e-ISSN: 3027-0650
Vol. 2, Issue 1, pp 134-144, November 6 -9, 2024

Understanding cyber threats in an era of digitally connected classrooms: Lessons for the Nigerian higher education system and society

Adedayo Olayinka Theodorio (PhD)
Global Institute for Teacher Education and Society
Cape Peninsula University of Technology, Cape Town, South Africa
Corresponding Emails: {theodorioa@cput.ac.za}

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. This review underscores the importance of continuous engagement with educators, students, parents and social awareness programs as part of addressing cyber threats in higher education and society. The author concludes by offering valuable insights to help shape resilient digitally connected higher instructional systems in Nigeria.

Keywords: Cyber threats, digitally connected classrooms, higher education, learning, society, teaching

1. Introduction

The emergence and widespread use of digital technology during and after the COVID-19 pandemic profoundly impacted higher education globally, sparking innovative changes and necessitating digitally connected educational practices [78]. For example, the advanced use of technology during and after the COVID-19 pandemic encouraged digitally connected educational practices, where teaching and learning occurred in the same or different spaces, facilitating flexible teaching plans and self-motivated and personalized learning experiences [36, 73, 81]. Additionally, digitally connected educational practices, which incorporate the use of interactive and interconnected teaching and learning technologies such as interactive mobile devices, smartboards, internet-oriented tablets, internet-enabled laptops, virtual laboratories, and the Internet of Things (IoT), are transforming instructional plans, connecting lecturers and students for real-time informative and collaborative engagements [29, 75].

For example, some of these digitally motivated technologies introduced during the COVID-19 pandemic are now widely used in higher education [9, 35] and will continue to disrupt teaching and learning in the future. Moreover, digitally connected classrooms are described as using electronic and digitally motivated technologies such as smart mobile devices, smartboards, software, tablets, laptops, virtual laboratories and data bundles to generate, store and process information or knowledge or learning resources on course lessons such that communications are initiated and knowledge of subject matter is shared between students and between students or between students and educators in the classroom [35, 75]. For example, [39] and [11] posited that digitally motivated technologies offer opportunities for flexible, affordable, collaborative, and innovative teaching strategies by employing digital technology to achieve curriculum objectives and allowing students to learn subject matter quickly in digitally connected classrooms.

Furthermore, the increased use of digitally connected technologies in digitally rich classrooms now helps extend teaching methods to create new opportunities for teaching and learning purposes in virtual or physical spaces for educational and personal development [12, 35, 39]. For example, [49] and [54] argued that the disruptive nature of digital technology, which includes rapid advancements and changes in the internet landscape, has recently necessitated rapid adaptation to learning and teaching in online environments, making learning and teaching possible from different locations and accessing resources or information in the cloud. Similarly, the study by [39] on the role of digital technologies in education argued that adapting digital technologies as a platform for connected teaching helps maintain students' collaborative, equal engagement and provides effective feedback in virtual settings.

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 the use of digital technologies for digitally connected education practices. In other words, [24], [41] and [46] contend that risks associated with teaching and learning in virtual spaces via digital technologies, otherwise known as cyber risk, remain a concern for educators and higher education stakeholders, generating debates for critique, repositioning, subjection, and research. The cyber risk, also known as cyber threats in higher education, includes unauthorized access to information from students, educators and institutional administrators [10, 62, 74, 24], leading to attacks on higher-level institutions' administrative classified documents, sensitive data, intellectual property, cutting-edge research outputs, and personal data of staff and students, making higher education vulnerable to phishing, theft and electronic ransomware attacks [10, 53, 76].

Additionally, [13], [7], [59] and [61] reasoned that recent advancements in artificial intelligence (AI) have led to the introduction of large language models, such as ChatGPT (Chat Generative Pretrained Transformers), Blender Bot 2.0, DALLE-E, Fireflies, Tome, Bard, BERT, and RoBERT. These large language models, collectively known as open AI tools, have brought opportunities to connect classroom teaching, learning and administrative practices in higher education. From their viewpoint, [13] opined that OpenAI tools offer benefits such as content generation, language translation, scientific research, assignment development, and virtual assistants for knowledge development and writing guidance. However, the researcher, who agreed with [26] on the use of OpenAI tools in higher education, argued that the use of OpenAI tools in higher education threatens intellectual property by storing and reproducing solutions for others, leading to potential plagiarism and ethical concerns. Although OpenAI tools have the potential to revolutionize learning and teaching practices, researchers contend that their use may also undermine educators' creative pedagogical approaches focused on critical thinking and fact-checking.

Furthermore, the challenges associated with using OpenAI in interconnected higher education practices include a lack of transparency, privacy concerns, and the potential for abuse among students, educators, and administrators [26, 2]. Unfortunately, these risks can lead to social and cognitive misalignments and unethical practices in higher education and society [14]. One other concern is that these large language models are trained on vast amounts of internet-sourced text data, making it difficult for them to fully understand or investigate the quality and biases of the information they disseminate [38]. Moreover, the use of large language models in instructional practices encourages unintentional plagiarism risk, which the author called OpenAI-giarism, as users may unknowingly rely on and reuse generalized information without acknowledgement, which is highly unacceptable in higher education. Although large language models such as Open AIs offer significant opportunities for innovation, their use in interconnected higher education classrooms, whether in the Global South or North, also brings about substantial cyber risks or threats to teaching and learning, undermining human moral development and sustenance in society and higher education [7, 66].

