Discover Computing

Review

Discerning cybers' threats in an era of digitally connected classrooms: lessons for the Nigerian higher education system and society

Adedayo Olayinka Theodorio[1]

Received: 2 December 2024 / Accepted: 17 April 2025
Published online: 07 May 2025
© The Author(s) 2025 OPEN

Abstract
This review explores the risks associated with digital instructional practices, focusing mainly on the implications of cyber threats in higher education digitally connected classrooms and society. Although advancements in technology have enabled the development and use of diverse and adaptable teaching methods and societal endeavours, their impact during and after COVID-19 has also introduced or escalated cyber threats in higher education digitally connected classrooms and society, necessitating a review of approaches to teaching, learning and social engagements in today's digitally rich environment. This review aims to identify the cyber threats confronting digitally connected higher classrooms and society, revealing their various forms in higher education or social environments. A systemic review of the literature was conducted in the study. Specifically, related literature was sourced from databases such as Google, the Online Public Access Catalogue (OPAC), Google Scholar and YouTube educational videos, which revealed malicious encryption, ransomware, cyber spoofing, Open AI-giarism and sextortion as key findings. The findings highlight the essentialities in emphasising the need for collective and continuous awareness of cybersecurity education that all higher education stakeholders must urgently address. Additionally, the findings underscore the importance of continuous engagement with educators, students, parents, and social awareness programs to address cyber threats in higher education and society. However, continuous engagement is not just important but integral to the solution, as it ensures that all stakeholders are actively involved in the fight against cyber threats in digitally connected higher education systems.

Keywords Cyber threats · Digitally connected classrooms · Higher education · Society · Teaching

1 Introduction

The emergence and widespread use of digital technology during and after the COVID-19 pandemic has not only profoundly impacted higher education globally but also sparked innovative changes. This innovativeness of digital technologies accelerates digitally connected educational practices, paving the way for flexible teaching plans and self-motivated or personalized learning experiences [41, 78, 87, 89].

Digitally connected educational practices, which incorporate the use of interactive and interconnected teaching and learning technologies, foster a sense of community among students and their educators, including educators and school administrators [43, 79]. Moreover, these digitally connected technologies, such as interactive mobile devices, smartboards, and virtual laboratories, are transforming instructional plans and connecting lecturers and students for real-time informative and collaborative engagements [83].

✉ Adedayo Olayinka Theodorio, theodorioa@cput.ac.za; theodoriodayor@yahoo.com | [1]Global Institute for Teacher Education and Society, Cape Peninsula University of Technology, Cape Town, South Africa.

Digitally connected technologies introduced during the COVID-19 pandemic for higher education instructional practices [9, 40], such as smartboards, software, tablets, laptops and virtual laboratories, were used to generate, store and process information such that communications are initiated, and knowledge of subject matter is shared between students and between students and between students and educators [40, 83]. The use of these technologies in higher education offers a plethora of opportunities. These include flexible, affordable, collaborative, and innovative teaching strategies that help achieve curriculum objectives and subject matter knowledge [11, 12, 43].

Moreso, the increased use of digitally connected technologies in digitally rich classrooms helps extend teaching methods to create new opportunities for teaching and learning purposes in virtual or physical spaces for educational and personal development [11, 12, 40, 43, 55, 57]. Mahmud et al. [55] and McHaney [57] argued that the disruptive nature of digitally connected technologies necessitated rapid adaptation to learning and teaching anywhere, making learning and teaching possible from different locations and accessing resources or information in the cloud. Conjoining Mahmud et al. [55] arguments, Haleem et al. [43] argued that adapting digital technologies in teaching helps maintain collaboration, equal engagement and effective feedback.

However, the advanced use of digitally connected technologies for educational practices from 2020 and beyond (the COVID-19 pandemic periods and after) has also brought sensitive and heightened debates regarding the threats associated with using digitally connected technologies for higher education practices [26], Hyppönen [44], Bala [21], Idowu [45] and Kergel et al. [49] all contend that risks associated with teaching and learning using digital technologies remain a concern for students, educators and higher education stakeholders. These risks include data breaches, privacy violations, and the potential for academic dishonesty.

Additionally, Alqahtani et al. [13], Alawida et al. [8], Neumann et al. [62], and Ou et al. [67] argued that recent advancements in digital technology, like open artificial intelligence (AI) tools and e-learning, have led to the introduction of large language models (applications) to support knowledge update and content delivery. These large language models, which are AI systems motivated and collectively known as open AI tools, have brought opportunities to classroom teaching, learning and administrative practices in higher education. However, their use also raises concerns about intellectual property, plagiarism, and the potential erosion of traditional pedagogical approaches.

Strengthening the point, Desai and Riedl [30] argued that using Open AI tools in higher education could open opportunities that threaten intellectual property by storing and reproducing solutions for others, leading to potential plagiarism and ethical concerns. Not only these, but Rane et al. [71] contend that their use may also undermine educators' creative pedagogical approaches focused on critical thinking and fact-checking. Reenergizing the aforementioned arguments, the researcher argued that the challenges associated with using Open AI or interconnected technologies in higher education classrooms and administrative practices exacerbate certain risks among students, educators, and administrators. In addition to this, Alyami et al. [14] and Adeola [2] contend that the risks associated with using digitally connected technologies can lead to socially unethical practices among youths or teenagers if they are not correctly oriented, guided or advised.

Based on the arguments presented by the authors mentioned, the researcher opines that it is urgent to be aware of the flaws of digital technologies in digitally connected higher education classrooms. The use of digitally connected technologies (software and hardware) in instructional practices could lead to a risk of unintentional plagiarism, as users may unknowingly rely on and reuse generalized information without adequate acknowledgement, which is highly unacceptable in higher education. Equally important is the potential danger of overreliance on technologies for learning and teaching purposes in higher education, as they could undermine human critical, creative, and responsible abilities [8, 72].

Besides these, in the context of a developing country like Nigeria, poverty, lack of training, support and inadequate or outdated teaching resources remain contested as significant problems confronting a smooth transition to modern learning and teaching practices [5, 18, 64]. To succinctly highlight the context in the Nigerian higher education sector, Igbinovia and Ishola [47], Akinyetun [6], and Badamasi and Utulu [19] identified poverty, stringent economic policy, and the lack of a guiding framework as part of the root cause factors precipitating cybercrimes in the Nigerian higher education, causing more havoc to higher education, and underline the urgent need for immediate attention.

Given the urgency of the issue, it is argued that addressing cyber threats and related risks in the Nigerian higher education sector, society, and elsewhere globally is crucial and of utmost importance to all concerns in higher education systems. Neglect could continue to raise significant concerns about the safety and security of the lives of students and educators and, most worrisomely, the mental health implications of the dilemma.

For clarification purposes, threats are used in this review as an adverse use of digitally connected technologies in such a way that they inflict pain, injury, and damage to actors, records, intellectual property, and the mental health of hardworking students and staff members [51, 76]. The threat could also come in the form of unauthorized and forceful

access to information, forceful payment, cyber-bullying, online scamming, and use of the information without the owner's consent [69, 70, 81].

