .74) and analysed using ANCOVA with the pretest as covariate; interviews with purposively selected experimental-group students supplied the qualitative strand. The CTCA group significantly outperformed the lecture group, $F(1, 48) = 25.72$, $p < .001$, with a large effect (partial eta-squared = .35; adjusted means 19.26 versus 13.46). Interview data indicated heightened interest, displacement of unproductive screen time, and the emergence of culturally anchored mental models of hacking, malware and cyber ethics. Because CTCA runs on cultural capital and the mobile devices learners already own, it offers a low-cost, low-carbon and locally sustainable route to SDG 4.4 and 4.7, to gender-equitable STEM participation, and to the national cyber-resilience capacity that SDG 9 and SDG 16 presuppose.

Keywords: Cybersecurity Education; Culturo-Techno-Contextual Approach; Indigenous Knowledge; Education for Sustainable Development; SDG 4; Digital Resilience; Culturally Responsive Pedagogy.

Introduction

The 2030 Agenda for Sustainable Development assumes a digital substrate. Financial inclusion, remote learning, telemedicine, e-government, climate monitoring and smallholder market access all now depend on networked systems, and the pace at which low- and middle-income countries are adopting these systems has outstripped the pace at which they are being secured. Cybersecurity risk has consequently become a first-order constraint on development rather than a technical footnote to it: incidents ranging from website defacement and denial-of-service attacks to ransomware and large-scale personal data theft carry measurable economic and social costs, and developing countries are especially exposed because institutional capacity and technical know-how are thin (World Bank, 2025). Continental assessments make the same point in blunter terms, treating cybersecurity not as a narrow technical problem but as a precondition for economic stability and sustainable growth in an African digital economy that is expanding faster than its defences (INTERPOL, 2024; African Union, 2024).

Cybersecurity is the practice of protecting computer systems, networks and data from unauthorised access, theft, disruption and damage. The threat surface confronting an ordinary user now includes malware, phishing, social engineering, ransomware and denial-of-service attacks, and the consequences of a successful attack extend well beyond the individual to data breaches, financial loss and reputational damage at institutional and national scale. A substantial technical countermeasure stack exists firewalls, intrusion detection and prevention systems, antivirus software, encryption yet decades of practice have established that these controls fail at the human boundary. Uchendu, Nurse, Bada and Furnell (2021), synthesising ten years of research on security culture, found that the behavioural and cultural determinants of security outcomes have proven far more stubborn than the technological ones, and that awareness and education remain the least substitutable elements of any protective posture.

If the human factor is decisive, then education is the intervention with the longest sustainability horizon. Technical controls depreciate, require recurrent capital expenditure and are frequently unavailable at the scale required in resource-constrained systems; an educated cohort of digital citizens is a durable, self-replicating asset. This is precisely the logic of Education for Sustainable Development, which locates in schooling the competences that allow societies to anticipate and absorb systemic risk rather than merely react to it (UNESCO, 2020). Framed against the Sustainable Development Goals, cybersecurity education speaks directly to Target 4.4, which concerns relevant technical and vocational skills for decent work, and to Target 4.7, which concerns the knowledge and skills needed to promote sustainable development; it also underwrites the resilient infrastructure of SDG 9 and the reduction of crime, illicit financial flows and institutional insecurity addressed by SDG 16 (United Nations, 2015; Ige, Kupa, & Ilori, 2024).

The urgency is amplified by how young people enter cyberspace. Mobile-first access has expanded far faster than the

protective knowledge that ought to accompany it, and the population of internet users affected by cybercrime continues to grow as smartphone penetration deepens (EDUCAUSE, 2018). Empirical work on student populations has repeatedly found that comfort with devices does not translate into security competence: college students recognise the importance of security awareness training yet participate in it sparingly, and their knowledge is thinnest exactly where it is not scaffolded by default settings or built-in software prompts (Kim, 2014); interventions targeted at raising awareness among students show gains but must contend with attackers who continuously innovate around whatever defensive habits are taught (Peker, Ray, Da Silva, Gibson, & Lamberson, 2016). Where understanding of cybersecurity is shallow, security risk rises, and the gap compounds as technology advances.

Nigeria has recognised this at policy level. The National Cybersecurity Policy and Strategy identifies capacity building and public awareness as pillars of national cyber resilience (Office of the National Security Adviser, 2021), and cybersecurity appears in the senior secondary computer studies curriculum. Delivery, however, is where the policy commitment thins out. Two constraints operate simultaneously in Nigerian classrooms. First, many computer studies teachers have not themselves been trained in cybersecurity as a substantive domain, and so present it declaratively rather than analytically. Second, and more consequentially for a practical subject, the ICT facilities in a large share of Nigerian schools are not equipped with the tools and devices that proper cybersecurity instruction assumes. Teachers therefore resort to classroom assumption in place of practical engagement. When a concept of this kind is delivered without demonstrable referents, learners experience it as abstract: the examples offered are not ones they can relate to, no strong cognitive connection forms, motivation and interest fall away, and achievement follows them down.