Addressing cyber threats or related risks in the post pandemic era, where digital technology continues to dictate and alter life proceedings, is crucial and of utmost importance to all concerns in higher education systems. This continues to raise significant concerns about the safety and security of the lives of students and educators, including unauthorized access to institutional information, records, intellectual property and, most worrisomely, the mental health implications of the dilemma. For reiteration purposes, threats are used in this review as an adverse use of digital technologies or communicable 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 [47, 70]. The threat also comes in the form of online abuse, bullying, scamming, and unauthorized entry to access and use information online without the owner's knowledge or consent [63, 62, 74]. Thus, identifying and analysing cyber threats in this paper review is essential for providing information, creating awareness, and offering guidance for higher education on recent but modern cyber threats that need an urgent address in digitally connected classrooms.

Additionally, this review becomes imperative as a document that could be actively used if the current security challenges connected to the misuse of cyber-motivated technologies in society and higher education are to be considered. The 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.

1.2 Objectives for the Review

The critical objectives considered in this review include the following:

1. Making sense of the world "cyber" and its relevance in today's digitally connected classrooms
2. Examining the nature of cyber threats in higher-education digitally connected classrooms.
3. Evaluating and discussing the various strategies to mitigate cyber threats in higher-education digitally connected classrooms.
4. Drawing insights from this review as lessons for the Nigerian higher education system and society

1.3 Importance of the Review

The use of digital technology in education, particularly in higher education, has significantly increased due to the impact of the COVID-19 pandemic [72]. However, interventions and shifts to digital technology during and after the COVID-19 pandemic encouraged the use of communication between digital and interconnected computers via a medium (otherwise known as cyber communications) to support and deliver objectives in higher education sectors. However, it has raised critical concerns regarding the safety and security of educators' and students' identities, including institutions' official information [17, 21, 52]. Although educational institutions have embraced digital and cloud-oriented technologies for connected teaching, learning and administrative spaces, the associated risks or threats have become a pressing global concern, raising continuous debates among education stakeholders [17, 21], with the Nigerian higher education sector not being left out [42].

In light of these challenges and ongoing debates, examining the cyber threats facing digitally connected higher education classrooms in these transitioning but uncertain periods is essential. This review examines the critical aspects of these cyber threats and their impacts on teaching and learning, explores possible solutions, and draws lessons applicable to higher education practices in Nigeria. By doing so, it seeks to equip students, educators, and education stakeholders in Nigeria with a deeper understanding of the multifaceted nature of cyber threats that could impact digitally connected classrooms in higher education.

Furthermore, the potential impact of this review on the Nigerian higher education system is significant, as it could help further raise or advance awareness of cyber threats in digitally connected classrooms in higher education, providing valuable insights for students, parents, educators, policymakers, and researchers within the Nigerian higher education system and society. The review also underscores the potential for enhancing the safety and security of digitally connected learning spaces in higher education, highlighting the crucial role that each stakeholder plays in this process and fostering a sense of optimism about the future.

2. Review process

Published scientific articles from databases such as Google, Google Scholar, Mendeley, and the Directory of Open Access Journals (DOAJ) were used to gather knowledge on the subject matter under consideration. Moreover, knowledge on the subject matter was also drawn from educational YouTube videos discussing and exemplifying incidents of cyber threats in education and society. In addition, specific keywords, such as cyber education, cybersecurity, cyber threats, and strategies for mitigating cyber threats in higher education, were instrumental in ensuring the relevance of the gathered literature. Additionally, the literature search was limited to articles published between 2020 and 2024, ensuring the currency and accuracy of this review. Moreover, the search was open to the literature within and outside Africa.

In addition to focusing on the literature from 2020--2024, this review selectively incorporates academic reports and educational blogs and videos from 2020--2024. The selection of these reports and blogs was based on their relevance, credibility, and depth of their insights. Their incorporation was also essential for substantiating the review process and providing a comprehensive understanding of cyber threats to interconnected classrooms in higher education contexts. Additionally, incorporating reports, educational blogs, and scientific articles helps gather and present rich reviews by offering a deeper, more nuanced understanding of the different forms of cyber threats to interconnected classrooms and the different stop-gap solutions and advice recommended in the literature. To ensure the appropriateness of the studies, reports and educational blogs included, the author carefully examined the titles and abstracts of published articles or blogs, filtering out irrelevant and outdated articles that were unrelated or aligned with the study's objectives.

This review examines the diverse impacts of cyber threats in digitally interconnected classrooms. It commences by defining the significance of cyber threats in today's digitally linked classrooms, explores the characteristics of cyber threats in such settings, and examines strategies to alleviate the various cyber threats that impede the success of digitally connected classrooms in post pandemic higher education and society. The review presents valuable insights that can be implemented in instructional scenarios in Nigerian higher education, imparting lessons to prepare for emerging crises and establishing resilient digitally connected instructional classrooms and administrative practices suitable for the Nigerian higher education sector. It also stresses the importance of professional development for educators in higher education, reiterating the need for them to continuously gain understanding and awareness of the various risks associated with using digital technologies for connected lessons. Furthermore, it underscores the vital role of the government, education stakeholders, educators, and parents in collaborating to address the identified issues, highlighting the importance of joint efforts in tackling these challenges.

In the next section, the author discusses the phenomenon of cybers in today's digitally connected classrooms by succinctly examining the definition and importance of cyber and interconnected computers and completing the section with the advantages of cyber-connected computers in higher education instructional practices.