To comprehend the subject matter clearly, a systematic review of the literature was adopted as a methodology in this study. The methodology adopted helps identify and analyse cyber threats, which is essential for providing information, creating awareness, and offering guidance for higher education on modern cyber threats that need an urgent address in higher digitally connected classrooms. The systematic review, in particular, is of utmost importance in understanding and addressing the current security challenges, underscoring the significance of the study. Additionally, the systematic review becomes imperative as a document that could be engaged if the current security challenges connected to the misuse of cyber-motivated technologies in society and higher education are to be considered. Not only that, but the systematic review also becomes important for drawing lessons that could prove important as added solutions to the current menace of the cyber and security challenges in Nigerian society and the higher education system. To achieve this aim, as previously mentioned, the author systematically reviews the literature to answer the following questions:

1. What does cyber imply in today's contemporary digitally connected classrooms?
2. What and how do cyber threats impact higher education and digitally connected classroom instructional practices?
3. What strategies, of critical importance, can be employed to effectively mitigate cyber threats in higher-education digitally connected classrooms?
4. How do insights from the review summarise as lessons for the Nigerian higher education system and society?

Furthermore, this systematic review begins by presenting the study's rationale and questions, emphasising the current debates about various cyber threats that digital technology poses in digitally connected higher education classrooms. These debates are particularly relevant in these uncertain and transitional times, marked by rapid technological advancements and the increasing digitisation of education. Not only those, but this systematic review examines the essential components of cyber threats and their impacts on society and higher education, considers possible remedies, and draws conclusions that might be implemented in Nigerian higher education practices.

Moving on, it could be safe to argue that the systematic review's consequences are not limited to Nigerian higher education alone, as it provides insightful viewpoints for students, parents, educators, governments, and scholars around the globe, making them feel included and part of a larger community interested in understudying cyber threats in higher education digitally connected classroom. Furthermore, this systematic review has great potential value since it might help raise awareness of cyber threats in higher education digitally connected classrooms. This could help educate and highlight the significance of each person's part in combating the various forms or products of cyber threats in digitally connected higher education classrooms.

Subsequently, the systematic review delves into the methodological approaches used to gather, analyse, and present data. It then concludes with the findings, insightful lessons, discussions, conclusions and implications for policy and practice in higher education. The review's potential impact on policy and practice is substantially discussed, providing insights and recommendations that can empower stakeholders to shape strategies to mitigate cyber threats in digitally connected higher education classrooms.

The following section briefly overviews the methodological approaches employed to gather, analyse, and present data that address the research questions.

2 Methodology

As previously mentioned, this study conducted a systematic approach to review the literature to discern cyber threats in digitally connected higher education classrooms, with a specific focus on both global and Nigerian higher education contexts. The author critically sourced literature from databases such as Google, the Online Public Access Catalogue (OPAC), Google Scholar and YouTube educational videos, focusing on digital technology, cyber meaning, cyber threats, digital classrooms and higher education. These criteria guide the systematic literature review, ensuring the study is thorough and reliable [82]. Notably, the author reviewed the literature to extract keywords related to the topic, which were then methodically arranged and discussed to address the following questions:

1. What does cyber imply in today's contemporary digitally connected classrooms?
2. What and how do cyber threats impact higher education and digitally connected classroom instructional practices?

3. What strategies, of critical importance, can be employed to effectively mitigate cyber threats in higher-education digitally connected classrooms?
4. How do insights from the review summarise as lessons for the Nigerian higher education system and society?

Furthermore, the author meticulously selected keywords such as "digital technology," "cyber," "cyber threats," "digital classroom," and "higher education" to guide the search. The search was limited to peer-reviewed articles, book chapters, conference proceedings and You Tube videos published between 2020 and 2025. The literature on higher education, cyber threats, digital classrooms, cyber and cyber threats in global higher education was thoroughly examined (n = 179). After that, the literature was carefully examined in relation to digital technology, digital classrooms, higher education and cyber threats. However, 139 studies were removed because they did not focus on digital technology, higher education, cyber threats, and neither the Nigerian nor global context.

Next, the author reviewed the remaining articles (n = 40) and recorded the findings on paper before exporting them into an Excel worksheet in Microsoft Word to provide a detailed analysis of the 40 studies. After this process, papers relevant to the research questions were identified. These papers were chosen for their direct relevance to the research questions, while also focusing on problem statement, digital technology, higher education, cyber threats, methodology, and results, all of which are crucial to understanding and addressing cyber threats in higher education.

Furthermore, the literature analysis advanced through a rigorous review of 40 retained articles focusing on cyber threats, higher education, digitally connected classrooms and digital technology. Of these, 24 articles focused on higher education outside the Nigerian context, whereas 16 addressed the Nigerian higher education context. The 24 articles from outside Nigerian higher education contexts helped understand the meanings, forms and suggestions to adhere to when addressing cyber threats in higher education digital classrooms. Likewise, the 16 articles that addressed the Nigerian higher education context helped understand the factors precipitating cyber threats in the Nigerian higher education context and the necessity for urgent address. The review of the included articles sought, identified, and discussed patterns related to cyber threats in digitally connected higher education classrooms (CTDCHEC, which stands for Cyber Threats in Digitally Connected Higher Education Classrooms).

Moving on, Table 1 provides a snippet of literature adapted from outside the Nigerian higher education context. In comparison, Table 2 shows the literature that addresses the subject studied in the Nigerian higher education context, and Table 3 highlights the findings drawn from the literature reviewed. These tables present snippets of the critical analysis of 40 retained studies, each of which contributes significantly to understanding cyber threats in contemporary higher education (HE) digitally connected classrooms, including the strategies that can be employed to mitigate CTDCHEC effectively.

In addition to Table 1 above, which describes CTDCHEC literature adapted outside the Nigerian higher education setting, Table 2 exemplifies CTDCHEC literature, and a YouTube video related to Nigerian higher education classrooms.

After presenting examples from the literature that emphasise CTDCHEC within and outside the higher education sector in Nigeria, Table 3, which follows, provides a summary of the findings derived from the comprehensive systematic literature review aimed at answering the research questions.

In the following headings, the author elaborates on the findings presented in Table 3.

3 Findings: the results are discussed in relation to the research questions outlined in Section 1

3.1 Cyber in contemporary digitally connected classrooms

This discussion in this section answers the question: What does 'cyber' imply in today's contemporary digitally connected classrooms? In this context, 'cyber', or "cyberspace", refers to using digital and interconnected computers, typically over the Internet, to exchange information and resources [53, 70]. It involves a network through which computers (e.g. digitally connected technologies), whether in the exact location or different locations, communicate and share resources to achieve specific objectives [7, 15].

In higher education, digitally connected learning spaces have led to the adoption of internet-enabled computers and AI tools, which provide access to online databases and enable intelligence gathering over the internet [52]. Moreover, the adoption of cyber-oriented digital technologies such as internet-enabled computers, smartphones, interactive whiteboards, and AI tools, for instance, has facilitated unrestricted access to resources for interactive, innovative and flexible