The conventional response to this diagnosis is to call for laboratories, devices and bandwidth. That response is correct but slow, capital-intensive and, at national scale, not obviously sustainable. It is worth asking whether the pedagogical resources already present in the classroom the learners' own cultural knowledge, the immediate physical surroundings of the school, and the mobile phones that learners and teachers already carry can be organised to do work that infrastructure has been assumed to do. This is the guiding intuition of the Culturo-Techno-Contextual Approach (CTCA), a teaching method developed by Okebukola (2020) after more than four decades of experimentation with strategies for breaking barriers to meaningful science learning in African settings. CTCA is an amalgam of three frameworks: the cultural context in which all learners are immersed, the technology mediation on which teachers and learners increasingly depend, and the locational context that gives every school a unique identity and supplies the illustrations and local case studies for its science lessons.

A one-size-fits-all model, transplanted from contexts with different material and cultural conditions, has not delivered for the majority of Nigerian learners, as successive public examination results

attest. Introducing methods that are culturally immersive and contextually repositioned is therefore not a matter of pedagogical fashion; it bears on whether a generation acquires the digital competence that national development now presupposes. The present study asks whether CTCA can produce measurably better learning of cybersecurity than the traditional lecture method and considers what an affirmative answer would mean for the sustainability of cybersecurity capacity building in the Global South.

Research Question and Hypothesis

One research question guided the study:

- Will there be a statistically significant difference in the achievement of students taught cybersecurity using the Culturo-Techno-Contextual Approach (CTCA) and those taught using the traditional lecture method?

The corresponding null hypothesis, tested at the .05 level of significance, was that there is no statistically significant difference in the mean achievement scores of students taught cybersecurity using CTCA and those taught using the conventional lecture method.

Literature Review

Cybersecurity as a Sustainable Development Concern

The framing of cybersecurity as a sustainability question is comparatively recent but now well established. Reviews of the intersection between cybersecurity strategy and the Sustainable Development Goals conclude that secure digital infrastructure is not parallel to sustainable development but constitutive of it, since the digital services through which development outcomes are increasingly delivered are only as reliable as their security posture (Ige et al., 2024). The distributional dimension matters here. The populations targeted by digital inclusion programmes first-time mobile money users, patients accessing telemedicine, smallholders using market platforms are frequently those with the least exposure to data exploitation and therefore the least capacity to recognise it, which means that inclusion without security education can convert a development intervention into a vector for fraud and identity theft.

At the institutional level, the World Bank's decade-long cyber resilience programme across 64 countries has centred on national incident response capability, yet its own assessment notes that only a minority of African states maintain an operational national CSIRT, and that as essential services in energy, banking, water and healthcare migrate onto digital rails, the developmental consequences of incidents scale accordingly (World Bank, 2025). Institutional capability of this kind is downstream of human capital. A national CSIRT requires analysts; analysts emerge from a pipeline that begins in secondary school. Cybersecurity education at the school level is thus not merely a protective measure for individual learners but the earliest stage of the workforce formation on which national cyber resilience and by extension the digital delivery of the SDGs depends.

Cybersecurity Education and the Human Factor

The evidence base on cybersecurity awareness among students converges on a consistent finding: exposure to technology does not generate security competence. Kim (2014), surveying undergraduate and

graduate business students against the NIST SP 800-50 framework, found that students understood the importance of information security awareness training and yet largely did not participate in it, and that their knowledge gaps clustered around topics not covered automatically by installed software or website defaults that is, precisely the topics requiring deliberate instruction. Peker et al. (2016) reported comparable patterns in their intervention work with college students, and subsequent studies across multiple regions have replicated the shape of the problem.

Two implications follow for pedagogy. First, security knowledge is not acquired incidentally through use, so curricular provision matters. Second, because attackers continuously develop new strategies to circumvent whatever countermeasures are current, instruction that transmits a fixed inventory of threats will date quickly; what transfers is a durable mental model of adversarial behaviour, trust boundaries and defensive posture. Rote transmission of definitions the dominant mode where teachers lack tools and confidence produces neither. Uchendu et al. (2021) reach a parallel conclusion from the organisational side: security culture is built through sustained, meaning-bearing engagement rather than through compliance-oriented information delivery.

Barriers to Meaningful Learning in Resource-Constrained Classrooms

Where cybersecurity is taught in Nigerian secondary schools, three barriers recur. The first is teacher preparedness: computer studies teachers are frequently generalists whose own training predates the salience of the domain. The second is infrastructural: laboratories are under-equipped or non-functional, so demonstrations that would make an attack surface visible cannot be staged. The third barrier is a consequence of the first two. Deprived of demonstrable referents, teachers fall back on assumption and assertion, and learners encounter cybersecurity as a vocabulary list rather than a set of relationships they can reason about. The concept is then perceived as abstract and difficult, motivation declines, and performance follows.