2.1 Cybers in contemporary digitally connected classrooms

The term "*cybers*" encompasses the exchange of information between digital and interconnected computers, typically over the internet [63, 51]. It involves a network through which computers, whether in the exact location or different locations, communicate and share resources to achieve specific objectives [51]. In higher education, digital, interconnected computers have led to the adoption of internet-enabled computers and open AI tools, which provide access to online databases and enable intelligence gathering over the internet [48]. Moreover, the adoption of cyber-oriented digital technologies such as internet-enabled computers, smartphones, interactive white boards, blackboards, and open AI tools, for instance, has facilitated unrestricted access to resources for innovative and flexible teaching and assessment methods, thereby connecting classroom teaching and learning practices in certain locations and contexts to global educational practices [55].

In Africa and elsewhere worldwide, higher education institutions have embraced the integration of cyber-oriented digital technologies that bring global perspectives into classrooms to revolutionize teaching and learning engagements [4, 9]. The aforementioned cyber-oriented digital technologies not only enhance teaching methods and foster greater engagement among students and educators in the classroom but also open up a world of possibilities for specific 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 and throughout students' and educators' lifetimes [4, 9]. Importantly, the rapid development of cyber inclinations and integration has resulted in global optimism for connected instructions and engagements in higher education.

Furthermore, the researcher added that the incorporation and inclinations of cybers in higher education-connected classrooms also promote digital citizenship, emphasizing the responsible, safe, and respectful use of internet-enabled digital resources by students, educators, and institution policymakers. Digital citizenship revolves and involves safeguarding and corrective use of information online, avoiding cyber threats or illegalities, and utilizing acquired information in a respectful, knowledgeable, and legal manner. Additionally, the presence of 'cybers' in digitally connected higher education classrooms is a catalyst for collaboration among students and educators. This collaboration fosters a sense of community and shared learning, as well as self-regulated learning.

Self-regulation, as conceptualized by [18] in 1991 and [80] in 2001, aligns with the author's reasoning on the subject matter under investigation and involves the ethical use of digital technologies and software to promote mental stability and ethical technology use in higher education. It is a valuable skill that enables individuals, including learners and educators, to navigate specific learning pathways and use devices ethically with limited supervision. Ultimately, integrating 'cybers' in connected classrooms empowers students and educators to take ownership of the teaching and learning processes, facilitating self-directed learning and the acquisition of reusable skills. With respect to all of these possibilities, there are a myriad of threats in today's higher education-connected 'cybers' classrooms. These threats have different natures, which are discussed below.

2.2 Nature of cyber threats in digitally connected classrooms and higher education

Before the COVID-19 pandemic, cyber threats and associated risks were not widely acknowledged in higher education systems [24]. There has been a limited emphasis on educating and raising awareness within academia and higher education-connected classrooms about the various natures and impacts of cyber threats. Today, sophisticated intelligent technologies for personal and general use are widely adopted, and their accessibility and diversity in the market are increasing [6, 69]. Intelligent technologies now offer unfettered access to information and resource acquisition for educators, students, and administrators in digitally connected higher education teaching and learning spaces [8]. However, the unethical use of these intelligent technologies has exacerbated cyber threats, significantly damaging intellectual property in higher education educational practices [11]. An example of the risks posed by using innovative technologies in higher education is the increased incidence of unauthorized access to and theft of resources and the promotion of predatory publications and designs that deceive scholars and students into investing their time and money in such projects.

The implications of these developments need to be thoroughly examined within the context of higher education. Although intelligent technologies facilitate the establishment of digitally connected classrooms, [25], [71] and [56] argue that their misuse for malicious purposes, such as hacking institutional and student bank accounts, individual or organisational information and identity theft to gain access to classified information, poses a significant threat. In higher education, personal intelligent technologies, whether connected to institutional devices or utilized in virtual environments, render the sector vulnerable. This vulnerability arises 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. However, this practice has led to some students mastering the misuse of technology, making it difficult for central information management staff to identify critical vulnerabilities in the institution's network. The offensive students tamper with security configurations and access communal resources, further complicating the security setup of the institution. Therefore, the concern here is further linked to privacy leakage in workplace networks, organisations, and individual information.

[57] argued that privacy concerns in higher education limit the trust-belief system, ultimately impacting the development of non-self-disclosure behaviours. Although [65] opined that AI-driven higher education transformation could help address privacy issues through predictive analytics, the author argues that higher education with productive interests in this era of post pandemic transformation needs to harness ethical considerations, potential biases, and concerns about faculty roles and pedagogical implications in ensuring fairness, transparency, and accountability in protecting students', educators' and institutions' data privacy and security.

In addition to discussing the nature of cyber threats in digitally connected teaching and learning spaces, other forms of cyber threats in higher education instructional practices and society are discussed below:

2.2.1 Ransomware

In addition to the previous nature of the cyber threat discussed, the higher education sector faces other cyber threats, with ransomware 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 [17, 62, 74]. [71] argued that higher education institutions are especially vulnerable to these attacks because of diverse network services, which are accessible via public internet protocol (IP) addresses. As a result, attackers view these 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.

In addition, [22] opined that privacy concerns and data breaches are significant issues that affect various sectors, including higher education. Higher institutions and other sectors, according to [22], store sensitive personal, financial, and research data, making them potential targets for malicious actors seeking to exploit vulnerabilities in their information systems. The consequences of such attacks, as reasoned by the researcher and in line with [58] considerations on the impacts of cyber threats to institutional settings, can be severe, leading to financial losses, damage to reputation, legal consequences, and disruptions to academic and administrative functions. Importantly, these disruptions impact students, faculty, and staff, underscoring the human cost of cyberattacks.