Table 1 Snippet of CTDCHEC literature adapted from outside Nigerian HE

Authors	Threats Identified	Research	Methodology	Inferences from the reviewed article(s) in association with CTDCHEC
Perwej et al. [70] Bahtiri et al. [20]	Malicious encryption and illegal access	A systematic literature review on the cyber security Cyber security in educational institutions	Systematic review of literature Literature review and interviews	Framework and research work on the various forms and strategies of mitigating cyber threats is needed to discourage cyber threats in higher education or workplaces
Suarez et al. [77]	Ransomware and bandwidth vulnerability	Unsafe at any Bandwidth: Towards understanding risk factors for ransomware in higher education	Case study approach	Higher education institutions are especially vulnerable cyber-threats because of their diverse network services, which are accessible via public internet protocol (IP) addresses. Attackers view institutions' IPs as attractive targets and tamper with them to redirect communications to gain access to the data or information of both the institution and its users, hereby giving them opportunity to request for money
Eshetu et al. [36] Cheng and Wang [28]	Malicious entry Unauthorised and malicious access	Cybersecurity vulnerabilities and solutions in Ethiopian university websites Institutional strategies for cybersecurity in higher education institutions	Survey Review of related literature	There is an urgent need to strengthen the security posture of the university websites, to protect it from malicious entry and redirecting to access sensitive data and of students, staff and organisation as a whole. The studies emphasizes the need for proactive cybersecurity measures, guidelines, and awareness in the realm of higher education instructional practices
Parray et al. [68]	Cyber spoofing	The dark side of publishing: Unveiling the deceptive tactics of cloned journals in India	Explorative case study	More awareness and research is needed to expose academics to fraudulent activities and invites for publication and conference presentation. This is envisaged to safe academics from paying money to fraudulent conferences and publications
Malasowe et al. [56]	Spoofing	Techniques and best practices for handling cybersecurity risks in educational technology environment	A methodical literature review	
Mohammadkarimi [59]	Open AI-giarism	Teachers' reflections on academic dishonesty in EFL students' writings in the era of artificial intelligence	Questionnaire and Interviews	The ethical use of Open AI tools must be prioritized and protected in higher education in order to produce morally upright and honest graduates

Table 2 CTDCHEC literature and YouTube video exemplifying the Nigerian HE context

Authors	Possible Threats Identified	Research	Methodology	Inferences from the reviewed article(s) in association with CTDCHEC
Adeola [2]	Cyber Bullying and Sex-Tortion	Nigerian scammers extradited to the US to face justice	A critical YouTube video exemplifying sex-tortion case	Parents and education stakeholders must intensify efforts to raise awareness of the implications of sextortion and cyberbullying in higher education environments and society at large
Ifon [46]	Cyber bullying	Management of cyberbullying: a qualitative exploratory case study of a Nigerian University	Interviews, documents, and archival records	
Idowu [45]	Yahoo-Yahoo: Malicious and dishonest behaviour, facilitating rapid financial independence	Cybercrimes and challenges of cybersecurity in Nigeria	Questionnaire and Review of literature	The urgent need to curb increasing cybercrime, such as Yahoo Yahoo, in Nigerian higher education cannot be overstated. A law that spells out the punishments for offenders and highlights the implications for the mental health of the victims needs to be prioritised and developed for public access and as a handbook for all higher education students in Nigeria
Igbinovia and Ishola [47]	Spyware, malicious attacks, data leakages, unauthorised data access	Cyber security in university libraries and implication for library and information science education in Nigeria	Questionnaire and interview	The university's records and information, whether stored online or in the e-library, are at risk of being accessed by unauthorized hackers. To combat information hacking, continuous training is crucial. It could enhance research, increase awareness and engagement, and, most importantly, equip staff, students, and higher education institutions with the knowledge and skills to safeguard their data and documents, ensuring that students and staff members are well-informed and prepared to face data security risks
Bala [21]	Academic dishonesty	The rise of generative AI Chatbots: Threat to academic integrity?	Review paper	Open AI tools have provided various avenues for knowledge access and opportunities to enhance subject matter expertise in higher education. Nonetheless, there is now noticeable unguarded and unprofessional usage, sparking discussions about managing intellectual property and fostering a culture of openness in research among students and educators
Ogwueleka [65]		Plagiarism detection in the age of artificial intelligence: Current technologies and future directions		

Table 2 (continued)

Authors	Possible Threats Identified	Research	Methodology	Inferences from the reviewed article(s) in association with CTDCHEC
Njoku et al. [63]	Malicious codes, malware and password attacks	Fostering cybersecurity in institutional repositories: A case of Nigerian universities	Structured questionnaire	Malware and password attacks may continue to rise, especially with the influx of new digital technologies and Open AI tools in higher education. While these tools can be beneficial to teaching, they also have the potential to perpetuate malicious activities in higher education. It is crucial to understand that perpetrators of malicious cyber-threats may be driven by factors such as lack of support, poverty, jealousy or wickedness. These issues raise concerns for higher educators, stakeholders, parents, and the government. However, they also present opportunities for collective proactive solutions, empowering all stakeholders to address cyber threats head-on

Table 3 Snippet of answers drawn from literature responding to the research questions

Research Question	Snippets from findings	Literature Sampled
What does cyber imply in today's contemporary digitally connected classrooms?	Integrating digitally connected technologies, such as internet-enabled computers, smartphones, interactive whiteboards, and AI tools, has enabled unrestricted access to resources for interactive, innovative, and flexible teaching and assessment methods. This development effectively links classroom teaching and learning practices in specific locations and contexts to global educational practices	Dimitriado and Lanitis [31] Mhlongo et al. [58] Alenezi and Alfaleh [10]
What and how do cyber threats impact higher education and digitally connected classroom instructional practices?	Unauthorized access to and theft of resources, the promotion of predatory publications, conferences and research that deceive scholars and students Privacy concerns and data breaches Spoofing Sex-Tortion Open AI-giarism	Butt et al. [24] Idowu [45] Suarez et al. [77] Adeola (2024) [68] Mohammadkarimi [59] Bala [21]
What strategies, of critical importance, can be employed to effectively mitigate cyber threats in higher-education digitally connected classrooms?	Firewall Implementation Routine system check by institution's IT managers Password changing and reauthorisation Workshop and communal continuous awareness	De Ramos [29] Krupa [50]
How do insights from the review summarise as lessons for the Nigerian higher education system and society?	Section 5	

teaching and assessment methods, thereby connecting classroom teaching and learning practices in specific locations and contexts to global educational practices [31, 58].

Furthermore, the aforementioned digital technologies not only enhance teaching methods and foster greater engagement and instant communication among students and educators inside and outside the classroom but also open up a world of possibilities for connected goal actualization and skills development. Moreover, the rapid development of cyber inclinations and the integration of cyber-oriented digital technologies in classroom practices has ushered in new teaching and learning approaches with the potential to extend learning experiences beyond traditional classroom settings [4, 9]. The rapid development of cyber inclinations and integration has resulted in global optimism for connected instructions and engagements in higher education. Higher education institutions in Africa and elsewhere worldwide have embraced integrating cyber-oriented digital technologies that bring global perspectives into classrooms to revolutionize teaching and learning engagements [4, 9].

Furthermore, the researcher added that the incorporation and inclinations of 'cybers' in higher education-connected classrooms also promote 'digital citizenship '. This concept emphasizes students, educators, and institution policymakers' responsible, safe, and respectful use of internet-enabled digital resources. Digital citizenship involves safeguarding and correctly using information online, avoiding illegalities, and utilizing acquired information respectfully and professionally [10].

However, given the myriad possibilities that cyber present in today's digitally connected classrooms, some higher education settings are still dealing with a complex array of threats that can undermine digitally connected higher education classrooms. These threats, including cyberbullying, data breaches, and ransomware, each with its unique nature, will be explored in the following section in response to the challenging question: What and how do cyber threats impact higher education and digitally connected classroom instructional practices?

3.2 Cyber threats impacting higher education and digitally connected classroom instructional practices

The systematic review of the literature for this study has uncovered a significant shift in the higher education landscape. For instance, before the COVID-19 pandemic, cyber threats and associated risks in digitally connected technologies were not widely acknowledged in higher education systems [26].

Regrettably, the misuse of digitally connected technologies has led to a surge in cyber threats, causing significant harm to intellectual property and knowledge formation in higher education practices [11, 12]. As an example, the increased use of digitally connected technologies in higher education has led to a rise in unauthorized access and theft of resources, as well as the proliferation of predatory publications, conferences, and research that deceive scholars and students into investing their time, knowledge, and money in such unethical practices [68, 75, 86]. This misuse underscores the urgent need for action to prevent the potential significant alteration of the landscape of higher education.