A fourth barrier is less often named. The instructional materials and examples in circulation are largely imported, and the cultural distance between the illustrations offered and the learner's lived world is itself a cognitive cost. Scholarship on culturally responsive science education in Africa has argued that the dominance of Western-derived teaching methods and materials has contributed to cultural erosion in African schools while simultaneously depressing learning outcomes, and has advanced culturally responsive approaches as a route to decolonising science education (Adam et al., 2025). The argument is not that indigenous knowledge substitutes for scientific content, but that it supplies the anchoring structure through which unfamiliar scientific content becomes learnable.

The Culturo-Techno-Contextual Approach

CTCA was developed by Peter Okebukola and launched in 2015 following more than forty years of inquiry into methods for teaching science meaningfully to African learners (Okebukola, 2020). Established methods cooperative learning, concept

mapping, discovery learning, demonstration, argumentation, mastery learning, vee diagramming has each demonstrated value, but singly or in combination they have not consistently produced deep learning in the presence of the contextual constraints that characterise many African classrooms. CTCA responds by hybridising three frameworks.

The cultural framework foregrounds indigenous knowledge: the accumulated result of communities interpreting the world through their own lens, a distillation of how they understand the world to work and how that understanding can be applied to wellbeing and quality of life. CTCA connects every lesson to the learner's indigenous knowledge system, so that subject matter arrives as an extension of what is already known rather than as a displacement of it. The technology framework responds to observed behaviour: survey evidence indicates that learners congregate on Facebook, YouTube, WhatsApp and comparable platforms for their online activity (Al-Adwan & Smedley, 2013), and CTCA deliberately targets these channels rather than competing with them, capitalising on an enthusiasm that already exists. The contextual framework draws illustrations and case studies from the immediate surroundings of the specific school, which gives every implementation a locally distinct texture.

The empirical record for CTCA has accumulated rapidly and across disciplines. Onowugbeda et al. (2022) found that senior secondary biology students taught variation and evolution through CTCA significantly outperformed a lecture-taught control group, $F(1, 134) = 15.40$, $p < .0001$, on a measure of meaningful learning; a subsequent study by the same group established gains in retention of biology concepts (Onowugbeda et al., 2024). Oladejo et al. (2023) reported comparable results in secondary physics. Adam et al. (2025) extended the evidence to culturally relevant biology pedagogy and critical thinking. Directly relevant to the present study, Awaah, Okebukola, Shabani, Solarin and Okyere (2022) applied CTCA to Python programming a concept students find difficult at secondary level within the Nigerian computer science education curriculum, and found in favour of the approach using ANCOVA with pretest scores as covariate.

What has not been tested is cybersecurity. The concept differs from those already studied in a way that makes it an interesting case: it is not merely difficult but adversarial and largely invisible, and it is the domain where the absence of laboratory infrastructure bites hardest, since the phenomena to be taught cannot be pointed at. If CTCA can carry a concept of that character, the claim that cultural and contextual resources can substitute for material ones is considerably strengthened. This study addresses that gap.

Theoretical Framework

The study rests principally on Vygotsky's theory of social constructivism and Ausubel's theory of the advance organiser, with Education for Sustainable Development supplying the interpretive frame for the findings.

Vygotsky (1962, 1978) held that higher cognitive functions originate in social

interaction and are internalised through mediated activity, and that learning is most productive within the zone of proximal development the distance between what a learner can accomplish independently and what they can accomplish with support. CTCA exposes learners to social interaction on two fronts. The first is cultural and intergenerational: the pre-lesson task of documenting indigenous knowledge and cultural practice requires learners to consult family and community, drawing an older knowledge system into the learning event. The second is peer-based: the mixed-ability, mixed-sex group discussion that follows creates a setting in which more capable peers scaffold less capable ones. Both fronts construct scaffolds operating within the zone of proximal development, and both are available at zero marginal cost, which is material to the sustainability argument developed later.

Ausubel (1963, 1968) proposed the advance organiser as a device for helping learners connect existing ideas to new material. Advance organisers are broader, more inclusive concepts under which incoming content can be subsumed, and their function is to convert what would otherwise be rote learning into meaningful learning. The correspondence with CTCA is direct: the pre-lesson assignment functions as an advance organiser, and the indigenous knowledge surfaced by that assignment supplies the superordinate structure into which the technical content of cybersecurity is then subsumed. Where a learner already possesses a robust concept of a community guardian who defends a settlement against intruders, the distinction between white-hat and black-hat activity is not new information to be memorised but an instance of a structure already held.

Layered over these is the ESD frame. UNESCO (2020) characterises education for sustainable development as requiring transformative, action-oriented and locally grounded pedagogy, and identifies the integration of local and indigenous knowledge as a means of building the competences that sustainable development requires. CTCA satisfies that specification directly, which permits the findings of an achievement study to be read as evidence about sustainable capacity building rather than about classroom technique alone. Figure 1 presents the conceptual relationship among the three CTCA components, the two learning theories and the achievement outcome.