2.2.2 Cyber Spoofing

In addition to the discussion of the nature of cyberattacks in higher education and the use of connected classrooms, another form of cyber threat in digitally connected higher education is cyber spoofing. Cyber spoofing is a particularly deceptive form of attack. Cyber spoofing involves an unknown individual or entity masquerading as someone familiar with gaining access to sensitive information, financial resources, or personal data [68]. The imposters pose as trusted colleagues, reputable sources, or known contacts to deceive their targets [20]. In the context of higher education, cyber spoofing often takes the form of enticing invitations or offers, such as invitations to academic conferences, online lectures, opportunities for book publishing, free access to online resources, or the chance to publish in journals. Unfortunately, many educators and students have fallen victim to these deceptive tactics, often by clicking on seemingly illegitimate emails or links that promise career advancement or academic opportunities [3, 37].

This fraudulent activity is made possible by the harvesting of information from publicly available sources, including the abstracts of published articles [5, 50]. Through this, imposters gain access to author(s)' demographic details. Cyber imposters then use this information to create convincing emails that appear to offer exciting prospects for students, academics, and professional growth [40]. Moreover, these deceptive emails typically end up as spam folders, and they often target individuals who are eager to expand their academic or research endeavours [77]. The author 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. Thus, the potential impact of cyber spoofing is significant, and it is essential for everyone in the higher education community and society to be vigilant and take proactive measures to protect themselves from these insidious threats.

2.2.3 Open AI-giarism

The widespread use of OpenAI tools, such as ChatGPT and other large language models, has made it easier for educators and students to access and generate responses via predetermined options within ChatGPT. However, it is essential to carefully consider the ethical implications of using these tools. Since machines have their own biases and cannot think

and adapt as humans do, they provide fixed solutions to queries, regardless of the users' geographical locations, which can lead to open AI-giarism. In this review, "open AI-giarism" is described as the use of exact solutions, writings, or methods stored in a database in different educational contexts [19]. Using or reusing the exact solutions, writings, or methods in articles, theses, and dissertations in various contexts and locations, for instance, can be identified via similarity index checker software, raising concerns about new threats to higher education in the post pandemic era, specifically plagiarism and relationships with the unethical use of cyber-oriented digital technologies. The potential for widespread use of open AI raises concerns about plagiarism among educators and students in this era of educational and social uncertainty. According to [56], the negative impact of AI on students and educators in this era of educational and social uncertainty includes the promotion of academic dishonesty and the hindrance of skill development.

Furthermore, [25] argued that open AI is now widely used for academic purposes, with some stakeholders (educators and students) not considering ethical implications. Additionally, an open AI tool such as ChatGPT can provide the same results, resources, outlines and contexts to students and educators in different countries without considering the implications for academic integrity, as it was previously loaded with predefined instructions. The author contend that the offensive use of AI and its shortcomings remain a threat to higher education connected classrooms, as it can lead to OpenAI-giarism. In support of this viewpoint, [23] suggested that known and unknown academic dishonesty in the use of open AI undermines trust in university educational practices. However, the research addresses the caveat that if academic dishonesty is caught through the conscious or unconscious use of open AI, such as ChatGPT, for academic purposes, the consequences are severe, as they can have lasting negative impacts on reputation.

2.2.4 Online Sex-Tortion

[2], in a video loaded on YouTube, relayed an experience of how an American student (male) was forced to pay ransom through online sex-tortion. In her explanation, she recounted that three students from global South bullied a certain teenager from the global North (name of the countries protected in this review) online by disguising themselves as women to date the boy from the global north online and, through that, requested that he (the boy from the global North) send his nude picture to three students from the global South. Upon sending the nude picture, according to [2], “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 wanted to keep his privacy away from his parents and the public. Unfortunately, the boy only had 300 dollars to give them, 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 [2] reported the incidence in the global North-South context, many similar cases might have been recorded in other parts of the world. The implications for the higher education sector and parents are that educators, especially school counsellors, need to 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 a majority of higher education students demand and want their privacy respected and spend more time using digital technology for entertainment purposes even when they are attending lectures, whether online in the classroom or online at home. The act, according to [34], [41], [27] and the researcher’s reasoning, leaves students vulnerable when they visit uncensored or unsafe websites and become psychologically demotivated and disinterested to socially interact and participate in learning activities, with the culprit of sextortion assassinating themselves or committing suicide in the process.

3. Mechanisms to mitigate cyber threats in post pandemic higher education and society

The researcher suggested that the institution's IT department and IT staff should consider implementing solid firewalls on its network computers. By activating firewalls, unauthorized access from within or outside the institution can be detected and blocked. Additionally, the researcher believes that the institution's IT staff should conduct regular security audits on all computers connected to the institution's network and ensure that passwords for students, educators, and administrators are changed regularly. Similarly, awareness programs on the advantages and challenges of cyber usage in institutions should be considered to educate the community about current or modern cyber threats in higher education and society.

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 to continue to 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 ongoing training, community-based awareness programs, and instruction on the various types of cyber threats that pose challenges to human and national development. In addition to these measures, parental involvement is crucial in educating students about the dangers of cyber threats in society and higher education. Most importantly, the researcher suggested that videos and images of victims and instances of cyber threats should be shown to students at home or in their schools to fully educate them about the dangers of cyber threats in today's post pandemic higher education and society.