However, the implications of these cloned developments in higher education are complex and require thorough examination. Chaudhry and Kazim [27] and Suarez et al. [77], and Mohammadkarimi [59] argue that digitally connected technologies and related artificial intelligence are being misused for malicious and dishonest purposes, posing a significant threat to knowledge development and the safety of information and humanity. Eshetu et al. [36] further note that digitally technologies, whether connected to institutional devices or utilized in virtual environments, can crash, leaving the higher education sector vulnerable to cyber-attacks.

Reflecting on Eshetu et al.'s [36] position on the subject matter, the researcher reasoned that the vulnerability could arise from students and educators being often permitted to bring and use their own devices and data bundles for learning and teaching purposes. As a result, students and educators are encouraged to use their devices in higher education with utmost caution. Orr et al. [66] and Cheng and Wang [28] argued that some students in higher education have mastered the professional skills of misusing and redirecting technology to unethically access details of the institution as well as access questions repositories, making higher education teaching practices a shadow of themselves and making it difficult for central information management staff to identify critical vulnerabilities in the institution's network.

It is crucial that higher education information technologists and faculty members are not only alerted to the offensive nature of cyber threats but also understand it. This understanding is key to identifying and addressing these threats effectively. They must be aware of the potential consequences of tampering with security configurations, unauthorized access to organisational resources, and suspicious attempts that can complicate the security setup of institutions' data repositories.

While the aforementioned discussion highlights generalised discussions on the cyber threats induced by the use of digitally connected technologies that impact teaching, learning, and administration in higher education spaces, it is important to note that other forms of cyber threats also affect higher education instructional practices and society. These threats, which will be discussed in the following sections, further underscore the need for heightened awareness and proactive measures to safeguard the serenity of the teaching profession and the security of information and records in higher education.

3.2.1 Malicious encryption and ransomware payment

In addition to the previous cyber threat discussed, the higher education sector faces other cyber threats, with ransomware and malicious encryption being a significant risk. Ransomware involves the use of malicious software to encrypt data or computer systems, with the threat of blocking access or publishing the data unless a ransom is paid [20, 69, 77, 81]. Suarez et al. [77] argued that higher education institutions are especially vulnerable to these attacks because of diverse network services accessible via public Internet protocol (IP) addresses. As a result, Suarez et al. [77] contend that attackers view institutions' IPs as attractive targets and tamper with them to redirect communications to gain access to the data or information of both the institution and its users.

To bolster the claims put forward by Suarez et al. [77], Butt et al. [24] and Idowu [45] contend that harmful encryption results in considerable privacy and data breaches, affecting multiple sectors, notably higher education. The researcher made sense of the issue by contending that higher education institutions store sensitive information across numerous network servers, making them attractive targets for malicious individuals seeking to exploit weaknesses in their information systems.

It is crucial to understand that the consequences of malicious encryption and attacks, as reasoned by the researcher and in line with the considerations of Nasir et al. [61] to institutional settings, can be severe. They can lead to significant financial losses, damage to reputation and disruptions to academic and administrative functions. However, the researcher contends that these severe consequences of cyber threats in digitally connected higher education classrooms raise serious concerns for immediate collective review and redress among the higher education community, potentially impacting each institution's resources and academic output.

3.2.2 Cyber spoofing

In addition to discussing the nature of cyberattacks in higher education and the use of connected classrooms, cyber spoofing is another form of cyber threat in digitally connected higher education. Cyber spoofing is a particularly deceptive form of attack. Cyber spoofing involves an unknown individual (an imposter) or entity masquerading as someone familiar with aim of gaining access to sensitive information, financial resources, or personal data [73].

Imposters, masquerading as trusted colleagues, reputable sources, or known contacts, aim to deceive their targets [23]. In the context of higher education, cyber spoofing often takes the form of enticing invitations or offers (which are fake or predatory), such as free invitations to academic conferences [68], free online lectures and courses, opportunities for book publishing, free access to online resources, or opportunities to publish in journals [80]. Educators and students must exercise caution, as some have unfortunately fallen victim to these deceptive tactics, often by clicking on seemingly illegitimate emails or links that promise free or cheap career advancement or academic opportunities [3, 42].

Most importantly, spoofing, a fraudulent activity, is also made possible by phishing information from public repositories, including the abstracts of published articles [56]. Through this fraudulent process, imposters access the author(s)' demographic and contact details. Imposters then use this information to create convincing emails offering exciting prospects for professional growth. However, cyber imposters' deceptive emails typically end up as spam folders, and they often target individuals who are ambitious to expand their academic or research endeavours through a cheap and easy channel [85]. The researcher added that if recipients agree to participate or click on illegitimate links, their personal information is compromised, and they may become targets of ransomware attacks. The potential impact of cyber spoofing is significant, and it is essential for everyone in the higher education community and society to be vigilant.

3.2.3 Open AI-giarism

The widespread use of Open AI tools or machines, such as ChatGPT (Chat Generated Pre-Defined Transformers) and other large language models, has made it easier for educators and students to access and generate responses to queries

via predetermined options [67]. It is crucial to carefully evaluate the ethical implications of utilising Open AI tools for academic purposes. Because Open AI tools are machines that inherently possess their own biases and cannot think and adapt as humans, they tend to offer fixed answers to queries, irrespective of the user's geographical context. The solution offered by the tools may result in "Open AI-giarism" if the solutions are reused without thorough critical assessment. This review defines "Open AI-giarism" as the uncritical use of exact solutions, writings, or methods stored in a database across various educational contexts, without appropriate acknowledgement or critical evaluation [22].

Using or reusing the exact solutions, blogs, articles, theses, and dissertations in various contexts and locations, for instance, could lead to concerns about plagiarism and the unethical use of digitally connected technologies such as the ChatGPT in higher education. Therefore, the potential for widespread use of Open AI tools raises concerns about plagiarism among educators and students in this era of educational and social uncertainty. Mohammadkarimi [59], Chaudhry and Kazim [27], Bala [21] and Ogwueleka [65] all made cases for the negative impact of Open AI tools on students and educators in this era of educational and social uncertainty, including the promotion of academic dishonesty and the hindrance of skills and knowledge development.

Additionally, the researcher reasons that an AI tool such as ChatGPT, which provides the same results, resources, outlines and contexts to students and educators in different countries, does not consider the implications of unethical usage or similar solutions for academic integrity as it was previously loaded with predefined instructions, made available online and reused by many scholars and students. Researchers contend that the offensive use of AI tools such as ChatGPT and its shortcomings remain threats to higher education-connected classrooms, as they can lead to Open AI-giarism. Supporting this viewpoint, Bylieva et al. [25] suggested that known and unknown academic dishonesty in using Open AI unethically undermines trust in educational practices. However, the researcher includes the caveat that if academic dishonesty is determined through the conscious or unconscious use of Open AI for academic purposes, the consequences are severe, as they can negatively impact reputation of the academic institution and the scholar in question.

3.2.4 Online sex-tortion

Adeola (2024), in a video loaded on YouTube, relayed an experience of how a student (male) from the Global North was forced to pay ransom through online sextortion. In her explanation, she recounted that three students from Global South bullied a teenager from Global North (name of the countries protected in this review) online by disguising themselves as women to date the boy from Global North and, through that, requested that he (the boy from Global North) send his nude picture to three students from Global South. Upon sending the nude picture, according to the YouTube page of Adeola (2024), "The boy from the global North was asked to pay a ransom of 1000 dollars; otherwise, his nude pictures would be made public. The demand scared the boy, and he wanted to keep his privacy away from his parents and the public. Unfortunately, the boy only had 300 dollars to give them and was scared to inform his parents. When the threat was too much online, the boy from the Global North sent 300 dollars and shot himself in the middle of the night in his room. The sound of the gun woke his parents in their room, only to find their dead son on the floor."