[Insert Fig

Materials and Methods

Research Design

The study employed a mixed-methods design combining quantitative and qualitative data collection. Both strands were used in order to provide a comprehensive analysis of the problem and to add depth of focus that neither strand would supply alone. The quantitative component adopted a pretest–posttest non-equivalent control group quasi-experimental design, administered to an experimental group taught through CTCA and a control group taught through the conventional lecture method. Random assignment of individual students was not feasible because the study operated within intact classes in functioning schools; the non-equivalent group design with pretest covariate adjustment is the standard

response to that constraint. The qualitative component was based on semi-structured interview responses from experimental-group participants and was used to explain the mechanisms underlying the quantitative result.

Participants

Participants were senior secondary one (SS 1, equivalent to 10th grade) students offering computer studies in public secondary schools in Lagos State, Nigeria. The control class comprised 23 students (8 male, 15 female). The experimental class comprised 28 students (15 male, 13 female) and was located in a different educational district from the control class in order to prevent interaction between the two groups and the treatment diffusion that such interaction would produce. Total enrolment in the study was therefore 51 students. Both schools were comparable in type, funding and facility level, and both were subject to the same infrastructural constraints described in Section 2.3. Students in the experimental group were randomly selected for the qualitative interviews.

Instrumentation

Achievement was measured using the Cybersecurity Achievement Test (CAT), a multiple-choice instrument constructed to cover the cybersecurity content of the senior secondary computer studies curriculum, including threat types, cyber ethics, hacking and malicious software. The instrument was validated by specialists in computer science education and measurement, and its reliability coefficient was established at .74, which is adequate for classroom achievement measurement. The same instrument was administered as pretest and posttest to both groups. Interview data were collected using a semi-structured schedule addressing learners' experience of the lessons, their engagement with the pre-lesson tasks, and their perception of the cultural illustrations used.

Treatment Procedure

The teacher in the experimental class followed the five-step CTCA protocol for every lesson in the cybersecurity unit, as set out in Table 1. Full implementation details for the protocol are documented at www.ctcapproach.com.

Table 1. The five-step CTCA implementation protocol as applied to the cybersecurity unit.

Step	Procedure
Step 1	A pre-lesson assignment was given to students on cybersecurity. The task required them to watch specified videos and consult web resources related to the concepts, and to document indigenous knowledge and cultural practices bearing on those concepts.
Step 2	Learners were organised into mixed-ability, mixed-sex groups of eight or more, depending on class size, and allowed ten minutes to interact and compare their findings.
Step 3	The lesson proceeded with interludes of humour and with practical examples drawn from the school's immediate surroundings.
Step 4	The lesson developed further as the teacher drew additional examples from students' day-to-day activities, sustaining teacher–student interaction, using content-specific humour and explicitly clearing misconceptions.

Step	Procedure
Step 5	At the close of each lesson, a summary was sent to the students via WhatsApp.

The control group was taught the same cybersecurity content, over the same period and by a teacher of comparable qualification and experience, using the traditional lecture method: expository presentation, board work, textbook reference and question-and-answer.

Cultural Content of the Treatment

The indigenous knowledge deployed in the experimental lessons was drawn from Yoruba cultural practice, which the participating learners shared. Cyber ethics was explained through the moral principles that regulate conduct in the culture the codified style of greeting elders, and the longstanding family prohibitions against particular activities establishing that a domain can be governed by internalised norms rather than by enforcement alone. Hacking was explained through the figure of the vigilante, known in Yoruba as olode, who guards the village against intruders: the olode occupies the position of the white-hat actor, and the intruder that of the black-hat actor, with the crucial insight that both possess the same knowledge of the village's weak points and are distinguished by intent. Malicious software was explained through the domestic injunction against buying beans containing weevils, kokoro in Yoruba, on the grounds that the presence of a few weevils will over time affect an entire quantity of beans a self-propagating contaminant introduced through an apparently ordinary transaction. Further detail on the full inventory of cultural anchors is contained in the larger project report.

Data Analysis

Because the dependent variable of interest was achievement and randomisation of the experimental and control groups was not possible, analysis of covariance (ANCOVA) was the appropriate analytical tool, with pretest scores entered as the covariate and testing conducted at the .05 level of significance. Preliminary assumption testing was carried out prior to the main analysis. Partial eta-squared was computed as an index of effect size. Qualitative interview data were transcribed and subjected to thematic analysis, with themes derived inductively and then examined against the theoretical propositions of the study. Quotations are reported verbatim and unedited.