To conclude, 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 unauthorized access to personal, institutional, and confidential information. For example, workshops could focus on strategies and activities to address the use of plagiarism detection tools and the integration of AI into teaching practices. It could also focus on ways to identify safe websites online, including recognizing spoof emails and methods of handling ransom demands. However, if these measures are overlooked in today's higher education practices, which are characterized by a high influx of technology and constantly changing dynamics of online information access [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, methodological implications in the form of learnable lessons for the Nigerian higher education system and society are discussed:

4. Learnable lessons for methodological implementation in the Nigerian higher education system and society

Having reviewed the concept of cyber threats in digitally connected classrooms in this era of post pandemic educational practices, it is critical to draw up insights from the review as learnable and reusable insights for methodological implementation in the Nigerian higher education system. Today, Nigerian society is facing massive cyber challenges, with their tentacles quickly spreading into the higher education system [15, 32, 79]. According to [29], [21], [31], [44] and [30], 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.

In addition, with the current technology expansion and adoption in Nigerian universities and society, the expansion, according to [43], will continue to precipitate cybercrimes, cause more havoc to education, call for redress and address the current education and security concerns caused by cyber threats. In support of [43] [60], but with a caveat suggesting a possible way out such that hardware, software and infrastructure grant access to the operation and identity of educators, students and administrators must be secured loaded on the institution work network, and the data contained therein should be reinforced to reduce incidents of unauthorized breaches or access. In addition, some of the previously discussed types of cyber threats identified by [62], [23], [68], [2] and [57] include breaching privacy, spoofing, ransomware, sextortion and open AI-giarism and resonating with those mentioned by [28], [31], [44], [5], [15] and [30] ideologies on the forms of cyber threats in the Nigerian higher education system and society.

However, to achieve [43]'s, [60]'s and [79]'s propositions on the subject matter, the researcher draws important lessons from the review that the Nigerian higher education system could adopt to expand awareness of cyber threats and various forms and mechanisms to curtail the menace in education and society:

1. Effective communications are 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 of them [45, 67].
2. The incorporation of cyber education in the higher education curriculum is now needed in all departments, aside offering it as a course in in only computer science departments, as students who perpetuate cyber fraud may not be limited to a particular department in the Nigerian higher education system [16, 28].
3. Collaborative activities among institution and student leaders and parents to increase awareness of cyber education in Nigeria [6]
4. Educators and students must investigate, reinvestigate, and confirm with colleagues before they accept online requests.

5. Parents need to show more love and responsivities in working with their children to avoid engaging in cyber fraud, perpetuating, or falling victim to cyber bullying or oppressions, as some students in the Nigerian education sector are receptive or engage in oppressing their contemporaries online or offline [1, 3].
6. Regular assessment and feedback practices for receiving timely and constructive feedback from students are needed to promote awareness or curbing the different forms of cyber threats in higher education [16, 79].
7. The government, higher education and student leaders need to consider engaging in community and social activities to discuss and exemplify cyber threats in education and society in both rural and urban settings in Nigeria. This will also help promote awareness of cybersecurity and possible dangers related to neglect or ignorance.
8. Continuous training for educators on cybersecurity and cyber threats is not just necessary; it is essential [14]. It will help educators stay updated and prepared to understand and adapt to constantly changing cyber disruptions, ensuring the quality of training despite technology misuse in higher education and society.
9. Higher education stakeholders, educators and student representatives need to engage in continuous and critical debates on the significance and drawbacks of open AI tools in higher education instructional practices.
10. 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. Counselling services must offer the necessary support to cope with the stress and challenges of cyber challenges by demonstrating a deep concern for educators' and students' mental uprightness.
11. IT personnel must play a critical role in securing institutional and students' 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.

The thoughtful analysis and application of the insights mentioned could minimize the susceptibility to cyber threats in digitally interconnected classrooms in Nigeria's higher education system and society.

5. Conclusion

The exploration of digital technology in higher education has led to significant progress in the use of digital tools for teaching and learning in digitally connected classrooms. However, the adoption and use of digital technology in digitally connected classrooms has also sparked concerns about cyber threats in teaching practices within higher education and society. This thorough review explores the different types, functions, and dangers of cyber threats in today's society and digitally connected classrooms in higher education.

Additionally, the review examines methods for preventing cyber threats in digitally connected classrooms by offering strategies to decrease these risks in higher education settings and in society. The perspectives presented in this review can be utilized to increase awareness among higher education stakeholders in Nigeria and society. In conclusion, the researcher emphasized the importance of continuous engagements and conversations between higher education stakeholders, educators, students, community representatives, and parents concerning the various types, functions, and dangers of cyber threats in today's society and digitally connected classrooms in higher education.

Neglecting to address these hazards in higher education and society may lead to severe consequences, such as disruptions in education, exposure to confidential information, and damage to the reputation of educational institutions, students, and the community.

References

[1] Aborisade, R. A. (2023). Yahoo boys, yahoo parents? an explorative and qualitative study of parents' disposition towards children's involvement in cybercrimes. *Deviant Behavior*, *44*(7), 1102-1120.

[2] Adeola Fayehun. (2024). Nigerian scammers extradited to the US to face justice**.** https://www.youtube.com/watch?v=vddlpLsSyWk

[3] Adorjan, M., & Colaguori, C. (2023). Scams Fraud and Cybercrime in a Globalized Society. *Crime, Deviance, and Social Control in the 21st Century: A Justice and Rights Perspective*, *407*.