Although Adeola (2024) reported the incidence in the global North—South context, similar cases have been recorded on sexual harassment, cyber bullying and sextortion by Druhanova et al. [33], Madhu and Ramesh [54] and Tzani et al. [84]. The implications for the higher education sector and parents are that educators, especially school counsellors, must occasionally educate new and old students on the dangers of visiting unsafe websites and avoid chatting or disclosing their information online to known or unknown persons. In addition, parents need to be remarkably close to the children (students) with lovely affect and interest in knowing what they are learning online, how they are solving school assignments online, how they are receiving lectures online and who they are interacting with online.

However, the conflicts are that some students demand and want their privacy respected in today's technologically disruptive higher education and society [1]. Some students spend more time using digital technology for entertainment, even when attending lectures online or at home [74]. The act, according to Franco et al. [39], Idowu [45], Dodds et al. [32] and the researcher's reasoning on the literature propositions on the subject matter, leaves students vulnerable when they visit uncensored or unsafe websites. They become psychologically demotivated and disinterested in socially interacting and participating in learning activities, with the culprit of sextortion resolving to assassinate or commit suicide in the process.

Having succinctly examined the impacts and forms of cyber threats in digitally connected higher-education classrooms, it is pertinent to suggest and discuss the strategies that can be used to address or mitigate these threats. These strategies or suggestions respond to the question: What strategies of critical importance can be employed to mitigate cyber threats in higher-education digitally connected classrooms?

4 Strategies to mitigate cyber threats in higher-education digitally connected classrooms

De Ramos [29] and Krupa [50] argued that an institution's IT (Information Technology) staff should consider implementing solid firewalls on network computers to protect against unauthorised entry and malicious encryption or attacks. By enabling firewalls, the researcher notes, unauthorised access from inside and outside the institution can be identified and prevented.

In addition, the researcher reasons that the institution's IT staff should conduct regular security audits on all computers connected to the institution's network and ensure that students, educators, and administrators' passwords are changed intermittently within semesters.

Furthermore, the researcher added that cybersecurity education should be incorporated into the teaching curriculum at all levels of education in any country, not only to create awareness but also to continue efforts aimed at mitigating cyber threats such as ransomware, spoofing, and privacy breaches in higher education. The researcher considers it essential to emphasize that the enactment of cybersecurity education is now imperative and needs to be urgently addressed by all education stakeholders. This education can be in the form of continuous training and community-based awareness programmes on the various types of cyber threats that pose challenges to higher education, human and national development.

In addition to these measures, the researcher identifies that parental involvement is crucial in educating students about the dangers of cyber threats in society and higher education [17]. Most importantly, the researcher suggested that videos and images of victims and products of cyber threats should be shown to students at home by parents or in higher education through counselling experts to fully educate students about the dangers of cyber threats in today's post-pandemic higher education and society.

To conclude, in the discussion of methods to mitigate cyber threats in post-pandemic digitally connected classrooms, institutional stakeholders should conduct various workshops with educators and offer advice, education, and examples of the consequences of the unethical use of technology that supports cyber threats, as well as the dangers of unauthorised access to personal, institutional, and confidential information. For example, workshops could help focus on the cyber threat products and strategies to address them in higher education learning and teaching practices. It could also focus on ways to identify safe websites online, including recognising spoof emails and methods of handling ransom demands.

However, if these measures are overlooked in today's higher education digitally connected classrooms, which are characterized by a high influx of technology and constantly changing dynamics of teaching and learning [4], educators and their students may continue to be susceptible to academic dishonesty, be vulnerable to ransomware, and waste effort and resources in predatory conferences and journals.

In the next section, learnable insights from the review are summarized as lessons for the Nigerian higher education system and society. These lessons respond to the question: How do insights from the review summarise as lessons for the Nigerian higher education system and society?

5 Lessons for the Nigerian higher education system and society

Having reviewed the concept of CTDCHEC in this era of disruptive higher education practices, it is critical to draw insights from the review as learnable and reusable insights for methodological implementation in the Nigerian higher education system. Today, Nigerian society faces massive cyber and security challenges, with their tentacles quickly spreading into the higher education system [16, 38, 88]. According to Essien and Edun [37], Iloanya et al. [48], Dunmade et al. [34], Igbinovia and Ishola [47], Njoku et al. [63] and Eli-Chukwu et al. [35], cyberbully, online fraud, racial abuse, pornography, data breaches, internet fraud, spoofing, and cyber threats imposed through the unethical use of Open AI tools affect the Nigerian higher education sector, culminating in poor reading habits and disinterest in classroom participation.

With the current technology expansion and adoption in Nigerian universities and society, the expansion, according to Igbinovia and Ishola [47], will continue to precipitate cybercrimes, causing more havoc to education and raising a call for redress to address the current higher education and security concerns induced by cyber threats. In support of Igbinovia and Ishola [47], Bala [21] and Njoku et al. [63], but with a caveat, the authors suggest a possible way out in that institutions' networks must be secured with intermittently changed alpha-numeric passwords. The data contained therein should be reinforced to reduce unauthorized breaches or access incidents.

Furthermore, cyber threats mitigating against higher education-connected classrooms identified by Patel and Tailor [69], Bylieva et al. [25], Scharfman [73], Adeola [2], and Mutimukwe et al. [60] include breaching privacy, spoofing, ransomware, sextortion and Open AI-plagiarism. All these threats are also mentioned by Dunmade et al. [34], Essien and Edun [37], Iloanya et al. [48], Igbinovia and Ishola [47], Njoku et al. [63] and Eli-Chukwu et al. [35] ideologies on the various forms of cyber threats in the Nigerian higher education system and elsewhere in the globe.

Considering the arguments made by the aforementioned studies focusing on the subject matter, the researcher draws essential insights from the review as learnable lessons that the Nigerian higher education system and society could adopt to expand awareness of cyber threats, including the mechanisms to curtail the menace in higher education and society:

i. Effective communication is crucial in digitally connected classrooms. Communication between educators and students is needed to discourage engaging in cyber fraud among students. Additionally, educators must provide transparent guidelines for assignments and examination assessments. By communicating with students, educators may reduce confusion, encourage engagement, and ensure that students comprehend what is required to learn with the support of digital technology.
ii. Besides being offered as a course in only computer science departments, cyber education must now be incorporated into the higher education curriculum in all departments, as students who perpetuate cyber fraud may not be limited to a particular department in the Nigerian higher education system.
iii. To increase awareness of cyber education in Nigerian societies, collaborative activities among institutions, student leaders, and parents are needed.
iv. Educators and students must investigate, reinvestigate, and confirm with colleagues before they accept online requests.
v. Parents play a crucial role in preventing cyber fraud. They need to show more love and responsibility in working with their children to avoid engaging in cyber fraud, perpetuating, or falling victim to cyberbullying or oppression. By doing so, they can empower themselves and their children to navigate the digital world safely, reducing the risk of cyber threats in the Nigerian education sector.
vi. Regular assessment and feedback practices that allow students to provide timely and constructive feedback are needed to promote awareness of and curb the different forms of cyber threats in higher education.
vii. The government, higher education, and student leaders must consider engaging in community and social activities to discuss and exemplify cyber threats in education and society in Nigeria's rural and urban settings. This helps promote cybersecurity awareness and makes everyone feel involved and responsible for addressing the possible dangers related to neglect or ignorance.
viii. Continuous training for educators on cybersecurity and cyber threats is not just necessary; it is essential. This ongoing education will help educators and students stay updated and prepared to understand and adapt to constantly changing cyber disruptions, fostering a sense of competence and confidence in safeguarding the quality of training despite technology misuse in higher education and society.
ix. Higher education stakeholders, educators and student representatives must engage in continuous and critical debates on the significance and drawbacks of Open AI tools in higher education instructional practices.
x. Providing comprehensive support services, including counselling services, is crucial for safeguarding the mental health of students and educators in this era of teaching and learning uncertainty. For example, school counsellors must demonstrate deep concern for educators' and students' mental uprightness by offering the necessary support to cope with the stress and challenges of cyber challenges.
xi. IT personnel are critical in securing institutional and student online resources. Their efforts to activate firewalls to resist unauthorized access and restrict access to the internet for unsecured or uncensored websites on campuses are integral to the smooth functioning of the institution. Recognizing and supporting their role in maintaining a secure digital environment is essential.