Ethical Considerations

Approval to conduct the study was obtained from the relevant education authority and from the management of both participating schools. Informed consent was obtained from parents or guardians and assent from the students themselves, participation was voluntary, and students were free to withdraw at any point without consequence. Data were anonymised at the point of collection and no identifying information is reported. On completion of the study, the cultural instructional materials developed for the experimental group were made available to the control school so that no participant was disadvantaged by group allocation.

Results

Preliminary Assumption Testing

Preliminary tests were conducted to establish that the achievement data satisfied the assumptions underlying ANCOVA. The Levene test of equality of error variances was not significant, $F = 1.616$, $p > .05$, indicating that the homogeneity of variance assumption was tenable. The test of normality likewise returned a significance value greater than .05, $F = .36$, $p > .05$, and the data were therefore treated as conforming to the normality assumption. On this basis the analysis proceeded.

The results revealed a statistically significant difference in the mean achievement scores of students taught cybersecurity using CTCA and those taught using the lecture method, in favour of CTCA, $F (1, 48) = 25.72$, $p < .001$. The adjusted mean achievement score of the experimental group was 19.26 against 13.46 for the control group, a difference of 5.80 points. The associated partial eta-squared of .35 indicates that instructional method accounted for approximately 35 per cent of the variance in posttest achievement after adjusting for prior knowledge, which by conventional benchmarks is a large effect. The null hypothesis was therefore rejected.

Qualitative Findings

Thematic analysis of the interview data yielded three themes that together account for the quantitative result. All quotations are reported unedited.

Theme 1: Displacement of unproductive screen time. Students in the experimental group reported that the pre-lesson video and web tasks did not add to their screen time so much as redirect it. Where most students are readily distracted by, or hooked on, prevailing social media trends, having material that was both watchable and instructional reduced the frequency with which they visited other sites. One respondent put it directly:

> *"I really enjoy watching the videos related to cybersecurity online, it kept me from just watching random videos that are not adding any knowledge to me"*

Students consequently spent part of their after-school time engaging with the subject matter and investigating cultural and indigenous practices bearing on cybersecurity, rather than in non-academic exchange with friends. The lesson summaries sent to the experimental group on WhatsApp served to reinforce learning at the point in the day when the learners were already on the platform.

Theme 2: Peer interaction as a route into the concept. The mixed-ability group discussion in Step 2 was consistently identified as valuable, and specifically as the point at which learners encountered alternative framings of the concept:

> *"I enjoyed the discussion we had in my group, and learning about other ways that cybersecurity can be explained with things around me"*

The formulation used by this respondent explaining cybersecurity with things around me is precisely the contextual mechanism the approach is designed to activate, and its appearance in a learner's own unprompted account suggests that the mechanism was salient to participants and not only to the researchers.

Theme 3: Cultural anchoring and the correction of worldview misconceptions. Students taught through CTCA reported excitement and heightened interest, and interest was reported as highest during the lessons dealing with indigenous knowledge and cultural practices bearing on cybersecurity. In implementing the cultural component, the teacher required students to document indigenous knowledge and cultural practices related to the topics taught. Completing this task allowed students to observe that their indigenous knowledge and cultural practices did not go unnoticed in the science classroom, and several connected those practices readily to the account of cybersecurity given in their instructional materials and textbooks. The cultural element exposed learners directly and indirectly to indigenous knowledge related to the concept, and served in addition to clear misconceptions arising from their cultural worldview a bidirectional function, in that the cultural material both supported the scientific content and was itself examined and corrected where it conflicted with it.

Discussion

Interpretation of the Achievement Effect

The significant advantage recorded by the CTCA group is consistent with the accumulated evidence on culturally relevant science teaching. Okebukola (2020) documents the positive effect of culturally relevant science instruction on both achievement and attitude; subsequent work has established school-context-relevant teaching and technology mediation as contributors in their own right. The present finding aligns with Onowugbeda et al. (2022) in biology, Oladejo et al. (2023) in physics, Adam et al. (2025) in culturally relevant biology pedagogy, and most closely with Awaah et al. (2022), who found in favour of CTCA for Python programming within the same national computer studies curriculum. The consistency of direction and the comparability of effect across four disciplines and multiple research teams is itself evidentially significant: it indicates that what is being observed is a property of the approach rather than an artefact of any single implementation.

The theoretical account of the difference draws on both frameworks set out in Section 3. On the Vygotskian side, the CTCA lessons generated social interaction that the lecture lessons did not: intergenerational interaction in the pre-lesson documentation task, and peer interaction in the mixed-ability group discussion. Both furnished scaffolding within the zone of proximal development, and Theme 2 of the qualitative data locates the value of that scaffolding in the learners' own accounts. On the Ausubelian side, the pre-lesson task functioned as an advance organiser, activating superordinate structures under which the technical content could be subsumed. This is where the specific cultural anchors did their work.