[4] Aithal, P. S. and Aithal, S. (2024). Future of Higher Education through Technology Prediction and Forecasting. Poornaprajna International Journal of Management, Education & Social Science (PIJMESS), 1(1), 1-50.

[5] Aivaz, K. A., Florea, I. O. and Munteanu, I. (2024). Economic Fraud and Associated Risks: An Integrated Bibliometric Analysis Approach. Risks, 12(5), 74.

[6] Alabdali, S. A., Pileggi, S. F. and Cetindamar, D. (2023). Influential factors, enablers, and barriers to adopting smart technology in rural regions: A literature review. Sustainability, 15(10), 7908.

[7] Alawida, M., Mejri, S., Mehmood, A., Chikhaoui, B. & Isaac Abiodun, O. (2023). A comprehensive study of ChatGPT: advancements, limitations, and ethical considerations in natural language processing and cybersecurity. Information, 14(8),

[8] Alenezi, M. (2023). Digital learning and digital institution in higher education. Education Sciences, 13(1), 88.

[9] Alenezi, M., Wardat, S. and Akour, M. (2023). The need of integrating digital education in higher education: Challenges and opportunities. Sustainability, 15(6), 4782.

[10] Ali, A. and Bhatti, B. M. (2024). Spies in the Bits and Bytes: The Art of Cyber Threat Intelligence. CRC Press.

[11] Ali, G., Mijwil, M. M., Buruga, B. A., Abotaleb, M. and Adamopoulos, I. (2024). A Survey on Artificial Intelligence in Cybersecurity for Smart Agriculture: State-of-the-Art, Cyber Threats, Artificial Intelligence Applications, and Ethical Concerns. Mesopotamian Journal of Computer Science, 2024, 71-121.

[12] Ali, M., Aini, M. A. and Alam, S. N. (2024). Integrating technology in learning in madrasah: towards the digital age. Indonesian Journal of Education (INJOE), 4(1), 290-304.

[13] Alqahtani, T., Badreldin, H. A., Alrashed, M., Alshaya, A. I., Alghamdi, S. S., bin Saleh, K. and Albekairy, A. M. (2023). The emergent role of artificial intelligence, natural learning processing, and large language models in higher education and research. Research in Social and Administrative Pharmacy, 19(8), 1236-1242.

[14] Alyami, A., Sammon, D., Neville, K. and Mahony, C. (2024). Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives. Information & Computer Security, 32(1), 53-73

[15] Amah, N. L., Musa, M. N., Mohammed, A. J. and Olu-Ojo, B. (2024). Cybersecurity Assessment and Vulnerability Modelling of Networks and Web Services in Nigerian Colleges of Education. ABUAD Journal of Engineering Research and Development, 7(2), 127-138.

[16] Aregbesola, A. and Van der Walt, T. (2024). Evidence-based strategies for effective deployment, and utilization of new media for educational purposes by Nigerian university students. Education and Information Technologies, 29(3), 3301-3364.

[17] Bahtiri, Y., Bytyçi, E., Idrizi, F., Ismaili, S. and Sejfuli-Ramadani, N. (2023). Cyber security in educational institutions. Journal of Natural Sciences and Mathematics of UT, 8(15-16), 307-314.

[18] Bandura, Albert (1991). "Social Cognitive Theory of Self-Regulation" (PDF). Organizational Behavior and Human Decision Processes.

[19] Baskara, F. R. (2023). Chatbots and plagiarism in higher education: navigating the ethical landscape. FX. Risang Baskara, 76.

[20] Bedwell, B. J. (2022). Overcoming the Imposter Phenomenon: Exploring the Strategies Secondary Educators Used to Cope During the COVID-19 Pandemic (Doctoral dissertation, University of Massachusetts Global).

[21] Begum, N. (2024). Cyber Safety Consciousness Among the Students Pursuing Higher Education: A Study of Selected Colleges and Universities in Bengaluru—the Capital City of Karnataka. Indian Journal of Public Administration, 00195561241271582.

[22] Butt, U., Dauda, Y. and Shaheer, B. (2023). Ransomware attack on the educational sector. In AI, Blockchain and Self-Sovereign Identity in Higher Education (pp. 279-313). Cham: Springer Nature Switzerland.

[23] Bylieva, D., Lobatyuk, V., Tolpygin, S. and Rubtsova, A. (2020). Academic dishonesty prevention in e-learning university system. In World Conference on Information Systems and Technologies (pp. 225-234). Cham: Springer International Publishing.

[24] Catal, C., Ozcan, A., Donmez, E. and Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. Education and Information Technologies, 28(2), 1809-1831.