The researcher, however, concludes the discussion in this section by contending that a thoughtful analysis and application of the insights summed up from the review, if adopted, could minimize the susceptibility to cyber threats in digitally connected higher education classrooms and society.

6 Discussions, implications, limitations, recommendation and conclusion of the study

This comprehensive review delves into the various types of CTDCHEC, their functions, and the risks they present in today's digitally connected higher education classrooms. The methodological approach involved a systematic literature review, drawing from databases such as Google, the Online Public Access Catalogue (OPAC), Google Scholar and YouTube educational videos using keywords such as digital technology, cyber threats, higher education, and digitally connected classrooms. A total of 40 articles, including a YouTube video, were scrutinised to uncover the meanings, nature, and strategies for mitigating or preventing cyber threats in digitally connected higher education classrooms.

Upon critically evaluating the review outputs, it became evident that literature reports, such as those of Adeola [2], Perwei et al. [70], Bahtiri et al. [20], Suarez et al. [77], Malasowe et al. [56], Cheng and Wang [28], Idowu [45], Ifon [46], and Bala [21], all highlighted specific cyber threats associated with the use of digital technologies in higher education. These findings were not limited to the Nigerian higher education context but were also echoed in studies conducted in other African nations and globally. For instance, Perwei et al. [70], Bahtiri et al. [20], Suarez et al. [77], Malasowe et al. [56], and Cheng and Wang [28] all reported, in line with the Nigerian studies, that modern cyber threats induced by the use of digital technologies in higher education include ransomware, phishing, malware, Open AI-plagiarism, data leakages, sextortion, malicious conference and publication alert, spoofing, cyberbullying, Yahoo Yahoo, data leakages, and ultimately, laziness and academic dishonesty.

These threats not only jeopardise critical independence in knowledge formation and self-moral development in higher education but also pose a significant risk to the reputation and morality of higher education institutions. Failure to address these threats with practical and collegial effort could lead to a decrease in higher education morality and a tarnished reputation. Moreover, higher education institutions are at high risk of their information and systems being manipulated at all levels.

Besides, the implications of cyber threats in higher education, if not effectively managed or addressed through technology integration policies in teaching and collegial awareness practices, may result in increased data breaches and the exposure of personal and institutional information to malicious actors. Such oversight could also lead to shortages in productive skills and inaccuracies in academic outputs. Moreover, students and educators might hesitate to pursue research in their respective fields, which could significantly hinder productivity in society and various industries. However, the potential impact of cyber threats on productivity is not a distant worry; it is a pressing issue that demands immediate attention and action.

In another vein, it is imperative to acknowledge the limitations of the review. First, the author's research eyes might have missed important literature that extensively examined the phenomenon reviewed. However, the author's unwavering optimism reassures the audience that the findings reported in this study could indeed impact or add to knowledge on cyber education in higher education teaching and learning spaces. Additionally, the author deems it necessary to make a note that all the arguments expressed in this review are solely those of the author derived from the literature and do not necessarily mean that such actions occur in other institutions or that proactive measures are not taken to curb cyber threats in higher education. On top of these, the author noted that his research eyes might have missed essential measures taken by higher educators and institutions' policymakers to curb the defects of cyber threats in the global and Nigerian higher education contexts.

Based on these, the author suggests that future research utilize either the same methodology or newer techniques to address the limitations noted in this study. For instance, the new study might concentrate on how susceptible Nigeria's higher education academics are to cyberattacks during this period of pedagogical and technological upheavals.

In conclusion, the perspectives presented in this review are not just for reading but also for actively increasing awareness among higher education stakeholders in Nigeria and society. The researcher underscores the importance of continuous engagements and conversations between higher education stakeholders, educators, students, community representatives, and parents. This ongoing dialogue fosters a sense of community and collaboration and is crucial in addressing the various types, functions, and dangers of cyber threats in today's society and digitally connected higher education classrooms.

Author contributions Dr Adedayo Olayinka Theodorio author undertook a comprehensive review of the relevant literature on cyber threats in digitally connected classrooms. He assumed full responsibility for the literature sourcing, analysis, drafting, reviewing, and editing of the article, ensuring a rigorous and thorough research process.

Funding Open access funding provided by Cape Peninsula University of Technology. This independent review, which received no internal or external funding, underlines the integrity and impartiality of its arguments, free from any external influence.

Data availability No datasets were generated or analysed during the current study.

Declarations

Ethics approval and consent to participate The study included a systematic review of relevant literature discussing the phenomenon studied. As such, no ethical clearance is needed to conduct the study. Additionally, a piece of the article was presented at the American University of Nigeria's 2nd International Conference. November 6–9, 2024. Available at https://www.aun.edu.ng/aunic2024.

Consent for publication Not applicable.