Indigenous Knowledge as Pedagogical Capital

It is worth being precise about why the particular anchors used in this study were effective, because the mechanism generalises. The olode analogy for hacking does not merely give a memorable label to an unfamiliar term. It transmits the structural insight on which the white-hat and black-hat distinction rests that the guardian and the intruder possess the same

knowledge of a settlement's vulnerabilities, and that what separates them is authorisation and intent. That is the conceptual core of ethical hacking, and it is a proposition that learners already hold with confidence in its cultural form. The kokoro analogy for malicious software is similarly load-bearing: it conveys self-propagation, latency and the contamination of a whole system through an apparently ordinary transaction, which is the behavioural profile of a worm or a trojan rather than a superficial resemblance. The cyber ethics anchoring in Yoruba moral codes establishes that a domain can be regulated by internalised norms operating in the absence of enforcement precisely the disposition that security awareness training seeks to build and that Uchendu et al. (2021) identify as the elusive core of security culture.

In each case the indigenous concept supplies not a mnemonic but a schema. This distinction matters for anyone seeking to replicate the approach in another cultural setting: the productive anchors are those whose internal structure is isomorphic to the structure of the target concept, and identifying them requires genuine knowledge of the culture rather than decorative reference to it. The finding also carries an implication that runs in the opposite direction to the one usually emphasised. Because the approach requires learners to document and bring forward cultural practice, and because that practice is then examined against scientific content and corrected where it conflicts, CTCA simultaneously transmits and interrogates the cultural inheritance. It is a mechanism for cultural continuity as well as for science learning, which is relevant to the concern that imported pedagogy contributes to cultural erosion in African schools (Adam et al., 2025).

Technology Mediation and the Redirection of Attention

The technological component produced an effect that the design did not anticipate but that the qualitative data made visible. CTCA brought teaching and learning onto platforms the learners already inhabited WhatsApp, Facebook and YouTube and in doing so competed for attention on the learners' own terrain rather than attempting to prohibit that terrain. The reported outcome was substitution rather than addition: instructional video displaced undirected video. This is a materially different proposition from conventional educational technology integration, which typically requires new devices, dedicated bandwidth and an institutional platform, and which in the Nigerian secondary context is frequently unaffordable. The technology used here was already in learners' hands and already paid for.

The observation is consistent with Al-Adwan and Smedley (2013), whose survey evidence on where learners congregate online informed the design of the CTCA technology framework. It also suggests a refinement worth testing: if the mechanism is attentional substitution, then the effect should be sensitive to the quality and specificity of the curated resources, and a poorly curated resource list should attenuate the advantage. That is a testable prediction and a candidate for subsequent work.

Gender and Equitable Participation

Students were organised into mixed-ability, mixed-sex groups throughout the intervention, and neither the quantitative data nor the interview data surfaced any indication that the approach advantaged one sex over the other. This is a promising signal in a domain where female participation is persistently low and where the pipeline into cybersecurity work is markedly unbalanced, and it accords with the broader CTCA literature, which has examined gender explicitly in several studies without finding differential benefit. It must nevertheless be stated plainly that the present study did not include sex as a factor in the analytical model, and the observation is therefore descriptive rather than inferential. A two-way ANCOVA with method and sex as fixed factors, and the method-by-sex interaction term specified, would be required to support a claim of gender-neutral efficacy. This is identified as a limitation in Section 7 and as a priority for the next study in Section 8.

Implications for Sustainable Development

The sustainability significance of this finding lies less in the size of the effect than in the resource profile of the intervention that produced it. The CTCA implementation required no laboratory, no procurement, no licensing and no new devices. Its inputs were the learners' cultural knowledge, the physical surroundings of the school, and mobile handsets already in circulation. Against a counterfactual in which comparable achievement gains are pursued through the equipping of ICT laboratories nationwide, the approach carries a fraction of the capital cost, negligible recurrent cost, no dependence on grid reliability, and no e-waste or embodied-carbon burden from hardware procurement. Interventions with this profile are the ones that survive the withdrawal of donor funding, which is the operational definition of sustainability in educational development.

Mapped to the Sustainable Development Goals, four linkages are direct. Target 4.4, concerning relevant technical skills for employment and decent work, is served by an approach that raises attainment in a domain with acute and growing labour demand. Target 4.7, concerning the knowledge and skills required to promote sustainable development, is served twice over: in the substantive content, since digital safety is a competence for participation in a digitalised society, and in the method, since UNESCO (2020) identifies the integration of local and indigenous knowledge as itself an ESD competence. Target 5.b and SDG 5 more broadly are engaged through the mixed-sex grouping structure and the absence of observed differential benefit, subject to the caveat in Section 6.4. SDG 9 and SDG 16 are engaged at one remove but substantially: resilient infrastructure and the reduction of illicit financial flows both depend on national cyber capability, and that capability is downstream of the school-level pipeline (World Bank, 2025; INTERPOL, 2024; Ige et al., 2024).