[25] Chaudhry, M. A. and Kazim, E. (2022). Artificial Intelligence in Education (AIEd): A high-level academic and industry note 2021. AI and Ethics, 2(1), 157-165.
[26] Desai, D. R., & Riedl, M. (2024). Between Copyright and Computer Science: The Law and Ethics of Generative AI. arXiv preprint arXiv:2403.14653.
[27] Dodds, T., Geboers, M. and Boukes, M. (2024). "It Became No Man's Land": The Burden of Moderating Online Harassment in Newswork. Journalism Practice, 1-18.
[28] Dunmade, A. O., Tella, A. and Onuoha, U. D. (2024). A Developed Framework for Studying Cyberethical Behaviour in North Central Nigeria. Journal of Cybersecurity Education, Research and Practice, 2024(1).
[29] El-Haggar, N., Amouri, L., Alsumayt, A., Alghamedy, F. H. and Aljameel, S. S. (2023). The effectiveness and privacy preservation of IoT on ubiquitous learning: Modern learning paradigm to enhance higher education. Applied Sciences, 13(15), 9003.
[30] Eli-Chukwu, N. C., Igbokwe, I. C., Ifebude, B., Nmadu, D., Iguodala, W., Uma, U. and Akudo, F. U. (2023). Challenges confronting e-learning in higher education institutions in Nigeria amid Covid-19. Journal of Applied Research in Higher Education, 15(1), 238-253.
[31] Essien, E. S. and Edun, E. E. (2024). Digitalizing cyber security for data management in higher education: Implication for Educational Management in Nigeria. International Journal of Education and National Development, 2(1), 70-78. https://www.openjournals.ijaar.org/index.php/ijend/article/view/489
[32] Essien, N. P. and Ekaiko, U. A. (2022). Cyber security: trends and challenges toward educational development in 21st century. Asia-Africa Journal of Education Research, 2, 141-156.
[33] Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. Journal of Cyber Policy, 6(2), 137–154. https://doi.org/10.1080/23738871.2021.1973526
[34] Franco, M., Falioun, S. A., Fisher, K. E., Gaggi, O., Ghamri-Doudane, Y., Nashwan, A. J. and Shwamra, M. (2022). 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).
[35] Funda, Vusumzi (2022). Covid-19 Pandemic: Digital Technology Innovations and Resilience in South African Higher Education Institutions. African Conference on Information Systems and Technology. 5. https://digitalcommons.kennesaw.edu/acist/2022/presentations/5
[36] Gonzalez, R., Sørum, H. and Raaen, K. (2022). Emergency digital teaching during the COVID-19 lockdown: Students' perspectives. Education Sciences, 12(3), 152.
[37] Gururaj, H. L., Janhavi, V. and Ambika, V. (Eds.). (2024). Social Engineering in Cybersecurity: Threats and Defenses. CRC Press
[38] Hadi, M. U., Qureshi, R., Shah, A., Irfan, M., Zafar, A., Shaikh, M. B. and Mirjalili, S. (2023). A survey on large language models: Applications, challenges, limitations, and practical usage. Authorea Preprints.
[39] Haleem, A., Javaid, M., Qadri, M. A. and Suman, R. (2022). Understanding the role of digital technologies in education: A review. Sustainable operations and computers, 3, 275-285.
[40] Hollis, T. R. (2023). All Quiet on The Digital Front: The Unseen Psychological Impacts on Cybersecurity First Responders. University of South Florida.
[41] Hyppönen, M. (2022). If it is smart, it is vulnerable. John Wiley & Sons.
[41] Idowu, O. A. (2021). Cybercrimes and Challenges of Cyber-Security in Nigeria. International Journal of Sociology and Development. Vol 3. No. 1. pp1-139
[42] Ifon, J. C. (2023). Management of cyberbullying: a qualitative exploratory case study of a Nigerian University. International journal of bullying prevention, 5(2), 161-177.
[43] Igbinovia, M. O. and Ishola, B. C. (2023). Cyber security in university libraries and implication for library and information science education in Nigeria. Digital Library Perspectives, 39(3), 248-266.
[44] Iloanya, K. O., Eneh, M. I. and Ogechukwu, A. O. (2024). Effect of Cybercrime on the Academic Performance of Students of Tertiary Institutions in Enugu State, Nigeria. Vol. 15. Issue 1. DOI: https://dx.doi.org/10.4314/jpds.v15i1.9
[45] Kahu, E. R., Thomas, H. G. and Heinrich, E. (2024). 'A sense of community and camaraderie': Increasing student engagement by supplementing an LMS with a Learning Commons Communication Tool. Active Learning in Higher Education, 25(2), 303-316.
[46] Kergel, D., Heidkamp, B., Telléus, P. K., Rachwal, T. and Nowakowski, S. (2018). The Digital Turn in Higher Education. Proc. International Perspectives on Learning and Teaching in a Changing World. Wiesbaden: Springer. https://doi. org/10.1007/978-3-658-19925-8.
[47] Kuah, A. T. and Dillon, R. (Eds.). (2021). Digital Transformation in a Post-Covid World: Sustainable Innovation, Disruption, and Change. crc Press.
[48] Kumar, S., Verma, A. K. and Mirza, A. (2024) Digital Transformation, Artificial Intelligence and Society. Opportunities and Challenges. https://link.springer.com/book/10.1007/978-981-97-5656-8