Competing interests The authors declare no competing interests.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Adam T. Addressing Injustices through MOOCs: A study among peri-urban, marginalised, South African youth [Apollo - University of Cambridge Repository]. 2020. https://doi.org/10.17863/CAM.56608
2. Adeola FayehunNigerian scammers extradited to the US to face justice**.** 2024. https://www.youtube.com/watch?v=vddlpLsSyWk
3. Adorjan M, Colaguori C. Scams fraud and cybercrime in a globalized society. Crime, deviance, and social control in the 21st century: a justice and rights perspective, 2023, 407.
4. Aithal PS, Aithal S. Future of higher education through technology prediction and forecasting. PIJMESS. 2024;1(1):1–50.
5. Ajayi O, Amorighoye DE, Osayi MI. Root causes of cybercrime among undergraduates in Benin City. Afr J Soc Behav Sci 2025;15(1).
6. Akinyetun TS. Poverty, cybercrime and national security in Nigeria. JCSI. 2021;1(2):86–109.
7. Alam T. Cloud-based IoT applications and their roles in smart cities. Smart Cities. 2021;4(3):1196–219.
8. Alawida M, Mejri S, Mehmood A, Chikhaoui B, Isaac Abiodun O. A comprehensive study of ChatGPT: advancements, limitations, and ethical considerations in natural language processing and cybersecurity. Information, 2023;14(8).
9. Alenezi M, Wardat S, Akour M. The need of integrating digital education in higher education: challenges and opportunities. Sustainability. 2023;15(6):4782.
10. Alenezi N, Alfaleh M. Enhancing digital citizenship education in Saudi Arabian elementary schools: designing effective activities for curriculum integration. Front Educ. 2024;9:1494487.
11. Ali G, Mijwil MM, Buruga BA, Abotaleb M, Adamopoulos I. A survey on artificial intelligence in cybersecurity for smart agriculture: state-of-the-art, cyber threats, artificial intelligence applications, and ethical concerns. Mesopotamian J Comput Sci. 2024;2024:71–121.
12. Ali M, Aini MA, Alam SN. Integrating technology in learning in madrasah: towards the digital age. INJOE. 2024;4(1):290–304.
13. Alqahtani T, Badreldin HA, Alrashed M, Alshaya AI, Alghamdi SS, et al. The emergent role of artificial intelligence, natural learning processing, and large language models in higher education and research. Res Social Adm Pharm. 2023;19(8):1236–42.
14. Alyami A, Sammon D, Neville K, Mahony C. Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives. Info Comput Security. 2024;32(1):53–73.
15. Amadeo M, Ruggeri G. Exploring in-network computing with information-centric networking: review and research opportunities. Future Internet. 2025;17(1):42.
16. Amah NL, Musa MN, Mohammed AJ, Olu-Ojo B. Cybersecurity assessment and vulnerability modelling of networks and web services in Nigerian colleges of education. ABUAD J Eng Res Dev. 2024;7(2):127–38.
17. Andrada MA, Barrot JS. Parental involvement during online learning of learners with special educational needs. Educ Rev. 2025. https://doi.org/10.1080/00131911.2025.2459387.
18. Anuoluwa AG. Influence of cybercrime on the performance outcomes of mass communication students in federal polytechnic in Ado Ekiti. AAU J Bus Educ. 2024;4(2):258–67.
19. Badamasi B, Utulu SC. Framework for managing cybercrime risks in Nigerian Universities. *ArXiv*. 2021. https://arxiv.org/abs/2108.09754
20. Bahtiri Y, Bytyçi E, Idrizi F, Ismaili S, Sejfuli-Ramadani N. Cyber security in educational institutions. J Nat Sci Math UT. 2023;8(15–16):307–14.
21. Bala T. The rise of generative AI chatbots: threat to academic integrity? AI and ethics, academic integrity and the future of quality assurance in higher education, 2025;10.
22. Baskara FR. Chatbots and plagiarism in higher education: navigating the ethical landscape. FX. Risang Baskara, 2023;76.

23. Bedwell BJ. Overcoming the imposter phenomenon: exploring the strategies secondary educators used to cope during the COVID-19 Pandemic (Doctoral dissertation, University of Massachusetts Global). 2022.
24. Butt U, Dauda Y, Shaheer B. Ransomware attack on the educational sector. In AI, Blockchain and Self-Sovereign Identity in Higher Education (pp. 279–313). Cham: Springer Nature Switzerland. 2023.
25. Bylieva D, Lobatyuk V, Tolpygin S, Rubtsova A. Academic dishonesty prevention in e-learning university system. In: World Conference on Information Systems and Technologies. Cham: Springer International Publishing; 2020. p. 225–34.
26. Catal C, Ozcan A, Donmez E, Kasif A. Analysis of cyber security knowledge gaps based on cyber security body of knowledge. Educ Inf Technol. 2023;28(2):1809–31.
27. Chaudhry MA, Kazim E. Artificial intelligence in education (AIEd): a high-level academic and industry note 2021. AI Ethics. 2022;2(1):157–65.
28. Cheng EC, Wang T. Institutional strategies for cybersecurity in higher education institutions. Information. 2022;13(4):192.
29. De Ramos NM, et al. Cybersecurity program for Philippine higher education institutions: a multiple-case study. Int J Eval & Res Educ ISSN. 2022;2252(8822):1199.
30. Desai DR, Riedl M. Between copyright and computer science: the law and ethics of generative AI. arXiv preprint arXiv:2403.14653. 2024.
31. Dimitriadou E, Lanitis A. A critical evaluation, challenges, and future perspectives of using artificial intelligence and emerging technologies in smart classrooms. Smart Learn Environ. 2023;10(1):12.
32. Dodds T, Geboers M, Boukes M. "It Became No Man's Land": the burden of moderating online harassment in newswork. Journal Pract, 2024, 1–18.
33. Druhanova O, Fedonenko A, Nalyvaiko O. Sexual harassment and sextortion in universities as an actual scientific problem. Continuing Profess Educ Theory Pract. 2022;73(4):27–35.
34. Dunmade AO, Tella A, Onuoha UD. A developed framework for studying cyberethical behaviour in North Central Nigeria. J Cybersecurity Educ Res Pract, 2024(1).
35. Eli-Chukwu NC, Igbokwe IC, Ifebude B, Nmadu D, Iguodala W, Uma U, Akudo FU. Challenges confronting e-learning in higher education institutions in Nigeria amid Covid-19. J Appl Res Higher Educ. 2023;15(1):238–53.
36. Eshetu AY, Mohammed EA, Salau AO. Cybersecurity vulnerabilities and solutions in Ethiopian university websites. J Big Data. 2024;11(1):118.
37. Essien ES, Edun EE. Digitalizing cyber security for data management in higher education: implication for Educational Management in Nigeria. Int J Educ Natl Dev. 2024;2(1):70–8.
38. Essien NP, Ekaiko UA. Cyber security: trends and challenges toward educational development in 21st century. Asia-Africa J Educ Res. 2022;2:141–56.
39. Franco M, Falioun SA, Fisher KE, Gaggi O, Ghamri-Doudane Y, Nashwan AJ, Shwamra M. A technology exploration towards trustable and safe use of social media for vulnerable women based on Islam and arab culture. In: Proceedings of the 2022 ACM Conference on Information Technology for Social Good (pp. 138–145). 2022.
40. Funda V. Covid-19 pandemic: digital technology innovations and resilience in South African higher education institutions. African Conference on Information Systems and Technology. 2022; 5.
41. Gonzalez R, Sørum H, Raaen K. Emergency digital teaching during the COVID-19 lockdown: students' perspectives. Educ Sci. 2022;12(3):152.
42. Gururaj HL, Janhavi V, Ambika V, (Eds.). Social engineering in cybersecurity: threats and defences. CRC Press, 2024.
43. Haleem A, Javaid M, Qadri MA, Suman R. Understanding the role of digital technologies in education: a review. Sustain Operat Comput. 2022;3:275–85.
44. Hyppönen M. If it is smart, it is vulnerable. John Wiley & Sons; 2022.
45. Idowu OA. Cybercrimes and challenges of cyber-security in Nigeria. Int J Sociol Dev. 2021;3(1):1–139.
46. Ifon JC. Management of cyberbullying: a qualitative exploratory case study of a Nigerian University. Int J Bull Prevent. 2023;5(2):161–77.
47. Igbinovia MO, Ishola BC. Cyber security in university libraries and implication for library and information science education in Nigeria. Digit Libr Perspect. 2023;39(3):248–66.
48. Iloanya KO, Eneh MI, Ogechukwu AO. Effect of cybercrime on the academic performance of students of tertiary institutions in Enugu State Nigeria. JPDS. 2024. https://doi.org/10.4314/jpds.v15i1.9.
49. Kergel D, Heidkamp B, Telléus PK, Rachwal T, Nowakowski S. The digital turn in higher education. Proceedings of the International Perspectives on Learning and Teaching in a Changing World. Wiesbaden: Springer. 2018. https://doi.org/10.1007/978-3-658-19925-8.
50. Krupa CR. 16 safeguarding digital learning. Cybersecurity and data science innovations for sustainable development of HEICC: healthcare, education, industry, cities, and communities, 228. 2025.
51. Kuah AT, Dillon R. (Eds.). Transformation in a post-covid world: sustainable innovation, disruption, and change. CRC Press. 2021
52. Kumar S, Verma AK, Mirza A. Digital transformation, artificial intelligence and society. opportunities and challenges. https://doi.org/10.1007/978-981-97-5656-8.2024.
53. Lnenicka M, Kysela T, Horák O. Building security and resilience: a guide to implementing effective cybersecurity and data protection measures in smart cities. SSBE. 2025.
54. Madhu S, Ramesh H. A study on online sextoration which targets students on higher education: Bullying and cyber bullying. In: proceeding Of International Conference on Psychology, Health and Humanity. 2023; Vol. 1, pp. 197-209.
55. Mahmud MM, Wong SF, Ismail O. Emerging learning environments and technologies post Covid-19 pandemic: What is next? Advances in information, communication and cybersecurity: proceedings of ICI2C'21, 308–319. 2022. https://doi.org/10.1007/978-3-030-91738-8_29
56. Malasowe BO, Aghware FO, Okpor MD, Edim EB, Ako RE, Ojugo AA. Techniques and best practices for handling cybersecurity risks in educational technology environment (EdTech). NIPES J Sci Technol Res 2024;6(2).
57. McHaney R. The new digital shoreline: How Web 2.0 and millennials are revolutionizing higher education. Taylor & Francis. 2023.
58. Mhlongo S, Mbatha K, Ramatsetse B, Dlamini R. Challenges, opportunities, and prospects of adopting and using smart digital technologies in learning environments: An iterative review. Heliyon. 2023. https://doi.org/10.1016/j.heliyon.2023.e16348.
59. Mohammadkarimi E. Teachers' reflections on academic dishonesty in EFL students' writings in the era of artificial intelligence. J Appl Learn Teach, 2023;6(2).