There is a further point about the direction of technology transfer. Cybersecurity capacity building in the Global South is ordinarily conceived as the importation of curricula, tooling and standards developed elsewhere. The present study inverts that conception: the pedagogical asset that

produced the gain was locally held and locally generated, and no external party could have supplied it. If culturally anchored instruction can carry a technical concept of this difficulty, then the constraint on cybersecurity education in resource-limited settings is not solely material, and capacity building strategies that treat it as solely material are leaving the cheapest available resource unused.

Limitations

Several limitations qualify these findings and should inform their interpretation.

1. Sample size and scope. The study involved 51 students in two schools in a single state. Statistical power was adequate to detect an effect of the magnitude observed, but the sample does not support generalisation to Nigeria as a whole, and both schools were public secondary schools in an urban state with atypically high connectivity relative to the national picture.
2. Absence of randomisation. Intact classes were used and assignment was at class level, so pre-existing differences between the groups cannot be excluded despite covariate adjustment. ANCOVA controls for measured prior achievement but not for unmeasured differences in teacher effectiveness, class climate or school-level factors.
3. Teacher effect. The experimental and control lessons were delivered by different teachers, so the treatment effect is confounded to an unknown degree with teacher identity. A crossover design, or the use of the same teacher for both conditions, would isolate the method effect more cleanly.
4. Gender not modelled. As noted in Section 6.4, sex was not entered as a factor in the analysis, and the observation of no differential benefit is descriptive only.
5. Short duration and absence of retention testing. Achievement was measured immediately following the instructional unit. Whether the advantage persists is not established here, although Onowugbeda et al. (2024) report retention gains for CTCA in biology, which suggests the question is worth putting.
6. Behavioural outcomes not measured. The study measured achievement on a written test. Whether improved achievement translates into safer online behaviour the outcome that actually matters for the sustainability argument was not assessed, and the literature gives ample reason to treat that translation as non-automatic (Kim, 2014).
7. Cultural specificity. The anchors used were Yoruba and the participants shared that heritage. Transferability to other Nigerian and African cultural settings requires the identification of structurally equivalent local anchors and cannot be assumed.

Conclusions and Recommendations

The findings of this study indicate that the Culturo-Techno-Contextual Approach significantly increased students' achievement in cybersecurity relative to the conventional lecture method, with a large effect size, in schools that lacked the ICT infrastructure conventionally assumed

necessary for teaching the subject. The qualitative evidence locates the mechanism in three places: the scaffolding produced by intergenerational and peer interaction, the subsumption of technical content under indigenous schemas that learners already held securely, and the redirection of existing screen time toward instructional material on platforms the learners already used. The continued use of CTCA can be expected to enhance learning in cybersecurity, and the approach represents a viable replacement for a conventional method that is failing the majority of learners, as successive public examination results indicate. The approach can be extrapolated to further concepts, consistent with the wave of research now testing its potency across disciplines and fields.

Read against the sustainability agenda, the more consequential finding is the resource profile. An intervention that improves attainment in a strategically critical domain while requiring no procurement, no recurrent expenditure and no new hardware is precisely the class of intervention that education systems under fiscal constraint can adopt at scale and sustain without external support. On that basis the following recommendations are offered.

1. Curriculum authorities should provide for culturally anchored delivery of cybersecurity within the senior secondary computer studies curriculum, rather than treating laboratory provision as a precondition for teaching the subject at all.
2. Teacher professional development should include structured training in identifying culturally isomorphic anchors, since the productive anchors are those whose internal structure matches the target concept and identifying them is a skill rather than an intuition.
3. A national or regional repository of validated indigenous knowledge anchors for STEM concepts, contributed to by teachers across cultural and linguistic groups, would lower the implementation cost for individual teachers and address the cultural-specificity limitation identified in Section 7.
4. Instructional resources for the technology component should be curated for low-bandwidth delivery and for asynchronous access on the messaging platforms learners already use, so that participation does not depend on data affordability.
5. Further research should employ a two-way design with sex as a factor, incorporate delayed post-testing to establish retention, extend to multiple cultural groups within and beyond Nigeria, and most importantly for the sustainability claim include a behavioural measure of online safety practice alongside the achievement measure.

Declarations

Informed Consent Statement: Informed consent was obtained from school authorities, and from all student participants involved in the study.

Data Availability Statement: The data supporting the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES

Adam, U. A., Ayanwale, M. A., Lameed, S. N., Owolabi, T., Onowugbeda, F. U., Oladejo, A. I., Okebukola, P. A., Ogolo, K. G., & Adebowale, M. A. (2025). Bridging culture and science: Culturo-Techno-Contextual Approach in culturally relevant biology pedagogy. The Journal of Educational Research, 118(2), 100–115. https://doi.org/10.1080/00220671.2024.2446898

African Union. (2024). African Digital Compact. Addis Ababa: African Union Commission.