[49] Mahmud, M. M., Wong, S. F. and Ismail, O. (2022). Emerging learning environments and technologies post Covid-19 pandemic: What is next? Advances in Information, Communication and Cybersecurity: Proceedings of ICI2C'21, 308-319.
[50] Malasowe, B. O., Aghware, F. O., Okpor, M. D., Edim, E. B., Ako, R. E. and Ojugo, A. A. (2024). Techniques and Best Practices for Handling Cybersecurity Risks in Educational Technology Environment (EdTech). NIPES-Journal of Science and Technology Research, 6(2).
[51] Mallick, M. A. I. and Nath, R. (2024). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. World Scientific News, 190(1), 1-69.
[52] Maranga, M. J. and Nelson, M. (2019). Emerging issues in cyber security for institutions of higher education. International Journal of Computer Science and Network, 8(4), 371-379.
[53] Mateus-Coelho, N. and Cruz-Cunha, M. (Eds.). (2023). Exploring cyber criminals and data privacy measures. IGI Global.
[54] McHaney, R. (2023). The new digital shoreline: How Web 2.0 and millennials are revolutionizing higher education. Taylor & Francis.
[55] Mhlongo, S., Mbatha, K., Ramatsetse, B. and Dlamini, R. (2023). Challenges, opportunities, and prospects of adopting and using smart digital technologies in learning environments: An iterative review. Heliyon, 9(6).
[56] Mohammadkarimi, E. (2023). Teachers' reflections on academic dishonesty in EFL students' writings in the era of artificial intelligence. Journal of Applied Learning and Teaching, 6(2).
[57] Mutimukwe, C., Viberg, O., Oberg, L. M. and Cerratto-Pargman, T. (2022). Students' privacy concerns in learning analytics: Model development. British Journal of Educational Technology, 53(4), 932-951.
[58] Nasir, N. N. I., Radzuan, S. N., Azhami, B. A. and Hamidon, H. (2023). Cyber Security in Higher Education: Problem and Solution. In Proceedings of 1st Glocal Symposium on Information and Social Sciences (GSISS) 2023 (p. 128).
[59] Neumann, M., Rauschenberger, M. and Schön, E. M. (2023). "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.
[60] Njoku, I. S., Njoku, B. C., Chukwu, S. A. and Ravichandran, R. (2023). Fostering Cybersecurity in Institutional Repositories: A Case of Nigerian Universities. African Journal of Library, Archives & Information Science, 33(1).
[61] Ou, A. W., Stöhr, C. and Malmström, H. (2024). Academic communication with AI-powered language tools in higher education: From a posthumanist perspective. *System*, *121*, 103225.
[62] Patel, A. and Tailor, J. (2020). A malicious activity monitoring mechanism to detect and prevent ransomware. Computer Fraud & Security, 2020(1), 14-19.
[63] Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N. and Jaiswal, A. K. (2021). A systematic literature review on the cyber security. International Journal of scientific research and management, 9(12), 669-710.
[64] Raiaan, M. A. K., Mukta, M. S. H., Fatema, K., Fahad, N. M., Sakib, S., Mim, M. M. J. and Azam, S. (2024). A review on large Language Models: Architectures, applications, taxonomies, open issues, and challenges. IEEE Access.
[65] Saaida, M. B. (2023). AI-Driven transformations in higher education: Opportunities and challenges. International Journal of Educational Research and Studies, 5(1), 29-36.
[66] Sakib, M. N., Islam, M. A., Pathak, R. and Arifin, M. M. (2024). Risks, Causes, and Mitigations of Widespread Deployments of Large Language Models (LLMs): A Survey. arXiv preprint arXiv:2408.04643. 462.
[67] Sato, S. N., Condes Moreno, E., Rubio-Zarapuz, A., Dalamitros, A. A., Yañez-Sepulveda, R., Tornero-Aguilera, J. F. and Clemente-Suárez, V. J. (2023). Navigating the new normal: Adapting online and distance learning in the postpandemic era. Education Sciences, 14(1), 19.
[68] Scharfman, J. (2024). 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.
[69] Sestino, A. (2024). The challenge of integrating "intelligent" technologies in luxury shopping contexts: The role of brand personality appeal and consumers' status consumption orientation. Journal of Retailing and Consumer Services, 76, 103488.
[70] Skiba, R. (2024). Shadows of Catastrophe: Navigating Modern Suffering Risks in a Vulnerable Society. After Midnight Publishing.
[71] Suarez, L., Alshubrumi, D., O'Connor, T. and Sudhakaran, S. (2024). Unsafe at any Bandwidth: Towards Understanding Risk Factors for Ransomware in Higher Education. Procedia Computer Science, 238, 815-820.
[72] Sultanova, L., Milto, L. and Zheludenko, M. (2021). The Impact of the Covid-19 Pandemic on the Development of Higher Education. Acta Paedagogica Vilnensia, 46, 132-147.
[73] Sun, Y. and Xu, X. (Eds.). (2024). The Development of Personal Learning Environments in Higher Education: Promoting Culturally Responsive Teaching and Learner Autonomy. Taylor & Francis.

[74] Thakur, S., Chaudhari, S. and Joshi, B. (2022). Ransomware: Threats, identification, and prevention. Cyber Security and Digital Forensics, 361-387.
[75] Thompson, B. W. (2016). The connected classroom: Using digital technology to promote learning. Teaching in nursing: A guide for faculty, 324-341.
[76] Ulsch, M. (2014). Cyber threat! How to manage the growing risk of cyber-attacks. John Wiley & Sons.
[77] Vijayakumar, B. and Thomas, C. (2024). The ethics of envisioning spam free email inboxes. AI and Ethics, 1-24.
[78] Wolhuter, C., & Jacobs, L. (2021). COVID-19, the global education project and technology: Disrupting priorities towards rethinking education. Research in Social Sciences and Technology, 6(2), 96-109.
[79] Yusuf, S. and Ibrahim, M. A. (2024). Educational Services in Nigerian Universities: Prospect, Challenges and Way Forward. Fuoye Journal of Educational Management, 1(1).
[80] Zimmerman, B. J. and Schunk, D. H. (2001). Self-Regulated Learning and Academic Achievement: Theoretical Perspectives. New York, NY: Routledge.
[81] Zografos, N. (2023). Student Teachers' Experiences of Online Learning During Emergency Remote Teaching to Inform Future Teaching Practice. Master's thesis, European University of Cyprus, Cyprus.