60. Mutimukwe C, Viberg O, Oberg LM, Cerratto-Pargman T. Students' privacy concerns in learning analytics: model development. Br J Edu Technol. 2022;53(4):932–51.
61. Nasir NNI, Radzuan SN, Azhami BA, Hamidon H. Cyber security in higher education: problem and solution. In: Proceedings of 1st Glocal Symposium on Information and Social Sciences (GSISS) 2023 (p. 128).
62. Neumann M, Rauschenberger M, Schön EM. "We need to talk about ChatGPT": The future of AI and higher education. In 2023 IEEE/ACM 5th International Workshop on Software Engineering Education for the Next Generation (SEENG) (pp. 29–32). IEEE.
63. Njoku IS, Njoku BC, Chukwu SA, Ravichandran R. Fostering cybersecurity in institutional repositories: a case of Nigerian Universities. Afr J Lib Arch Info Sci 2023;33(1).
64. Ogunode NJ, Musa A. Higher education in Nigeria: challenges and the ways forward. ERJBS, 2020;3.
65. Ogwueleka FN. Plagiarism Detection in the age of artificial intelligence: current technologies and future directions. AI and ethics, academic integrity and the future of quality assurance in higher education, 2025;10.
66. Orr SG, Bonyadi CJ, Golaszewski E, Sherman AT, Peterson PA, Forno R, Rodriguez J. Shadow IT in higher education: survey and case study for cybersecurity. Cryptologia. 2024;48(1):26–90.
67. Ou AW, Stöhr C, Malmström H. Academic communication with AI-powered language tools in higher education: From a posthumanist perspective. System. 2024;121: 103225.
68. Parray UY, Loan FA, Khan AM. The dark side of publishing: Unveiling the deceptive tactics of cloned journals in India. JLIS. 2024. https://doi.org/10.1177/09610006241256392.
69. Patel A, Tailor J. A malicious activity monitoring mechanism to detect and prevent ransomware. Comput Fraud Security. 2020;2020(1):14–9.
70. Perwej Y, Abbas SQ, Dixit JP, Akhtar N, Jaiswal AK. A systematic literature review on the cyber security. Int J Sci Res Manage. 2021;9(12):669–710.
71. Rane NL, Choudhary SP, Tawde A, Rane J. ChatGPT is not capable of serving as an author: ethical concerns and challenges of large language models in education. Int Res J Modern Eng Technol Sci. 2023;5(10):851–74.
72. Sakib MN, Islam MA, Pathak R, Arifin MM. Risks, causes, and mitigations of widespread deployments of large language models (LLMs): a survey. arXiv preprint arXiv:2408.04643. 462. 2024.
73. Scharfman J. Crypto phishing and spoofing scams. In: The cryptocurrency and digital asset fraud casebook, Volume II: DeFi, NFTs, DAOs, Meme Coins, and Other Digital Asset Hacks (pp. 193–219). Cham: Springer Nature Switzerland. 2024.
74. Simamora RM, De Fretes D, Purba ED, Pasaribu D. Practices, challenges, and prospects of online learning during Covid-19 pandemic in higher education: lecturer perspectives. Stud Learn Teach. 2020;1(3):185–208.
75. Singh S, Remenyi D. Researchers beware of predatory and counterfeit journals: are academics gullible? EJBRM. 2016;14(1):50–9.
76. Skiba R. Shadows of catastrophe: navigating modern suffering risks in a vulnerable society. After Midnight Publishing. 2024.
77. Suarez L, Alshubrumi D, O'Connor T, Sudhakaran S. Unsafe at any bandwidth: towards understanding risk factors for ransomware in higher education. Procedia Comput Sci. 2024;238:815–20.
78. Sun Y, Xu X. (Eds). The development of personal learning environments in higher education: promoting culturally responsive teaching and learner autonomy. Taylor & Francis. 2024.
79. Tariq MU. Empowering learning through networked and connected education: case studies in digital engagement. In: Cases on Enhancing P-16 Student Engagement with Digital Technologies (pp. 169–198). IGI Global Scientific Publishing. 2025.
80. Teixeira da Silva JA, Al-Khatib A, Tsigaris P. Spam emails in academia: issues and costs. Scientometrics. 2020;122:1171–88.
81. Thakur S, Chaudhari S, Joshi B. Ransomware: threats, identification, and prevention. Cyber Secur Dig Forensics. 2022. https://doi.org/10.1002/9781119795667.ch16.
82. Theodorio AO, Waghid Z, Wambua A. Understanding the influence of online learning platforms on preservice teachers' mental and academic wellness: a systematic review of the literature. utilising positive psychology for the transition into university life, 2024, 181–199. https://doi.org/10.1007/978-3-031-72520-3_11
83. Thompson BW. The connected classroom: using digital technology to promote learning. Teaching in nursing: A guide for faculty, 2016, 324–341.
84. Tzani C, Ioannou M, Fletcher R, Williams TJV. Psychological factors leading to sextortion: the role of personality, emotional factors and sexual needs in victimization. Comput Human Behav, 2024, 108323.
85. Vijayakumar B, Thomas C. The ethics of envisioning spam free email inboxes. AI and Ethics, 2024, 1–24.
86. Wilson P. Academic fraud: Solving the crisis in modern academia. Exchanges. 2020;7(3):14–44.
87. Wolhuter C, Jacobs L. COVID-19, the global education project and technology: disrupting priorities towards rethinking education. Res Soc Sci Technol. 2021;6(2):96–109.
88. Yusuf S, Ibrahim MA. Educational Services in Nigerian Universities: Prospect, Challenges and Way Forward. Fuoye J Educ Manage 2024;1(1).
89. Zografos N.Student Teachers' Experiences of Online Learning During Emergency Remote Teaching to Inform Future Teaching Practice. Master's thesis, European University of Cyprus, Cyprus. 2023

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.