Agbanimu, D. O., Okebukola, P. A., Onowugbeda, F. U., Peter, E. O., Oladejo, A. I., Gbeleyi, O. A., & Ademola, I. A. (2025). Mitigating difficulty in computer studies through Culturo-Techno-Contextual Approach. *The Journal of educational research, 118*(2), 147-155.

Al-Adwan, A., & Smedley, J. (2013). Exploring students' acceptance of e-learning using the Technology Acceptance Model in Jordanian universities. International Journal of Education and Development using Information and Communication Technology, 9(2), 4–18.

Arah, A. N. (2017). Reality Television and the Change Imperative: A Critical Appraisal of Jeta Amata's Dawn in the Creeks". The Creative Artist: *A Journal of Theatre and Media Studies,13(2),* pp 80-90.

Arah, A. N. (2025). Reverse-Acculturation and Identity: An Overview of Recent Tittle-taking Trend among Diaspora Onitsha Indigenes". *Journal of Humanities and Leadership Studies: Journal of Faculty of Arts, Dennis Osadebey University, Asaba, Delta State*, 1(2), 2025, 2971-5741.

Ausubel, D. P. (1963). The psychology of meaningful verbal learning. New York: Grune & Stratton.

Ausubel, D. P. (1968). Educational psychology: A cognitive view. New York: Holt, Rinehart & Winston.

Awaah, F., Okebukola, P., Shabani, J., Solarin, D., & Okyere, E. E. (2022). "I am a cultural teaching method I was successful in the ICT class in the Global South". Cogent Education, 9(1), 2134704. https://doi.org/10.1080/2331186X.2022.2134704

EDUCAUSE. (2018). EDUCAUSE information security guide and student data risk report. Louisville, CO: EDUCAUSE.

Ige, A. B., Kupa, E., & Ilori, O. (2024). Aligning sustainable development goals with cybersecurity strategies: Ensuring a secure and sustainable future. GSC Advanced Research and Reviews, 19(3), 344–360.

INTERPOL. (2024). African cyberthreat assessment report 2024. Lyon: INTERPOL / AFRIPOL.

Kim, E. B. (2014). Recommendations for information security awareness training for college students. Information Management & Computer Security, 22(1), 115–126. https://doi.org/10.1108/IMCS-01-2013-0005

Office of the National Security Adviser. (2021). National cybersecurity policy and strategy 2021. Abuja: Federal Republic of Nigeria.

Okebukola, P. A. (2020). Breaking barriers to learning: The Culturo-Techno-Contextual Approach (CTCA). Slough, UK and Delhi: Sterling Publishers.

Oladejo, A. I., Okebukola, P. A., Akinola, V. O., Amusa, J. O., Akintoye, H., Owolabi, T., Shabani, J., & Olateju, T. T. (2023). Changing the narratives of physics-learning in secondary schools: The role of culture, technology and locational context. Education Sciences, 13(2), 146. https://doi.org/10.3390/educsci13020146

Oluwatosin, A. D., Odoh, C. E., Ufoma, O. F., & Fatusi, O. A. (2025). Exploring the Efficacy of the Culturo-Techno-Contextual Approach in Enhancing Students' knowledge Retention in Flowcharts and Algorithms. *UNIZIK Journal of Educational Research and Policy Studies*, *20*(2).

Onowugbeda, F. U., Okebukola, P. A., Agbanimu, D. O., Ajayi, O. A., Oladejo, A. I., Awaah, F., Ademola, I. A., Gbeleyi, O. A., Peter, E. O., & Ige, A. M. (2022). Can the culturo-techno-contextual approach (CTCA) promote students' meaningful learning of concepts in variation and evolution? Research in Science & Technological Education, 42(2), 395–411. https://doi.org/10.1080/02635143.2022.2084060

Onowugbeda, F. U., Okebukola, P. A., Ige, A. M., Lameed, S. N., Agbanimu, D. O., & Adam, U. A. (2024). A cultural, technological and contextual pedagogy to enhance retention of biology concepts. The Journal of Educational Research, 117(2), 49–60. https://doi.org/10.1080/00220671.2024.2324714

Peker, Y. K., Ray, L., Da Silva, S., Gibson, N., & Lamberson, C. (2016). Raising cybersecurity awareness among college students. Journal of the Colloquium for Information Systems Security Education, 4(1), 17.

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387. https://doi.org/10.1016/j.cose.2021.102387

UNESCO. (2020). Education for sustainable development: A roadmap. Paris: United Nations Educational, Scientific and Cultural Organization.

United Nations. (2015). Transforming our world: The 2030 Agenda for Sustainable Development (A/RES/70/1). New York: United Nations General Assembly.

Vygotsky, L. S. (1962). Thought and language. Cambridge, MA: MIT Press.

Vygotsky, L. S. (1978). Mind in society: The development of higher psychological processes. Cambridge, MA: Harvard University Press.

World Bank. (2025). Enhancing cyber resilience in developing countries. Washington, DC: The World Bank Group.